

NÄRINGSPOLITISKT FORUM RAPPORT #15

BLOCKCHAIN

DECENTRALIZED TRUST



NÄRINGSPOLITISKT
FORUM

BLOCKCHAIN

DECENTRALIZED TRUST

David Bauman
Pontus Lindblom
Claudia Olsson

ENTREPRENÖRSKAPSFORUM

Entreprenörskapsforum är en oberoende stiftelse och den ledande nätverksorganisationen för att initiera och kommunicera policyrelevant forskning om entreprenörskap, innovationer och småföretag. Stiftelsens verksamhet finansieras med såväl offentliga medel som av privata forskningsstiftelser, näringslivs- och andra intresseorganisationer, företag och enskilda filantroper. Författarna svarar själva för problemformulering, val av analysmodell och slutsatser i rapporten.

För mer information se www.entreprenorskapsforum.se

NÄRINGSPOLITISKT FORUMS STYRGRUPP

Per Adolfsson (ordförande), Bisnode

Karin Apelman, styrelseproffs

Anna Belfrage, Körsbärsträdgården

Ulf Berg, Speed Identity

Anna Büniger, Tillväxtverket

Enrico Deiaco, Tillväxtanalys

Anna Hallberg, Almi

Carl B Hamilton, särskild rådgivare till EU-kommisionen

Peter Holmstedt, egen företagare och affärsängel

Daniel Johansson, Vinnova

Christian Ketels, Harvard Business School

Hans Peter Larsson, PwC

Annika Lundius, styrelseproffs

Göran Marklund, Vinnova

Sara Melén, Handelshögskolan i Stockholm

Jan-Eric Sundgren, Volvo

Elisabeth Thand Ringqvist, SVCA

Ivo Zander, Uppsala universitet

TIDIGARE UTGIVNA RAPPORTER FRÅN NÄRINGSPOLITISKT FORUM

#1 *Vad är entreprenöriella universitet och "best practice"?* – Lars Bengtsson

#2 *The current state of the venture capital industry* – Anna Söderblom

#3 *Hur skapas förutsättningar för tillväxt i näringslivet?* – Gustav Martinsson

#4 *Innovationskraft, regioner och kluster* – Örjan Sölvell och Göran Lindqvist, medverkan av Mats Williams

#5 *Cloud Computing - Challenges and Opportunities for Swedish Entrepreneurs* – Åke Edlund

#6 *3D printing – Economic and Public Policy Implications* – Maureen Kilkenny

#7 *Patentboxar som indirekt FoU-stöd* – Roger Svensson

#8 *Byggmarknadens regleringar* – Åke E. Andersson och David Emanuel Andersson

#9 *Sources of capital for innovative startup firms* – Anna Söderblom och Mikael Samuelsson

#10 *Företagsskattekommittén och entreprenörskapet* – Arvid Malm (red)

#11 *Innovation utan entreprenörskap?* – Johan P Larsson

#12 *Sharing Economy* – Anna Felländer, Claire Ingram och Robin Teigland

#13 *A Review of the Circular Economy and its Implementation* – Almas Heshmati

#14 *Den svaga länken? - inkubatorernas roll i det svenska innovationssystemet* – Olof Ejeremo

© Entreprenörskapsforum, 2016

ISBN: 978-91-89301-85-6

Författare: David Bauman, Pontus Lindblom och Claudia Olsson

Grafisk produktion: Klas Håkansson, Entreprenörskapsforum

Omslagsfoto: IStockphoto

Tryck: Örebro universitet

Förord

Näringspolitiskt forum är Entreprenörskapsforums mötesplats med fokus på förutsättningar för entreprenörskap i Sverige, näringslivets utveckling och innovationsförmåga samt för svensk ekonomis långsiktigt uthålliga tillväxt. Ambitionen är att föra fram policyrelevant forskning till beslutsfattare inom såväl politiken som inom privat och offentlig sektor. De rapporter som presenteras och de rekommendationer som förs fram inom ramen för Näringspolitiskt forum ska vara förankrade i vetenskaplig forskning. Förhoppningen är att rapporterna också ska initiera och bidra till en allmän diskussion och debatt kring de frågor som analyseras.

Blockkedjetekniken har vuxit fram de senaste sju åren genom en kombination av utvecklingen av internet, stark kryptering, öppen källkod och peer-to-peer-fildelningsteknik. Tekniken möjliggör delning av information, tillgångar och värden mellan valfria parter globalt utan mellanhänder eller centrala aktörer. Genom blockkedjan kan handel, kommunikation, ingående av kontrakt och permanent tidsstämplad registrering av information på sikt komma att göras i stor skala utan behov av anförtrödda tredjeparter. Vi vet inte vart denna teknik kommer att föra oss men det är hög tid att diskutera dess utmaningar och möjligheter.

I rapporten *Blockchain – Decentralized Trust* belyses blockkedjeteknikens funktion, utveckling och genomslag, samt möjliga tillämpningar inom näringsliv och samhälle. Författarna framhäver att en bättre förståelse för blockkedjetekniken kan potentiellt vara mycket viktig för ett konkurrenskraftigt näringsliv som tar vara på de senaste tekniska framstegen och kan hantera dess utmaningar. I rapporten undersöks även tänkbara samhällsliga konsekvenser av en utbredd framtida användning av blockkedjeteknik. Bland rekommendationerna lyfts att ett ökat fokus på forskning, utveckling och utbildning inom blockkedjeteknik på sikt skulle kunna bidra till bättre organiserade samhällsfunktioner, mer kostnadseffektiva transaktioner, bättre skyddad data och ett innovativt företagsklimat.

Rapporten är författad av David Bauman, entreprenör med mångårig erfarenhet av blockkedjan, Pontus Lindblom, disputerad forskare Linköping universitet och Claudia Olsson, vd och grundare Exponential Holding samt Associate Faculty Singularity University. Den analys samt de slutsatser och förslag som presenteras i rapporten delas inte nödvändigtvis av Entreprenörskapsforum, författarna svarar själva för dessa.

Stockholm i oktober 2016

Johan Eklund

Vd Entreprenörskapsforum och professor JIBS

Table of Contents

Förord	3
Vocabulary and Definitions	7
Sammanfattning	9
Executive Summary	15
Introduction	19
1. What is Blockchain Technology?	21
1.1 Applications of Blockchains	21
1.2 Bitcoin and Altcoins	23
1.3 Public versus Private Blockchains	26
2. The History and Technology of Blockchain	27
2.1 Historical Context	27
2.2 How Blockchain Technology Developed	29
2.3 Forking and Decision Making	30
2.4 How Blockchain Technology Works	30
2.5 The Consensus Algorithm	34
2.6 Layers on top of Blockchain	35
3. The Global Blockchain Ecosystem	37
3.1 Geographical Distribution	38
3.2 Companies and Organizations	41
3.3 Banks and Financial Institutions	44
3.4 Research and Education	48
4. Blockchain Developments in Sweden	51
4.1 Companies and Organizations	51
4.2 Banks and Financial Institutions	54
4.3 Research and Education	55
5. Regulatory Barriers and Opportunities	57
5.1 Criminal Uses of Cryptocurrency	57
5.2 The Complexity of Blockchain Regulation	59
5.3 Regulating the Anonymity of Cryptocurrencies	59
5.4 Transparency and Accountability	60
5.5 Blockchain Regulations to Date	62
6. Political and Economical implications	67
6.1 Lowered Transaction Cost	67
6.2 Transparency in Society	68
6.3 Evolving Governance Systems	71
6.4 The Impact on National Currencies	73
6.5 Challenges and Risks with Blockchain-Based Systems	76
7. Future Scenarios	79
7.1 Digitized Public Sector Scenario	80
7.2 The Hive Scenario	84
7.3 The Cooter Scenario	86
7.4 Reflections Concerning Future Scenarios	87
8. Policy Measures to Spur Further Innovation	91
9. Conclusions	93
Om författarna	95
Acknowledgements	95
References	97
Appendix one: Further Resources	109

Vocabulary and Definitions

Altcoin	All modified or unmodified clones of the Bitcoin concept.
Antifragility	A property of systems that gain in strength, resilience, and robustness in response to attacks, shock, stress, and failures.
API	Application Programming Interface. A set of functions, tools, and other means to interact with or build solutions within a system.
Asymmetric Encryption	Public-key cryptography. Cryptographic algorithms where pairs of encryption keys are used, usually one public and one private. A public key can be used both to authenticate signatures made with the corresponding private key and to encrypt data, which is only possible to decrypt using the private key.
Bitcoin	Bitcoin, with an uppercase B, is the name of a cryptocurrency, a payment network, a protocol, and its open source community. Units of the currency are referred to as bitcoin, with a lowercase b.
Blockchain	A blockchain is essentially a database, where information is chronologically stored in a continuously growing chain of data blocks, implemented in a decentralized network in a way that creates data integrity, trust, and security for the nodes, without the need for central authorities or intermediators.
Content Management System (CMS)	A system that provides a higher abstraction layer when generating digital content, for instance, by jointly collecting multiple languages, protocols, and image-handling techniques into a common user interface.
Cryptocurrency	Internal virtual currency of a blockchain. Bitcoin and Altcoins.
Cryptography	Etymologically, "hidden information" from Greek <i>kryptos</i> "hidden" and <i>graphia</i> "description of." Techniques and algorithms for securely encoding information to prevent adversaries from getting access to it.
Cypherpunk	An active movement of activists advocating the use of cryptography and privacy-enhancing technologies to defend personal privacy and the idea of an open society in the digital world. Not to be confused with Cyberpunk, which is a science fiction subgenre.
DAO	Decentralized autonomous organization. An organization being run completely algorithmically, using smart contracts distributed on a blockchain.
Distributed	Code executing in parallel and spread out in multiple locations. Not running on one single computer, node, or place.
Forking	In software development, a fork is when a copy of the source code is made to start a separate independent path of development. It is also used to refer to the branching of a blockchain into two or more chains.
Hash	A hash function is an algorithm that can map data of arbitrary size to data of fixed size, called the hash. Cryptographic hash functions are used for checksums and fingerprints of files by mapping them to an easily verifiable fixed-size string of bits.
Hashrate	Processing power in terms of hashes computed per second.
Mining	In Bitcoin, the process of verifying and adding transactions to the ever-growing distributed ledger. Miners lend processing capacity to the Bitcoin network for producing proof-of-work and get paid in bitcoins through block awards and transaction fees.

Peer-to-Peer	A peer-to-peer (P2P) network is a non-hierarchical computer network in which nodes do not have specific roles or privileges in the communication; all nodes can act in any role, as opposed to traditional server and client role-based computer communication.
Point-to-Point	A direct link between two endpoints in network topology.
Proof-of-Work	A string of data bits that is the solution to an algorithmic puzzle implemented as a CPU cost function. It is simple to verify and requires computational resources to produce. In blockchains, proof-of-work cryptographic hash algorithms are often used as consensus algorithms, where anyone can verify that the combined computing power of the whole network was used to build on the data chain.
Satoshi	Satoshi is the first name of the pseudonym Satoshi Nakamoto, used by the founder(s) of Bitcoin and inventor(s) of blockchain. Written without capitalization, satoshi is the actual unit token of the Bitcoin currency. One bitcoin is one hundred million satoshi. As of June 2016, one EUR cent is approximately 1,700 satoshi, and one USD cent is approximately 1,500 satoshi.
Satoshi Nakamoto	Pseudonym used by the person or group that invented the blockchain and cryptocurrency and later assisted in creating Bitcoin.
SHA-256	Cryptographic hash algorithm used in Bitcoin, for instance. Subset of SHA-2 family of secure hash algorithms developed by the NSA.
Smart Contract	In the context of blockchain technology, it involves running distributed computer code in a blockchain network. It was initiated as a feature to do scripted transactions but evolved into more advanced ways of distributing discretionary code.
SMTP	Simple Mail Transfer Protocol. The Internet standard protocol for e-mail.
TCP/IP	Transmission Control Protocol/Internet Protocol. The architecture and collection of protocols for network communication. Used on the Internet, for instance, to provide the IP-addresses used in communication.
Token	In the case of blockchains, another word for blockchain native assets, which can be used to digitally represent any asset including currency.
Turing Machine	Computer. Historically, a model of an abstract general computer, invented by Alan Turing in 1936. ¹ Alan Turing is often considered the father of computer science and artificial intelligence. The original automatic machine model was more limited than computers of today; nowadays, the term Turing machine is often used interchangeably with a general computer.

1. Hodges, A. (2012, November 30). Alan Turing: the enigma. Random House.

Sammanfattning

Den accelererande tekniska utvecklingen ställer höga krav på företag och institutioner att hålla sig uppdaterade om nya teknikers potential och genomslagskraft. En teknik som får allt mer uppmärksamhet av såväl företagsledare som politiska beslutsfattare är blockkedjetekniken. Denna har vuxit närmast exponentiellt de senaste åren och har inspirerat och i vissa fall även tvingat finansiella institutioner och regeringar över hela världen att reagera. Hittills har detta främst berott på att den utgör navet i decentraliserade digitala valutor men de möjliga framtida tillämpningsområdena är betydligt mer omfattande.

Vad är blockkedjeteknik?

Blockkedjetekniken lanserades tillsammans med idén om kryptovalutan Bitcoin genom en artikel i november 2008 undertecknad Satoshi Nakamoto, en pseudonym vars verkliga identitet som person eller grupp är okänd. De olika komponenter som krävts för att skapa blockkedjetekniken har dock vuxit fram successivt med början i internets utveckling på 60-talet, stark kryptering på 70-talet, öppen källkod-rörelsen på 80-talet och peer-to-peer-fildelningstekniken som kom runt millennieskiftet. Bitcoin skapades som en produkt ur Cyberphunk rörelsen som växte fram under 90-talet, en aktiviströrelse som förepräkar användning av stark krypteringsteknik och integritetsfrämjande teknologier för att möjliggöra en fri och öppen värld i den digitala tidsåldern. Bitcoin-blockkedjan är i grunden ett nätverksprotokoll för skapandet av en transparent databas som är öppen för alla, där transaktioner och information registreras permanent och irreversibelt i en tidsstämplad kedja av datablock. Bitcoin-blockkedjan har en inbyggd incitamentsstruktur via en intern valuta som belönar dem som hjälper till att upprätthålla den decentraliserade databasen. Blockkedjan kan betraktas som en fullständig reskontra över alla transaktioner i valutans historia där de enskilda datablocken innehåller samtliga transaktioner och all information som lagts till under de senaste tio minuterna (i genomsnitt) sedan föregående block. Mjukvaran består helt av öppen källkod och kan kopieras och modifieras för användning i andra blockkedjor.

Blockkedjetekniken har möjliggjort digitala decentraliserade valutor som kan utgöra ett globalt komplement till dagens nationella valutor, men erbjuder samtidigt en plattform för byggande av andra decentraliserade applikationer. Dessa möjliggör för människor och maskiner att kommunicera med varandra, utbyta varor och tjänster,

och ingå kontrakt med varandra utan behov av mellanhänder. Nya applikationsområden utvecklas ständigt och ekosystemet runt blockkedjetekniken är ett kraftigt växande globalt fenomen.

Blockkedjeteknik internationellt idag

Ekosystemet kring blockkedjeteknik är idag en snabbt växande och mångsidig global rörelse som inkluderar mjukvaruutvecklare, företag, organisationer, privata användare, företagsanvändare, investerare, forskare, entusiaster och utbildare. Under de sju år som blockkedjetekniken existerat har den utvecklats från att vara ett kommunikationsprotokoll med en intern valuta utan marknadsvärde, till ett komplext ekosystem där exempelvis Bitcoin har ett marknadsvärde på ca tio miljarder USD (5 sep 2016). Tekniken stöds av ett globalt ekosystem av företag som erhållit över en miljard USD i riskkapital hittills och det sker en ständig utveckling av de kommunikationsprotokoll med öppen källkod som tekniken bygger på, och nya versioner och funktioner utvecklas ständigt. Över 100 000 företag accepterar idag Bitcoin som betalningsmedel, varav Microsoft, Dell, WordPress, Expedia och Overstock.com kan nämnas som några av de största. Antalet regelbundna användare uppskattas till närmare tio miljoner och ca 250 000 transaktioner utförs per dag.

Intresset hos samhällsaktörer växer och regeringar och etablerade finansiella aktörer har tagit tydliga steg mot att öka sin förståelse för blockkedjeteknik och hur de kan använda dess egenskaper. Över 40 av de största globala bankerna med en samlad omsättning på över 600 miljarder USD, där svenska SEB och Nordea deltar har format ett partnerskap för att utveckla samarbeten kring blockkedjeteknik.

Blockkedjetekniken har potential att ge omedelbara värdeöverföringar, kryptografiskt säkrade transaktioner med full spårbarhet, permanent registrering av information, förenklad redovisning, selektivt integritetsskydd samt automatisering av affärsfunktioner och automatisk avstämning av information mellan alla inblandade parter. I en rapport av Världsekonomiskt forum där 800 experter inom informations- och kommunikationsteknologi tillfrågades, förväntade sig en majoritet att motsvarande tio procent av världens BNP kommer att finnas lagrad med blockkedjetekniken 2025. Intresset från forskarvärlden växer också stadigt och över 600 artiklar och avhandlingar om blockkedjetekniken har publicerats, hittills fördelat på ämnena; ekonomi (25%), datavetenskap (23%), kryptografi och datasäkerhet (17%), juridik (15%), finans (10%), sociologi (8%), miljö (1%) och politik (1%). Flera universitet i världen erbjuder idag kurser om blockkedjeteknik och MIT lanserade ett särskilt initiativ fokuserat på blockkedjeteknik i april 2015. Denna utveckling verkar bara vara början på ett teknologiskt skifte som kan påverka stora delar av samhället.

Blockkedjeteknik i Sverige idag

Sverige ligger på fjärde plats globalt, efter USA, Nederländerna och Storbritannien vad gäller offentliga riskkapitalinvesteringar i företag som fokuserar på blockkedjeteknik.

Svenska blockkedjeföretag inkluderar KnC Miner som utvecklat och driver mining-utrustning för Bitcoin (efter att bolagets moderbolag KnC Group lämnat in konkursansökan i maj 2016 har verksamheten köpts ut från konkursboet för att drivas vidare av bolaget GoGreenLight, med kopplingar till Uppsalaföretaget Borderlight), Safello som driver verksamhet för växling och betaltjänster i över 30 länder samt blockkedjeteknikföretagen StrawPay och ChromaWay. Sverige var i maj 2015 det första landet i världen som fick ett börshandlat certifikat vilket gjorde det möjligt att exponera sig för Bitcoin-priset på Stockholmsbörsen. Flera av Sveriges största banker arbetar aktivt med att implementera blockkedjeteknik och även statliga myndigheter har visat intresse, exempelvis i juni 2016 då en blockkedjebaserad lösning för landregistrering (utvecklad av ChromaWay i samarbete med Lantmäteriet) annonserades.

Regulatoriska hinder och möjligheter

Med utvecklingen av blockkedjetekniken har frågor väckts om användningen av systemet för illegal verksamhet. Brottsbekämpande myndigheter har uppmärksammat att Bitcoin används för olaglig handel med varor och tjänster, särskilt droger. Kryptovalutor kan potentiellt möjliggöra anonyma transaktioner utanför det traditionella finansiella systemet, vilket väcker oro för att myndigheterna skulle förlora kontrollen över gränsöverskridande betalningar och att olaglig verksamhet skulle kunna bli svårare att spåra. Eftersom alla Bitcoin-transaktioner lagras offentligt och permanent på blockkedjan så är de mindre anonyma än kontanter, och öppna för nätverkstekniska analyser. För ändamål där sändare och mottagare är kända, kan blockkedjetransaktioner bidra till ökad öppenhet och tillförlitlighet. Då transaktioner i Bitcoin är irreversibla finns det heller ingen mellanhand som kan hantera konflikter i betalningar. En teknisk lösning på detta finns dock inbyggt i Bitcoin och andra blockkedjor som möjliggör transaktioner där parterna kan använda sig av en valfri gemensamt pålitlig tredje part som mellanhand eller medlare vid behov.

Då blockkedjor och dess tillämpningar är i en inledande fas, står det ännu inte klart vilka typer av regleringar som kommer att behövas och för vilka syften. De stora befintliga implementationerna utgörs av kryptovalutor, främst Bitcoin. Därmed har de flesta nuvarande regleringarna sin utgångspunkt i just kryptovalutor. Aktuella frågeställningar handlar om hur kryptovalutor ska hanteras och regleras som tillgångar. Avsaknad av centrala aktörer och andra grundläggande skillnader har gjort det svårt att reglera dem på samma sätt som traditionella valutor. Beroende på om de betraktas som t ex egendom, råvara, värdepapper eller betalningsmedel medför det olika konsekvenser för exempelvis skattemässig hantering samt olika trösklar för aktörer att rent praktiskt nyttja teknikens fördelar.

Myndigheter har hittills hanterat frågan om reglering på olika vis. Särskilt när det gäller monetära transaktioner har lagstiftare börjat stifta både reaktiva och proaktiva lagar. Som exempel, har delstaten New York valt att implementera en särskild licensiering av verksamhet med kryptovalutor, och länder som Kanada och Hong Kong har valt att reglera blockkedjevalutor så lite som möjligt för att inte hindra innovation och

nyföretagande. Bolivia, Ecuador, Bangladesh och Island har uttalat att Bitcoin är olagligt att använda för deras invånare, framförallt för att de har lagar för upprätthållande av kapitalkontroller. Som svar på en prövning initierad av svenska Skatteverket tog EU-domstolen i oktober 2015 beslutet att Bitcoin inte är momspliktigt, vilket ger det legal status i paritet med andra betalningsmedel. Fortsatt utveckling inom lagstiftning rörande blockkedjetekniken är att vänta i takt med att antalet användare växer.

Politiska och samhällsekonomiska implikationer

Blockkedjetekniken har potential att förenkla och optimera kommunikation, transaktioner, kontrakt och organisationsstrukturer i samhället genom att avskaffa behovet av mellanhänder och central infrastruktur. Finansiella transaktioner kan potentiellt göras säkrare, snabbare och billigare vilket kan få stor samhällsekonomisk betydelse. Transaktioner i publika blockkedjor, så som Bitcoin, kan inte stoppas eller censureras av enskilda aktörer, vilket potentiellt kan bidra till ökad ekonomisk autonomi för individer och organisationer på global skala. Men det kan även innebära utmaningar för reglerande organ som kan förlora viss möjlighet till ekonomisk och social styrning.

Decentraliserad lagring av data genom blockkedjeteknik har potential att göra hantering av stora mängder data och stora register betydligt säkrare än dagens centraliserade lösningar, som är sårbara för både internt missbruk och utomstående hackare. Politiska val utan risk för valfusk skulle kunna bli en möjlighet samt datorer som gör precis vad de instrueras att göra utan att någon har möjlighet att stoppa eller modifiera ett kommando. Detta kan t ex innebära att hackare inte kan ta över en dator eller en server för sina egna syften på teknisk väg. Samtidigt innebär denna automation även risker, t ex i de fall där själva indatan är fel eller korrupt eller där parter önskar återkalla transaktioner.

Blockkedjetekniken har potential att påverka en mängd olika branscher, men är fortfarande i ett tidigt skede och det är möjligt att infrastrukturen, internet-protokollet, kan bli en del av ryggraden i befintliga eller nya IT-system. Blockkedjetekniken möjliggör ett decentraliserat transaktions- och datalagringssystem som i framtiden skulle kunna användas av miljarder av aktörer på en global nivå. Tekniken undanröjer behovet av betrodda mellanhänder, liksom behovet av att lita på motparter i ekonomiska transaktioner. Blockkedjetekniken representerar ett datavetenskapligt genombrott som möjliggör ett robust decentraliserat globalt system för verifiering av faktiska transaktioner som är öppet för alla att använda och kontrollerbart av alla i realtid. Om utvecklingen av blockkedjetekniken följer det mönster vi sett med andra internetprotokoll så kommer den sannolikt ha stor påverkan på samhälle och näringsliv.

Policyrekommendationer och politiska överväganden

Då blockkedjetekniken är i ett tidigt stadium är det svårt att förutse för vilka områden som nya eller förändrade regleringar blir mest aktuella. Viktigt är att nya regleringar inte hindrar innovativa lösningar som kan ligga till grund för effektivisering av företag

och samhällsfunktioner, men att de samtidigt förmår hantera riskerna med exempelvis illegal handel av varor och tjänster. Beslutsfattare bör noggrant följa utvecklingen runt blockkedjeteknik och om möjligt upplåta testbäddar, infrastruktur och data för experimenterande med tekniken. En viktig insats är även att stödja universitet, skolor och forskningscentra som vill utforska teknikens möjligheter och potentiella tillämpningsområden.

Executive Summary

The accelerating pace of technological development places high demands on companies and institutions to stay abreast of new technologies and their potential impact. One of the technologies that has become of significant interest to business leaders and policy makers is blockchain technology. Its uptake has been nearly exponential in recent years, and it has inspired – and in some cases even forced – financial institutions and governments all over the world to react. Until now, this has primarily depended on its linchpin status for decentralized digital currencies, but there are many other potential future applications.

What is Blockchain Technology?

The technology was launched with the idea of the cryptocurrency Bitcoin in a November 2008 paper signed by Satoshi Nakamoto, a pseudonym for a person or group, that to date remains unidentified. The components required to create blockchain technology have evolved gradually, beginning with the development of the Internet in the '60s, strong encryption in the '70s, the open source movement in the '80s, and peer-to-peer file-sharing technology around the millennium shift. Bitcoin was created as a product of the cypherpunk movement that emerged in the '90s, an activist movement that advocates the use of strong encryption technology and privacy-enhancing technologies to enable a free and open world in the digital age. At its core, the Bitcoin blockchain is an Internet network protocol for the creation of a decentralized, transparent database that is open for anyone to use, where transactions and information can be recorded permanently and irreversibly in a time-stamped chain of data blocks. The Bitcoin blockchain has an incentive structure in the form of an internal currency, which rewards those who help maintain the decentralized database. The software is entirely open source and can be copied and modified for use in other blockchains.

Blockchain technology has enabled decentralized digital currencies that can serve as a global complement to regular national currencies, while also enabling applications that allow people and machines to communicate with each other, exchange goods and services, and enter into contracts without the need for intermediaries. New application areas are continuously being developed, and the blockchain ecosystem today is a rapidly growing, diverse global movement.

The Global Blockchain Ecosystem

The ecosystem around the technology comprises software developers, companies, organizations, private users, business users, investors, researchers, enthusiasts, and educators. In the 7 years that blockchain technology has existed, Bitcoin has evolved from a communication protocol with an internal currency that had no market value to a system with a market value of about 10 billion USD (Sep 6, 2016). The technology is currently supported by a global ecosystem of companies that have raised more than 1 billion USD in venture capital funding, and the open source protocols that the technology is based on are constantly developing.

Global blockchain activity is increasing fast, and the diversity of actors applying the technology and exploring possible new blockchain based business models is growing. Over 100,000 companies have started accepting Bitcoin as payment; the number of Bitcoin users is estimated at nearly 10 million, and about 250,000 transactions take place on the network each day. The interest from governments and established financial institutions is growing. Over 40 of the largest banks in the world, with a combined market capitalization of more than 600 billion USD, have formed a consortium to explore and implement blockchain technology. The blockchain infrastructure has the potential for instant value transfer and settlement, cryptographically secured transactions with full provenance and chain of custody, immutability, perfect auditability, selective privacy, business automation through smart contracts, and automatic reconciliation of information between all parties involved. The World Economic Forum issued a report after surveying 800 experts in information and communication technology; a majority of the respondents expected that the equivalent of 10% of the global GDP will be stored on blockchains by 2025. So far, over 600 academic papers on blockchain technology have been published worldwide, and several universities offer courses on this new technology. These developments seem to only be the beginning of a technological shift that could affect a variety of industries.

The Blockchain Ecosystem in Sweden

Sweden is in fourth place worldwide, after the United States, the Netherlands and the United Kingdom in terms of publicly disclosed venture capital investments in companies focusing on blockchain technology. Swedish blockchain enterprises include KnC Miner, which develops and runs Bitcoin-mining hardware; its former sister company XBT Provider, which has listed Bitcoin exchange-traded notes on Nasdaq (the mother company KnC Group filed for bankruptcy in May 2016; KnC Miner has been bought by the new company GoGreenLight, sharing founders with an older Swedish IT and Telecom firm Borderlight, and XBT Provider was acquired by Jersey based Global Advisors Ltd); Safello, which handles exchange and payment services in over 30 countries; and the blockchain technology companies StrawPay and ChromaWay, which have significant international reach. Sweden was the first country in the world, in May 2015, to have a Bitcoin tracking exchange-traded note launched on the Nasdaq Stockholm. Several of the largest banks in Sweden are working actively on implementing blockchain

solutions. The government has also shown some interest, as a blockchain solution for land registration was announced in June 2016 by ChromaWay in partnership with the Swedish National Land Survey (Lantmäteriet).

Regulatory Barriers and Opportunities

With the development of blockchain technology, questions have been raised concerning use of the system for criminal activities. Law enforcement agencies have noticed that Bitcoin has been adopted for illicit trade of products and services, especially drugs. Cryptocurrencies can potentially allow anonymous value transactions outside the traditional financial system, which raises the concern that authorities might lose control of cross-border payments and that illegal activities might become more difficult to track. However, as all Bitcoin transactions are stored publicly and permanently on the blockchain, they are less anonymous than cash and open to data forensics. For situations in which the sender and receiver are known, the traceability of the transactions can contribute to greater transparency and accountability. As Bitcoin transactions are irreversible, there is also no intermediate payment processor that can handle disputes. A technical solution to this is available in Bitcoin and other blockchains using escrow transactions that can protect both senders and receivers to some extent.

As blockchain and its applications are in an initial phase, it is not yet clear what kinds of regulations will be needed and for what purposes. The major existing implementations consist of cryptocurrencies, primarily Bitcoin. Thus, most current regulations are based on cryptocurrencies. The current issues concern how cryptocurrencies should be managed and regulated as assets. The absence of central entities and other fundamental differences have made it difficult to control them in the same way as traditional currencies. Depending on whether they are considered property, commodity, security, or currency, different consequences for taxes and other regulations must be taken into account for different use cases.

Various authorities are handling the issue of regulation differently. Particularly in the case of monetary transactions, legislators have started to form both reactive and proactive legislation. For example, the State of New York has chosen to deploy a separate licensing scheme for businesses handling cryptocurrencies, and countries such as Canada and Hong Kong have called for a regulatory light touch to avoid stifling the development of blockchain technology at its early stages within their jurisdictions. Bolivia, Ecuador, Bangladesh, and Iceland have stated that the use of Bitcoin as a currency is illegal for its citizens, primarily because they have laws in place to enforce capital controls. In response to an investigation initiated by the Swedish Tax Agency, the EU Court of Justice ruled in October 2015 that Bitcoin is not subject to VAT, giving it legal status on a par with other means of payment for European Union (EU) citizens. Further developments in legislation are to be expected to meet the growing number of users of blockchain networks.

Political and Economical Implications

Blockchain technology has the potential to simplify and optimize communications, transactions, contracts, and organizational structures by eliminating the need for intermediaries and central infrastructures. Financial transactions can potentially be made safer, faster, and cheaper, with a significant potential impact on society. Transactions in permissionless public blockchains, such as Bitcoin, cannot be stopped or censored by any single actor, which could potentially spur a greater economic autonomy for individuals and organizations on a global level. However, it could also pose challenges for regulating bodies and policy makers, who may lose some economic and social influence.

Decentralized data storage using blockchains holds the promise of making the management of large amounts of data and large registers safer than present-day centralized solutions that are vulnerable both to internal abuse and external hackers. This new technology could enable new areas of interest, such as elections that are impervious to electoral fraud and decentralized, failsafe computing. This could mean that hackers could not take over a computer or a server for their own purposes by technical means. At the same time, this automation also has risks, for example, in cases where the input data is incorrect or corrupt or where the parties wish to recall transactions.

Blockchain technology has the potential to impact a variety of industries but is still at an early stage, and it is possible that the infrastructure – the Internet protocol – might become part of the backbone of existing or new IT systems. Blockchain technology enables a decentralized transaction and data storage system that eventually could be used by billions of actors on a global level. The technology obviates the need for trusted intermediaries as well as the need to trust counterparties in economic transactions. Blockchain represents a breakthrough in computer science that enables a robust, decentralized global system of verification of actual transactions that is open to everyone and auditable by anyone in real time. If it continues to evolve similarly to the progress that has been witnessed for other Internet protocols, it will most likely be highly impactful for businesses and society.

Policy Recommendations and Political Considerations

As blockchain technology is at an early stage, it is difficult to predict in which areas new or changed regulations will be needed. It is important that new regulations do not prevent innovative solutions that can be the basis for improving the efficiency of business and social functions, but at the same time manages the risks of, for example, the illegal trade of goods and services. Decision makers should closely monitor the developments around blockchain technology and, if possible, promote test beds, infrastructures, and data for experimentation. An important contribution that policy makers can make is to support universities, schools, and research centers that wish to explore the possibilities and potential areas of blockchain applications.

Introduction

Blockchain technology emerged as a convergence of the developments of the Internet, strong encryption, the open source movement, peer-to-peer file-sharing technology, and the activism of the cypherpunk movement. The latter has attempted to create a native digital currency for the Internet since the late '90s. A blockchain can be regarded as a global spreadsheet, or an incorruptible digital ledger, where financial transactions and any data or asset can be represented, shared, and transacted with. Interaction via blockchain, enabled by a global network of consensus, eliminates the need for trusted middlemen between parties exchanging information or value. The infrastructure enables these interactions point-to-point over a trustless network. Smart contracts and future application layers promise to change how data can be transacted, accessed, stored, and secured. Blockchain technology could enable fundamental changes in the way society is organized. With blockchain technology, it is possible to move from organizations with centrally controlled hierarchical structures of interaction and control (by necessity) to decentralized peer-to-peer organizations. In Sweden, the ecosystem around the technology is just starting to develop, and policy makers, business leaders, and entrepreneurs are seeking to understand the potential of the technology and the possible implications for different societal functions and industries.

The aim of this report is to explore what blockchain technology is, what it enables today, and what developments and potential applications blockchain technology could permit going forward. Since the peer-reviewed literature about this new field is limited, we primarily base our study on interviews with key opinion leaders, developers, entrepreneurs, and researchers, as well as on publications both in internationally recognized journals and newspapers and publications and blogs that specialize in the coverage of the blockchain industry. Naturally, we need to be critical about the conclusions presented through these sources, as they often represent the impressions and sometimes desires of the early adopters. Still, they provide an insight into a technology that could benefit society in many ways, if applied for a good cause. Thus, our ambition is that this paper will contribute to the understanding of blockchain technology and spur the interest among potential future stakeholders that might apply the technology for increased efficiency and productivity. References are given as footnotes with a weblink to enable easy, direct access to the source when possible. A complete reference list is available at the end of the report.

INTRODUCTION

The following chapters explore what blockchain technology is, how it is currently being used, regulations concerning the technology, implications, and its future potential. We also present broader conclusions and recommendations to policy makers and business leaders for how to harness the potential of this relatively new, but fast-developing technology.

1. What is Blockchain Technology?

A *blockchain* is essentially a database, where information is chronologically stored in a continuously growing chain of data blocks, implemented in a decentralized network in a way that creates data integrity, trust, and security for the nodes, without the need of central authorities or intermediators. In its most tangible form, it is computer code that tells each computer in which it is implemented to store data locally. It is also part of a global network with thousands of other computers, also storing data with the same (compliant) programming code.

The above definition of blockchain is a bit broader than usually found. Most definitions refer to Bitcoin or other cryptocurrencies, since blockchain technology was invented as the mechanism making Bitcoin possible. In the case of Bitcoin and other blockchain-based cryptocurrencies, the data blocks contain transactions. As such, the Bitcoin blockchain is a globally distributed and public ledger of all the Bitcoin transactions ever made, containing complete information on all addresses and balances at each point in time in the history of the Bitcoin network.

Since transactions and internal cryptocurrencies are cornerstones in most blockchain implementations today, these features are often included in general blockchain definitions. It is worth noting that it may be possible to implement different kinds of blockchains in the future, with datasets other than those for transactions and without internal currency. For the purpose of this report, a broader definition has therefore been chosen to include future possible implementations as well.

1.1 Applications of Blockchains

Internal tokens in blockchains can be used for many different types of digital assets, such as financial instruments, licenses, certificates, tickets, digital keys, and public and private records (e.g., identity documentation, birth certificates, and medical records). Blockchains could also be used for control and ownership of physical assets if such solutions would be given legal status as authoritative registers for physical properties.

Proof of existence is a very useful function enabled by blockchain technology, as it can provide permanent verifiable documentation.² Since all registered transactions – with included metadata – on the Bitcoin blockchain are time-stamped and immutable, it can be used to prove that a certain document (text, picture, audio, or video) existed at a particular point in time. To do this, a cryptographic fingerprint digest (a hash) that can uniquely identify the document is embedded as metadata in a transaction. To prove at a later time that a document is the same document fingerprinted at a certain point in time on the blockchain, the hash needs to match. If it does not match, it is not the same document. This can be used to prevent falsification of historical events and enable verifiably accurate accounting records of different processes. It can be used for immutable tracking of authenticity and provenance of both digital and physical products, which could revolutionize supply chain management, regulatory oversight, and intellectual property management.

Blockchain-based cryptocurrencies also support more advanced transactions, such as multiple signature transactions and scripted transactions. This enables smart contracts. These are contracts recorded on the blockchain that are executed automatically when the conditions of the contract are met. The execution of a smart contract results in the transfer of digital assets on the blockchain to the parties in the contract. By signing contracts directly into a public blockchain, which no single party controls and thus all parties can rely on, the human counterparty risk is eliminated. The terms of the contract are automatically enforced through the blockchain, instead of through traditional institutions and legal systems.

Smart property is a term used for any property, digital or physical, where ownership is controlled via a blockchain.³ This makes it possible to prove ownership, transfer ownership of a property, and control its use through smart contracts, without the need to trust any counterparty. It can reduce fraud and mediation fees and allow trades that otherwise would never happen.

Through blockchain technology, it becomes easy to grant granular token-controlled access to different resources, both digital and physical. Token is an alternative name for a native digital asset on a blockchain, which can be used to represent many other things beside currency. In this use case, a specific token on a blockchain, or a given combination of tokens, could be used to control different levels of access. Thus, the information and resources that can be accessed could depend on the tokens that a specific user holds. A simple illustration of this could be that people who access a webpage are presented with different information depending on what tokens they have in their blockchain wallet. This specific use case can also be called a token-controlled viewpoint.⁴

Blockchain technology enables trustworthy computing, where the execution of a computer program does not depend on a central point of control through a single computer that

2. <https://bitscan.com/articles/how-to-establish-proof-of-existence-on-the-bitcoin-blockchain>

3. http://cointelegraph.com/news/understanding_smart_property

4. <https://letstalkbitcoin.com/blog/post/tcv>

could be corrupted or controlled.⁵ The second most popular public blockchain, Ethereum, is specifically designed to enable Turing-complete smart contracts, meaning that a set of contracts on the blockchain can be programmed to do everything that a generalized computer can do. This means that the Ethereum blockchain enables computer programs to be executed on a decentralized virtual computer in the form of the Ethereum network, distributed across many traditional computers, protected by cryptography and consensus technology.⁶ This computing environment becomes as secure and reliable as the blockchain it is based on, with no single points of control or corruption.

Blockchain technology could offer a solution for secure online voting.⁷ Traditional voting with paper forms and manual counting is vulnerable to electoral fraud. However, computerized voting systems are even more vulnerable because it is not possible to guarantee the integrity of the computers in the system. Blockchain technology can solve this through its decentralized consensus system, which would be nearly impossible to manipulate. Votes could be cast anonymously, making it possible for each voter to cryptographically prove that their vote was assigned to the correct candidate in the final result.

Blockchain technology can also enable decentralized autonomous organizations (DAOs).⁸ Through open source software that handles smart contracts, it is possible to create DAOs where humans and machines can organize in a peer-to-peer manner to produce services and products without any central owner that could be controlled or held legally accountable. In the future, it is possible that companies such as Ebay, Airbnb, and Uber could be replaced by DAOs and that customers and sellers could be directly connected through DAOs on a blockchain.

Blockchain technology provides new means for the ways in which many societal functions could be organized, shifting from top-down hierarchical structures with single points of control and failure to decentralized peer-to-peer organizations without single points of control and failure. The peer-to-peer nature of blockchain technology makes it possible for humans and machines to exchange value, communicate, engage in contracts, and organize without intermediaries or third parties involved. In the future, many of the services that are currently provided by centralized organizations could potentially be decentralized and provided at lower cost with fewer bottlenecks in administrative processes.

1.2 Bitcoin and Altcoins

Blockchain technology was introduced to the world through the borderless digital peer-to-peer currency Bitcoin. Bitcoin was described in late 2008 in the paper "*Bitcoin: A Peer-to-Peer Electronic Cash System*" authored by Satoshi Nakamoto (a pseudonym).⁹ The anonymous creator (or creators) of Bitcoin was the first to find a

5. <http://unenumerated.blogspot.com/2014/12/the-dawn-of-trustworthy-computing.html>

6. <https://github.com/ethereum/wiki/wiki/White-Paper>

7. <https://bitcoinmagazine.com/articles/blockchain-technology-key-secure-online-voting-1435443899>

8. <https://github.com/DavidJohnstonCEO/DecentralizedApplications>

9. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. <https://bitcoin.org/bitcoin.pdf>

solution to how double spending could be avoided in a decentralized electronic payment network. This problem had made it impossible to create an electronic currency, without a central trusted third party, as the central party was needed to verify that the digital coins were not copied and used multiple times. Satoshi's solution proposed that all transactions should be publicly published to all participants (nodes) in the network. For all participants to agree on a common history of every transaction, the agreed history or transcript of transactions would be locked cryptographically in an ever-growing chronological chain of data blocks (a blockchain). The technical details of this are further explained in Chapter 2.

At its core, the Bitcoin blockchain is an Internet network protocol for the creation of a decentralized, transparent database that is open for anyone to use, where transactions and information can be recorded permanently and irreversibly in a time-stamped chain of transaction blocks. The Bitcoin blockchain has an incentive structure in the form of an internal currency, which rewards those who help maintain the decentralized database. The software is entirely open source and can be copied and modified for use in other blockchains. The price of Bitcoin is determined solely by supply and demand in what constitutes one of the world's freest global markets. When Bitcoin was first started in early 2009, bitcoins had no market value. Through being given a subjective value at some point in time by a few individuals, perhaps because they thought it had properties that would make others value it in the future, the currency value has grown organically over time together with its user base. Today, the total market capitalization of all bitcoins in existence is about 10 billion USD (Sep 6, 2016).





















An important aspect of Bitcoin is that it is a push-transaction technology, just like physical cash, meaning that the sender performs the transfer. In contrast, credit/debit card payments are a pull-transaction technology, meaning that the receiver performs the transfer. With a credit/debit card, the merchant's payment terminal receives all the secret credentials from the customer's account (the private keys) and then decides how much money it will pull from it. This puts the card owner at risk of losing money if he or she uses the card in a compromised terminal or hands it over to a fraudulent person that copies the secret account credentials. At the same time, merchants are exposed to the risk of accepting card payments from individuals or entities who are not the rightful owners, which often results in chargebacks and loss of money. Merchants can try to protect themselves against fraudulent card payments by requiring personal identification, which some argue could be seen as an invasion of privacy. Card payments can be disputed for 60 days.¹⁰ This means that merchants cannot be sure that they will keep the money until at least 60 days have passed, and if there is a dispute, the merchant has to use valuable time to address the dispute and prove that he or she was not careless when accepting the payment. A 2009 study calculated that in one year in the United States, banks lost 11 billion USD, customers lost 4.8 billion USD,

10. <https://www.consumer.ftc.gov/articles/0219-disputing-credit-card-charges>

and merchants lost 190 billion USD due to credit/debit card fraud.¹¹ Using Bitcoin, the owner of a wallet is in control and never has to expose any secret credentials (private keys) to send a transaction. Compared to physical cash, Bitcoin offers advantages in terms of being impossible to counterfeit and being transferable digitally anywhere in the world within minutes. Bitcoin also minimizes the need for trust, since the parties taking part in a transaction do not require any personal details from each other.

A lot of Bitcoin alternatives have been created, since anyone can easily copy the code, modify it, and start their own Bitcoin clone or similar cryptocurrency. These alternatives, which are cryptocurrencies other than Bitcoin, are often collectively referred to as altcoins.¹² Some altcoins have been started due to disputes around choices made in the Bitcoin community, some have optimized parameters targeting different situations than Bitcoin, and some have explored new or different features and algorithms. Others were started simply for the founders to earn money by being on top of a new pyramid scheme; still others were premised to be distributed targeting a specific demographic, and so on. The list is long. There are over 400 altcoins, with a current market value,¹³ and over 400 altcoins have perished, according to the Coindesk state of Bitcoin 2016 report.¹⁴ The top 10 cryptocurrencies in terms of market capitalization as of September 6, 2016, are shown in Figure 1.

FIGURE 1. Cryptocurrency Market Capitalization, Top 10

▲#	Name	Market Cap	Price	Available Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	 Bitcoin	\$9,680,892,537	\$610.68	15,852,540 BTC	\$74,468,200	1.16%	
2	 Ethereum	\$964,269,639	\$11.52	83,707,595 ETH	\$6,664,910	-2.29%	
3	 Ripple	\$209,322,751	\$0.005927	35,316,813,001 XRP *	\$615,748	0.12%	
4	 Litecoin	\$188,525,975	\$3.97	47,437,704 LTC	\$1,726,750	-0.38%	
5	 Monero	\$165,418,208	\$12.89	12,831,771 XMR	\$26,649,500	-0.65%	
6	 Ethereum Cla...	\$122,382,271	\$1.46	83,673,320 ETC	\$2,700,130	-2.22%	
7	 Steem	\$108,920,422	\$0.805678	135,191,009 STEEM	\$75,907	-0.58%	
8	 Dash	\$74,991,032	\$11.16	6,721,855 DASH	\$567,628	-2.46%	
9	 NEM	\$50,310,180	\$0.005590	8,999,999,999 XEM *	\$141,434	-1.51%	
10	 MaidSafeCoin	\$41,098,864	\$0.090816	452,552,412 MAID *	\$428,359	-0.01%	

Source: <https://coinmarketcap.com/> retrieved September 6, 2016

11. <http://www.forbes.com/sites/haydnshaughnessy/2011/03/24/solving-the-190-billion-annual-fraud-scam-more-on-jumio/>
12. <https://en.bitcoin.it/wiki/Altcoin>
13. <http://coincap.io/>
14. <http://www.coindesk.com/research/state-bitcoin-blockchain-2016/>

1.3 Public versus Private Blockchains

The Bitcoin blockchain sprung from the idea of creating a pure peer-to-peer online electronic cash system.¹⁵ Instead of having to use trusted third parties for establishing a consensus on the chronological order of transactions to prevent double spending, Bitcoin uses computationally difficult cryptographic proofs (proof-of-work) to verify transactions. The use of proof-of-work enables a secure decentralized consensus over a shared transaction history in a public, permissionless, censorship-resistant peer-to-peer network. No trust is needed, since no single entity controls the network. However, during the past few years, the blockchain technology has also been implemented for internal solutions in so-called private, or permissioned, blockchains. Private blockchains are implemented to leverage blockchain technology for a permissioned and controlled environment, for example, in regulated financial markets or for government services.

A consortium of banks or other institutions can choose to create a ledger that is only accessible and distributed within their own chosen network. An example of a permissioned, distributed ledger is Linq, a private blockchain solution developed and implemented in 2015 by Nasdaq for trade with unregistered securities.¹⁶ Inherently, by not being publicly distributed, private blockchains need more traditional measures of infrastructure and security solutions, since they are not provided by a public network. The infrastructure enables more central control that can be applied to the whole or to chosen parts of the implementation.

Private blockchains can be beneficial solutions when several entities are cooperating, for instance, when building on available open source technology for establishing a consensus about facts and processes across entities, without a single entity being able to unilaterally make changes. In various situations with multiple bodies in a trusted network, private blockchain solutions may have advantages over public blockchain solutions. By using a private blockchain solution in a shared network with an agreed upon protocol, benefits such as data integrity, record of history, and consensus will be similar to the benefits gained from public blockchain alternatives. Also, by controlling a consensus algorithm, whereby all participants are already trusted, it could be possible to keep resource usage and energy consumption lower than in the case of a public blockchain.

Private or nonpublic solutions can benefit from applying elements of blockchain technology for internal use. What blockchain enthusiasts question is whether these private implementations should still be considered blockchains.

When the blockchain banking consortium R3 presented their distributed ledger platform (Corda), designed for regulated financial services, their CTO Richard Gendal Brown explained why they decided not to build a blockchain. He stated that Bitcoin is a “wonderfully neat solution” to the business problem of “how do I create a system where nobody can stop me spending my own money?” However, he noted that regulated banks actually have the inverse business problem.¹⁷

15. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. <https://bitcoin.org/bitcoin.pdf>

16. <http://ir.nasdaq.com/releasedetail.cfm?releaseid=948326>

17. <http://r3cev.com/blog/2016/4/4/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services>

2. The History and Technology of Blockchain

This chapter provides an introductory probe into technical specifics and gives a more extensive background as to how blockchain technology evolved. The target audience for this chapter is ordinary readers with a general technical interest and developers looking for an introduction to the concepts. The chapter is not to be seen as a technical reference for developers and does not require engineering background. Some parts and images are simplified, with details and corner cases left out on purpose, to better focus on pedagogical conceptual explanation. Readers that are not interested in a deeper understanding of the underlying technology may continue directly to Chapter 3.

2.1 Historical Context

Technological innovations do not just happen in a vacuum. Instead, they tend to build on many previously invented bits and pieces that are combined in a new way or as well-established methods and techniques applied in a new area. Blockchain technology is no different and builds on a long history of developments in Internet technology, strong encryption techniques, open source development, and peer-to-peer file-sharing technology.

The fundamental aspects of the Internet were invented in the '60s in the form of protocols allowing computers to communicate with each other through a network. This eventually evolved into the decentralized, globally interconnected network of networks, which we today call the Internet. Some important milestones of the standardized communication protocols forming the Internet include the e-mail protocol SMTP and the Internet protocol suite TCP/IP (which both came 1982), the World Wide Web in 1989, and the first version of HTML in 1993.

Until the '70s, encryption was mostly used by military and intelligence organizations, but that trend changed due to the development of computers and the Internet. IBM invented and published a symmetric encryption algorithm called the Data Encryption Standard (DES) in 1975. It was widely adopted after being selected as an official encryption standard in the United States in 1977. In 1976, Whitfield Diffie and Martin

Hellman at MIT published the groundbreaking concept of asymmetric encryption.¹⁸ Instead of sharing a common encryption key, which has to be communicated safely between parties beforehand as in symmetric encryption, asymmetric encryption uses a mathematically connected pair of keys. In the latter case, a private key can be used to decipher messages encrypted with the corresponding public key, which makes it possible to communicate privately and safely without the prior exchange of secret keys. The concept of asymmetric encryption was further developed and optimized in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman,¹⁹ also at MIT, when they described how large prime numbers can be used to generate key pairs in an efficient and secure way. Elliptic curve cryptography (ECC) is a variant of asymmetric encryption that was invented in 1985²⁰ and came in to a wider use around 2004. ECC is the type of cryptography used in Bitcoin and other blockchains to generate secure key pairs for sending, receiving, and storing cryptocurrencies.

Originating in the early '80s, *open source* is the concept of publicly available software code distributed under licenses, making it more or less free to use, read, copy, modify, and distribute. Open source has proven to be a good way of guaranteeing that a computer program is safe and does exactly what it is expected to do. This is because anybody can choose to review the code and contribute to optimizing it, improving it, and fixing bugs and security leaks. Open source code makes it possible for people to collaborate freely and, in a decentralized way, develop open software. The open source operating system, Linux, was launched in 1991 and got further traction through collaborative development and fast-growing use during the '90s. The open source initiative was launched in 1998, and the GIT versioning system established in 2005 further expanded the possibilities of distributed community collaboration.

P2P file-sharing technology was introduced in 1999, and its implementations soon created a large concern for the music industry through services such as Napster (1999) and BitTorrent (2001). In a peer-to-peer network, all computers are equivalent nodes acting both as server and client to each other, which enable the decentralized organization of information sharing, without the need for hierarchies.

The idea of a free virtual and globally distributed world not ruled by governments, national jurisdictions, and industrial companies is not new. Much of the ideology and driving effort in the cyber libertarian community where blockchain was originally invented is the very same ideology as expressed by John Perry Barlow, for instance, 20 years ago.²¹ Already then, the evolution of digital solutions for collective mind and resource sharing were predicted. It was also predicted that these solutions would conflict with more traditional rules based on physical assets, borders, and individualism.

18. Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE transactions on Information Theory*, 22(6), 644-654.

19. Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), 120-126.

20. Miller, V. S. (1985). Use of elliptic curves in cryptography. In *Conference on the Theory and Application of Cryptographic Techniques* (pp. 417-426). Springer Berlin Heidelberg.

21. <https://www.eff.org/cyberspace-independence>

Today, these ideas have evolved into established and growing concepts, such as the sharing economy.

Hal Varian's concept, outlined in his paper entitled "Computer Mediated Transactions" in 2010,²² explains how the Internet and the World Wide Web, through a long history of collective actions, have led to a successively increased pace of combinatorial innovation through collaborative efforts. The innovation of blockchain and cryptocurrencies can be seen as a natural progression in the same ecosystem that led to the development of the Internet.

2.2 How Blockchain Technology Developed

Since the late 1980s, an active movement called Cypherpunks – not to be confused with Cyberpunk – has engaged activists advocating the use of cryptography and privacy-enhancing technologies to defend personal privacy and the idea of an open society in the digital world.²³ On October 31, 2008, a user named Satoshi Nakamoto posted a paper for a decentralized money system named "Bitcoin: A Peer-to-Peer Electronic Cash System"²⁴ to a Cypherpunk email forum at metzdowd.com.²⁵ The technical solution proposed, blockchain, was a combination of previously known solutions, several of which had been proposed earlier in the very same forum. The breakthrough was figuring out how to use economic incentives to secure and bootstrap a decentralized system of digital cash using the previously proposed solutions. For one of the pieces of technology used – proof-of-work (explained more thoroughly in Chapter 2.3) – Satoshi referred to Hashcash,²⁶ for instance, an idea proposed by Adam Back on the Cypherpunk forum in May 1997. In the discussion following Adam Back's proposal, Wei Dai proposed an anonymous distributed electronic cash system in November 1998 named B-money,²⁷ which would make use of the proof-of-work system. Also in 1998, Nick Szabo proposed Bit Gold²⁸ as a reusable proof-of-work concept based on a system very closely related to what we call a blockchain today. Szabo's idea was a distributed linked list of time-stamped strings, each connected by a proof-of-work function, where the owner of each string of Bit Gold could be verified using cryptographic signatures. In the Bitcoin proposal, Satoshi had moved the proof-of-work and transaction verification system in the previously proposed systems into a concept called mining, separated from the actual usage of the payment system, and carried out by actors called miners. This makes the quorum of the blockchain based on the processing capacity of miners instead of a quorum of addresses. Miners in that way

22. <http://people.ischool.berkeley.edu/~hal/Papers/2010/cmt.pdf>

23. <http://www.wired.com/1993/02/crypto-rebels/>

24. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. <https://bitcoin.org/bitcoin.pdf>

25. <https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html>

26. Back, A. (2002). Hashcash-a denial of service counter-measure.

27. <http://www.weidai.com/bmoney.txt>

28. <http://unenumerated.blogspot.co.uk/2005/12/bit-gold.html>

constitute the infrastructure and security of the Bitcoin network and are rewarded for their participation through built-in economic incentives.

The smallest element of the internal currency in the Bitcoin blockchain is called a satoshi, named after its inventor. Satoshis are most commonly measured in units of 100,000,000, called one bitcoin. A coin in the network is defined by a chain of digital signatures, which can be traced back through every transaction to the block in the blockchain where it was created, thus making each coin unique and making digital scarcity possible. Using the network involves generating an asymmetric cryptographic key pair, where the public key is used as an address that can receive funds, and the private key is used for signing transactions. Receiving funds is as easy as someone else making a transaction to the address. Sending funds involves describing a transaction, signing it, and sending it to the Bitcoin network for miners to verify it and include it in a block. Generating addresses is cheap, so new addresses can essentially be generated for every single transaction. In Bitcoin, this process is simplified for users today by the automated collection of addresses and generation of transactions in the most common user applications, called Bitcoin wallets.

In 2009, Satoshi released a first version of the Bitcoin software as open source, which launched the network and created the first tokens of the Bitcoin cryptocurrency. In mid-2010, having collaborated with other developers to improve the code after the initial release, Satoshi handed over all control to the community and discontinued contributing. Since then, community development efforts have continued, the Bitcoin network has been growing, mining capacity has multiplied, and transaction volumes have surged.

2.3 Forking and Decision Making

Since all the software building blocks of the Bitcoin network are open source (available here²⁹), the natural decision-making process in the community is by forking.³⁰ As soon as one branch is used by a majority of the network, the rest will follow swiftly. This allows for a smooth upgrade process most of the time, but it could also, in the event of a contentious (near 50: 50) fork, theoretically cause a split of the currency into two, whereby both branches could live on supported by separate communities of miners. If that would happen, holders of the original cryptocurrency could keep their initial saldo spendable as separate currencies on the separate branches.

2.4 How Blockchain Technology Works

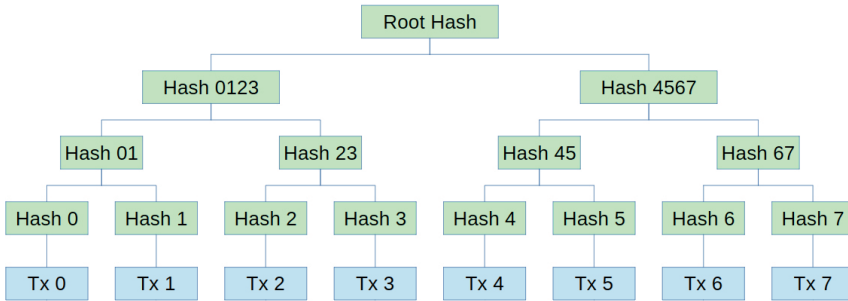
The process of block creation and transaction verification (in Bitcoin, implementing the proof-of-work idea) is called mining. Miners continuously listen to the network, verify,

29. <https://github.com/bitcoin>

30. <https://peterodd.org/2016/soft-forks-are-safer-than-hard-forks>

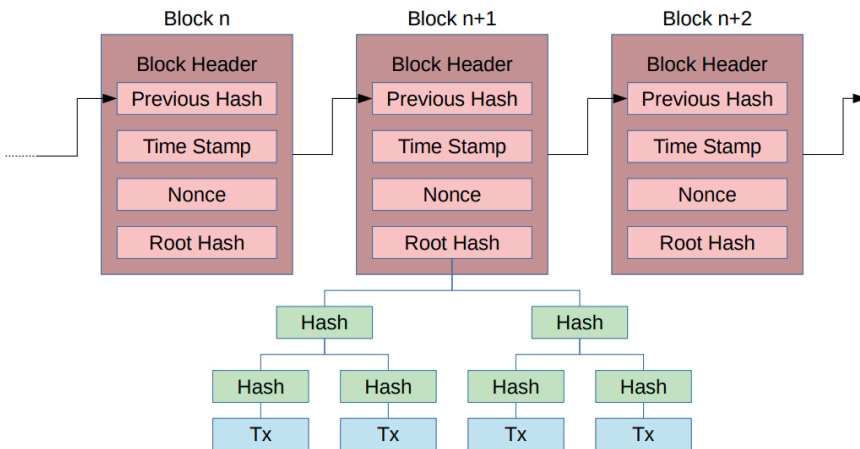
and add transactions to the block currently being worked on. A block is a data block of transactions that are hashed together in a hash tree, producing a hash tree root. The concept is called a Merkle Tree,³¹ named after its inventor Ralph Merkle (Figure 2).

FIGURE 2. Transactions in a Merkle Tree



The cryptographic hash algorithm used in Bitcoin is SHA-256. The processing power of a miner determines its hash rate in terms of how many hashes it can produce per second. Each block in the blockchain contains a root hash of all transactions, a time stamp, a block version number, and a parameter called nonce. These are hashed into a block header together with the block header hash from the previous block, which cryptographically links them together (Figure 3).

FIGURE 3. Blockchain Structure



31. Merkle, R. C. (1987). A digital signature based on a conventional encryption function. Conference on the Theory and Application of Cryptographic Techniques. Springer Berlin Heidelberg.

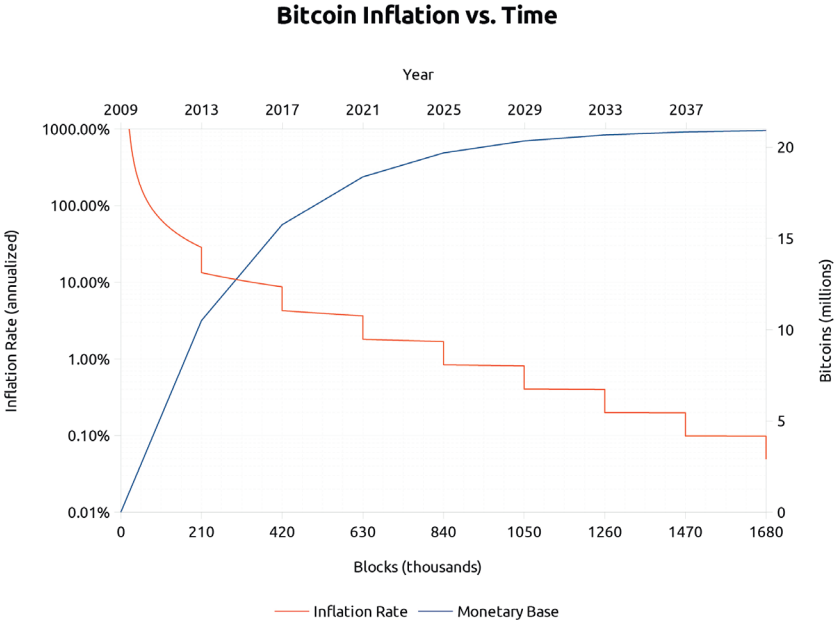
To be found valid, the hash of the block header has to meet a certain criterion, called difficulty. In Bitcoin, difficulty is the number of zeroes expected in the beginning of a valid block header hash. The target difficulty of a block is also present in the block header. Miners calculate their block header hash and check if it meets the difficulty target criterion. If not, the block is modified (usually by incrementing the nonce parameter), and the hash is calculated and checked again – and so on. When a miner finds a block that meets the criterion, it is shared with the rest of the network, verified by other miners, and added to the blockchain.

Miners are always working on the longest chain. Difficulty is adjusted for total processing power (the hash rate) of the network at certain intervals of blocks. Thus, the total hash rate of the network is needed to statistically solve the difficulty criterion to validate a new block every 10 minutes on average. This automatically regulates the pace in which new blocks are created. It also provides security and a quorum of processing power, since any minority in terms of hash rate trying to do something on its own will quickly fall behind. With each new block, on top of all transactions included, an extra special transaction with a certain amount of new bitcoin currency is created – the coinbase transaction. These new bitcoins are awarded to the miner creating the block. The block reward is a built-in economic incentive for miners to contribute computing power to verify transactions and secure the network. This is also the mechanism for distributing a controlled monetary supply over time without a central bank or other central authority, divided among all miners by ratio of their contributed hash rate. All bitcoins that exist have been created this way, as rewards to miners for verifying blocks in the blockchain. In Bitcoin, the block reward starts at 50 bitcoins and is then halved every 210,000 blocks. Since a block is found approximately every 10 minutes, the Bitcoin block reward halving occurs about every four years. In total, there will be no more than 21 million bitcoins, out of which 75% is already in circulation (Figure 4). Since ownership and control of bitcoin addresses involve the handling of private keys, which is pure information, many bitcoins can become permanently inaccessible. In the best of worlds, all keys are backed up and handled in a secure way such that no one else but the owner of the keys can access them, but in an imperfect world, that is not the case. Some private keys get forever lost through memory failures, computer failures, and negligence. Also, it is technically possible to construct addresses that do not even have any keys associated with them in the first place. Bitcoins sent to such addresses will be visible in the blockchain, but practicality destroyed, since no one will ever be able to access them. From that perspective, the total number of available bitcoins will be less than 21 million.

In Bitcoin, in addition to the block reward, there is yet another incentive for miners in the form of transaction fees. It is voluntary to include a fee when sending a transaction – users can choose to add any fee or none at all. The miner that validates a block by solving the proof-of-work receives the transaction fees for all transactions in the block. If there are more transactions in a 10-minute period than can fit in the next block, miners are incentivized to include the transactions with highest transaction

fees first. Theoretically, the importance of transaction fees will increase over time, as transaction volume surges and block rewards are curtailed. Most wallets (client applications) have a default setting that automatically chooses a recommended transaction fee. The normal transaction fee chosen is based on the amount of data in the transaction and is therefore the same regardless of the amount sent. The average transaction fee is around 0.1 USD as of September 2016.³²

FIGURE 4. Bitcoin Monetary Inflation



Source: <https://bitcointalk.org/index.php?topic=130619.0>

The phenomenon in which there is more than one version of the last valid block, worked on by different parts of the mining network, is called a fork. Due to the nature of blockchain, forks in the chain are natural and happen all the time. An example of a common fork is when different miners each find a valid block at approximately the same time. They send their blocks out to the network, and each node accepts the valid block they received first and rejects the other one. The conflict is naturally resolved whenever one of the branches finds the next block after that. Since the valid chain is always the longest one, as soon as one branch is longer than the other, miners and nodes on the losing branch will quickly jump over to the winning branch. Blocks rejected by the

32. <https://bitcoinfees.21.co/>, retrieved September 6, 2016

blockchain like that are called stale blocks. The process of implementing and deciding on new features in the code or protocol of the blockchain is very similar. A fork is created by a part of the network that implements new features while another continues using old rules. The branch with the majority in term of hash rate will soon have a longer chain, forcing the minority branch to either accept the new rules or continue with their newly created valueless altcoin blockchain. The total mining processing power (21,100,000 PetaFLOPS)³³ securing the Bitcoin blockchain as of September 2016 is about 200,000 times higher than the capacity of the fastest supercomputer in the world, the Sunway TaihuLight (93 PetaFLOPS).³⁴

2.5 The Consensus Algorithm

A public blockchain network, such as the Bitcoin network, consists of nodes, where each node in the network continually collects new transactions into a block that is cryptographically linked to the previous block of transactions. Each node works on generating a proof-of-work required for their block to be included in the chain. When a node manages to generate the proof-of-work for a block, it is broadcasted to all other nodes, which accepts the block into their copy of the blockchain. Then, they immediately start working on the next block. Which node finds the solution to the proof-of-work requirement can be likened to a lottery, where a higher share of computing power gives a higher share of the lottery tickets, but where the winning ticket is randomly selected. This is important, since if it was known which node in the network would validate the transactions in the next block, it would likely be possible to control the network, and it would thus not be decentralized. The longest chain of blocks is created by the majority of computing power and serves as the history of transactions in the network. The blockchain cannot be changed without redoing the proof-of-work, so the record remains secure as long as a majority of the computing power is controlled by nodes that are not cooperating to attack the network. The proof-of-work algorithm ensures that energy, time, and thus work are expended in the decentralized process of arriving at a consensus over the state of the network. It is uncertain if a secure decentralized blockchain can be built without using proof-of-work. The energy consumed is tightly linked to time having passed, which cannot be falsified due to the laws of nature.³⁵ In comparison, information secrets, such as private keys, can be leaked. Using the energy consumed for mining in the entire mining network each 10 minutes (in the case of the Bitcoin blockchain) is what makes it possible to securely and irreversibly time-stamp information into the blockchain.

Proof-of-stake is an alternative proposed mechanism to provide distributed consensus and protection against double spending that a few alternative cryptocurrencies (altcoins) have implemented. In a proof-of-stake system, instead of the nodes with the

33. <http://bitcoincharts.com/bitcoin/>, retrieved September 6, 2016

34. <https://www.top500.org/news/china-races-ahead-in-top500-supercomputer-list-ending-us-supremacy/>

35. <https://webonanza.com/2015/10/12/the-bitcoin-formula-energy-time-truth/>

most computing power, it is the nodes that control the most coins that validate new transactions. One argument is that this consensus system would be more costly to attack since it would require any attacker to own the majority of coins, so the attacker would mostly hurt itself. Another argument in favor of proof-of-stake is that it does not rely on an expensive and potentially environmentally unfriendly work, such as using electricity to perform computational calculations. This is, however, also the Achilles heel of proof-of-stake. Since the verification of transactions in the blockchain does not require any actual work, there is nothing at stake³⁶ and no cost for creating alternative histories of the blockchain. Therefore, it could enable double-spend transactions. The only way to protect against such a nothing-at-stake-attack might be to use trusted third parties that introduce points of centralization or alternatively to anchor the blockchain with proof-of-work. Another criticism is that in the proof-of-stake system, new coins get distributed in a way that makes the people holding the most coins richer without them doing any actual work. Vitalik Buterin, the founder of the second largest public blockchain (Ethereum), has said,

All “pure” proof-of-stake systems are ultimately permanent nobilities where the members of the genesis block allocation always have the ultimate say. No matter what happens ten million blocks down the road, the genesis block members can always come together and launch an alternate fork with an alternate transaction history and have that fork take over.³⁷

Proof-of-stake could perhaps be preferable for some blockchains where a tradeoff between security and other properties, such as storage capacity and speed, are deemed appropriate.

2.6 Layers on top of Blockchain

The Bitcoin blockchain and other blockchains allow room for metadata that can be embedded into transactions, which can be used to encode new protocol layers on top of the blockchain. These overlaying layers can be used to perform logic for issuance and transactions with new asset types for new types of applications. The underlying blockchain serves as a secure backbone on which these new types of transactions and processes are settled. This allows building decentralized applications on top of, for instance, the Bitcoin blockchain.

A small amount of bitcoin or other cryptocurrency can be earmarked through attached metadata to represent another digital asset type, for example, a share in a company. The general term used for this is colored coins. Colored coins are handled by software that can interpret attached metadata, write new metadata, and perform a

36. <https://bytecoin.org/blog/proof-of-stake-proof-of-work-comparison/>

37. <https://blog.ethereum.org/2014/07/05/stake/>

defined set of operations according to the rules for that particular overlaying protocol. Several open source platforms, such as Counterparty, Coinprism, Omni, and Colored Coins, have been developed for these second-layer blockchain protocols that enable peer-to-peer issuance, transactions, and contracts in new types of financial instruments and other digital assets, which could also represent physical assets.

Pegged sidechains, or altchains, offer another approach that could extend the functionality of Bitcoin and other blockchains.³⁸ Sidechains are blockchains that are pegged to and interoperable with the main blockchain, so for example, Bitcoin and other digital assets encoded in Bitcoin could be moved between the Bitcoin blockchain and different sidechains in the future. An argument for building sidechains instead of separate altcoins is that sidechains do not require a new technology stack to be built, and they also do not need new coin distribution and market valuation. Sidechains can allow innovation, experimentation, and implementation of new features without requiring changes to the main blockchain. Sidechains would need to be secured, which could be achieved through the reuse of the proof-of-work that miners of the main blockchain produce in a process called merged mining, which in theory could make sidechains as secure as the main chain. Rootstock is a Bitcoin sidechain that is being developed. It is intended to provide Bitcoin with unlimited smart contract scripting capabilities, which is currently available with the separate altcoin blockchain Ethereum.³⁹

Payment channels are another form of layer that can enable trustless, low cost transactions between parties and be particularly useful for microtransactions. In this system, the parties in a payment channel exchange and settle transactions with each other off-chain, where each new transaction replaces and updates the previous transaction. Eventually, the payment channel will close when either party decides to submit the latest signed transaction between them to the blockchain. The Lightning network is an evolution and extension of the payment channel concept that could allow Bitcoin to scale to millions of transactions per second with immediate settlement.⁴⁰

38. <https://www.blockstream.com/wp-content/uploads/2014/10/sidechains.pdf>

39. <https://www.weusecoins.com/assets/pdf/library/Rootstock-WhitePaper-Overview.pdf>

40. <https://lightning.network/lightning-network-paper.pdf>

3. The Global Blockchain Ecosystem

The blockchain ecosystem today is a rapidly growing, diverse global movement, comprised of software developers, companies, organizations, private users, business users, investors, researchers, enthusiasts, and educators. Blockchain technology enables permissionless innovation in new ways of value transfer, communication, and organization of people and machines. Internet pioneer Marc Andreessen has compared it to the early days of the Internet in regard to the technology's possible future impact on society.⁴¹

The impact of blockchain technology on people at large, business models, public policy, and the overall economy is limited so far. Bitcoin, the first and most popular blockchain cryptocurrency with around 80% of the total market, has a market capitalization of about 10 billion USD (about the size of the GDP of Malta) and around 10 million users (Sep 6, 2016). More than 100,000 businesses accept payments in Bitcoin, and Microsoft, Dell, WordPress, Expedia, and Overstock.com are some of the biggest ones. Upwards of 1 billion USD in venture capital has been invested in Bitcoin and blockchain companies to date, which is comparable to the amount invested in all Internet companies until 1996, when the Internet started to take off.⁴²

The interest from governments and governmental agencies has also started to grow. The first Senate hearing in the United States (November 2013) was called a Bitcoin lovefest by the *Washington Post*.⁴³ The three government officials who testified stressed that Bitcoin has legitimate uses and argued that no new regulations were needed to police illicit uses of the network. This gave an early boost to the legitimacy of Bitcoin. A Senate hearing in Canada (October 2014) resulted in a report that called for a "regulatory light touch" on Bitcoin and digital currencies and deemed the technology "ingenious" and capable of potentially meeting critical needs in both the financial sector and for the unbanked in the world.⁴⁴ Several governmental agencies have

41. <http://www.coindesk.com/marc-andreessen-balaji-srinivasan-discuss-bitcoin/>

42. <http://www.coindesk.com/research/state-bitcoin-blockchain-2016/>

43. <https://www.washingtonpost.com/news/the-switch/wp/2013/11/21/heres-how-bitcoin-charmed-washington/>

44. <http://www.parl.gc.ca/Content/SEN/Committee/412/banc/rep/rep12jun15-e.pdf>

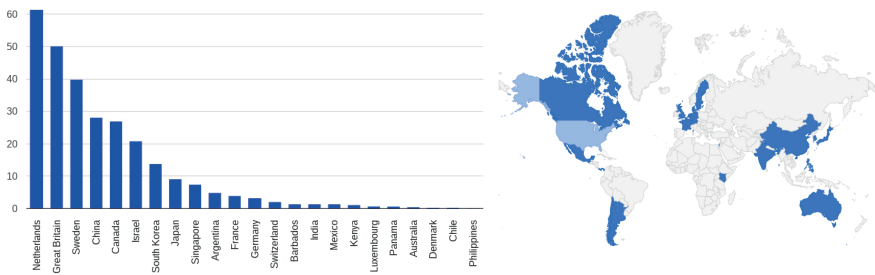
published reports that have analyzed Bitcoin and blockchain technology, such as FBI 2012,⁴⁵ The Commonwealth 2015,⁴⁶ Rand Corporation 2015,⁴⁷ and the UK Government Office for Science 2016.⁴⁸ Some of their conclusions are mentioned in later parts of this report regarding regulatory concerns and possible socioeconomic impacts. The World Economic Forum identified blockchain technology as one of six mega-trends in a survey report published in September 2015.⁴⁹ In the survey conducted with 800 executives and experts from the information and communications technology sector, a majority expected that 10% of the global gross domestic product (GDP) would be stored on blockchains by 2025. The report estimated the current worth of all bitcoins in the blockchain at around 20 billion USD, or about 0.025% of global GDP (around 80 trillion).

In this chapter, we give an insight into the global ecosystem and its geographic distribution as well as an overview of stakeholders, such as companies and organizations, banks and financial institutions, and researchers and academia.

3.1 Geographical Distribution

The Bitcoin and blockchain ecosystem is largest in the United States in terms of software developers, companies, organizations, users, and venture capital investments. Silicon Valley alone accounts for about half of all the publicly disclosed venture capital funding received by Bitcoin and blockchain companies.⁵⁰ Next after the United States, countries in Europe, China, Canada, Israel, South Korea, Japan, and Singapore are home to companies that have attracted the most venture capital funding (Figure 5, Figure 6).

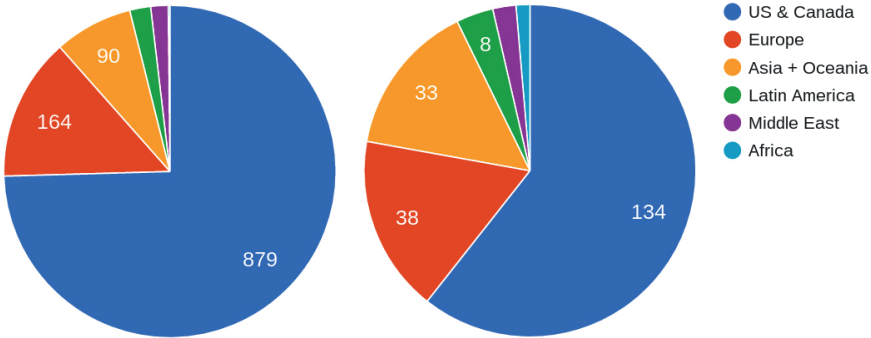
FIGURE 5. Venture Capital Investments by Country Outside the US in \$m (L) and Global Map (R)



Source of data: <http://www.coindesk.com/bitcoin-venture-capital> retrieved March 21, 2016

45. http://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf
 46. <http://thecommonwealth.org/media/event/commonwealth-virtual-currencies-working-group-meeting>
 47. http://www.smallake.kr/wp-content/uploads/2016/02/RAND_RR1231.pdf
 48. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf
 49. http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf
 50. <http://www.coindesk.com/bitcoin-venture-capital/>, retrieved September 8, 2016

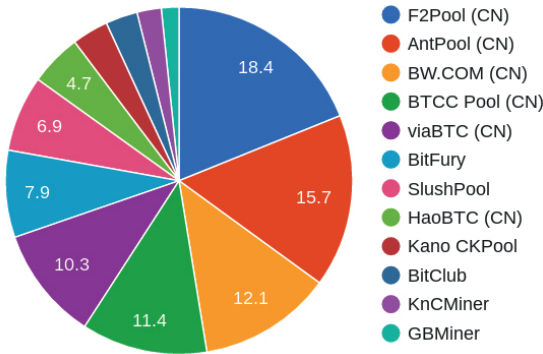
FIGURE 6. Venture Capital by Region in \$m (L) and Number of Companies (R)



Source of data: <http://www.coindesk.com/bitcoin-venture-capital> retrieved September 8, 2016

China is leading the charge in Bitcoin mining, with over 70% of the global Bitcoin mining power currently residing in mainland China⁵¹ (Figure 7). China also has the largest trading volume (CNY to Bitcoin) ahead of the trading done in USD and EUR.⁵²

FIGURE 7. Bitcoin Mining Pool Hash Rate Distribution in Percent; (CN) = Based in China



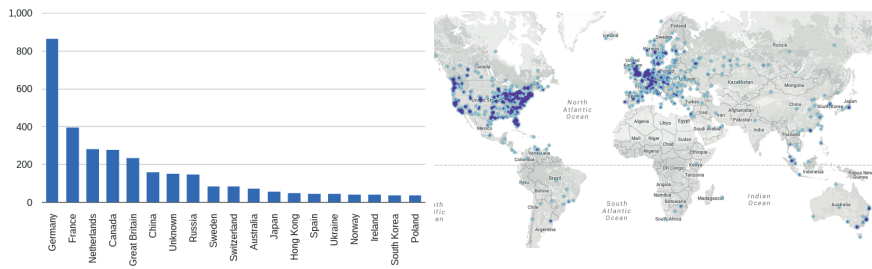
Source of data: <https://blockchain.info/pools> retrieved September 6, 2016

The number of Bitcoin network nodes can serve as a proxy for the proportion of high-level users and companies that a country has in comparison to other countries. The United States dominates this metric with about 27.7% of the current 5,137 Bitcoin nodes, followed by Germany (16.8%), France (7.8%), the Netherlands (5.6%), Canada (5.4%), and the United Kingdom (4.6%), with Sweden in place 10 with 1.7% (Figure 8).

51. <https://blockchain.info/pools>, retrieved September 6, 2016

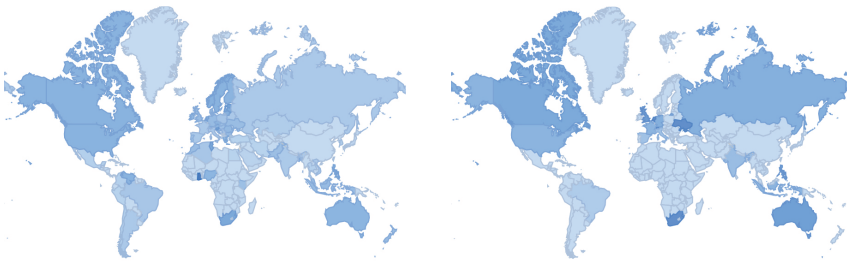
52. <https://bitcoincharts.com/markets/>, retrieved September 8, 2016

FIGURE 8. Bitcoin Network Nodes by Country outside US (L) and Global Distribution (R)



Source: <https://bitnodes.21.co> retrieved September 8, 2016

FIGURE 9. Google Search Volume past 12 Months for Bitcoin (L), Blockchain (R), where Darkest Blue = Index 100



Source: <https://www.google.com/trends> retrieved March 21, 2016

The search volume on Google for words such as “Bitcoin” and “Blockchain” can serve as an indicator of the interest in this technology in different countries. It is interesting to note that Ghana stands out with the highest search volume for “Bitcoin” in the past 12 months, which probably can be attributed to a very active Bitcoin community in Accra,⁵³ followed by Slovenia, South Africa, Tunisia, and Latvia (Figure 9). However, if we instead look at the city level, it looks quite different, with San Francisco in the lead, followed closely by Toronto, New York, Amsterdam, and Los Angeles.

Another measure of adoption is the number of physical Bitcoin ATMs available in each country where people can exchange cash to Bitcoin. The United States has the most installed Bitcoin ATMs with 412, followed by Canada (110), the United Kingdom (32), Spain (24), Australia (19), Finland (17), Switzerland (15), the Czech Republic (14), and Austria (14). Sweden is ranked 26th in the world with only two Bitcoin ATMs.⁵⁴ In gene-

53. <https://news.bitcoin.com/ghana-interested-bitcoin/>

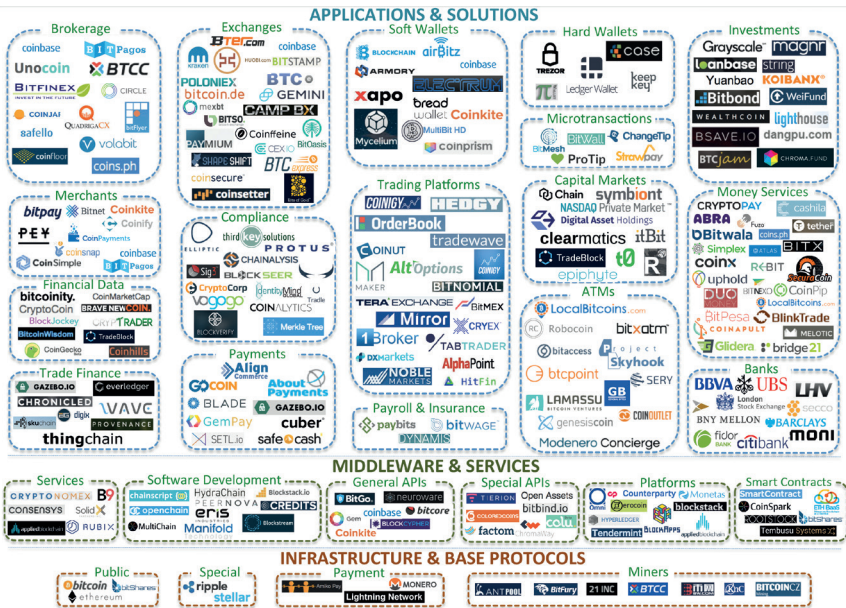
54. <https://coinatmradar.com/countries> retrieved September 5, 2016

ral, countries with a well-educated population, high technical knowledge, and good IT infrastructure are leading this global movement.

3.2 Companies and Organizations

The first nascent Bitcoin companies were established in 2010, and from there, the number of companies and organizations has grown organically. William Mougayar, an entrepreneur, marketer, and business strategist based in Toronto, has made an overview of the blockchain ecosystem, including a selection of 268 companies subdivided into 27 categories and divided into three generic segments: infrastructure, middleware, and applications (Figure 10). These are the same three generic segments he used 20 years ago to understand the Internet ecosystem.

FIGURE 10. Global Landscape of Blockchain Companies in Financial Services



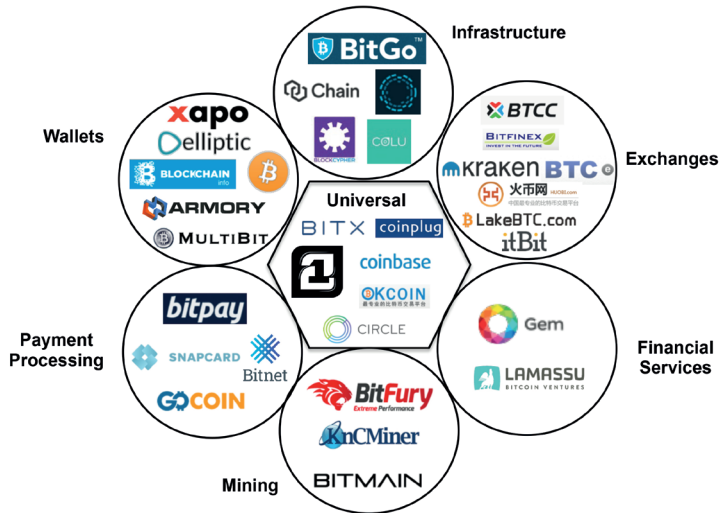
Source: <http://startupmanagement.org/> by William Mougayar

In a report released in March 2016, PwC identified 700 companies entering the blockchain space, with 25 of them expected to emerge as industry leaders.⁵⁵ Coindesk, which is one of the leading platforms for news and analysis of the blockchain ecosystem, uses seven broader categories of industry sectors for the purpose of keeping

55. <http://informs.pwc.es/fintech/assets/pwc-fintech-global-report.pdf>

track of publicly disclosed venture capital funding of companies in the area (Figure 11, Figure 12).

FIGURE 11. Examples of Venture Capital Funded Companies in Seven Industry Sectors

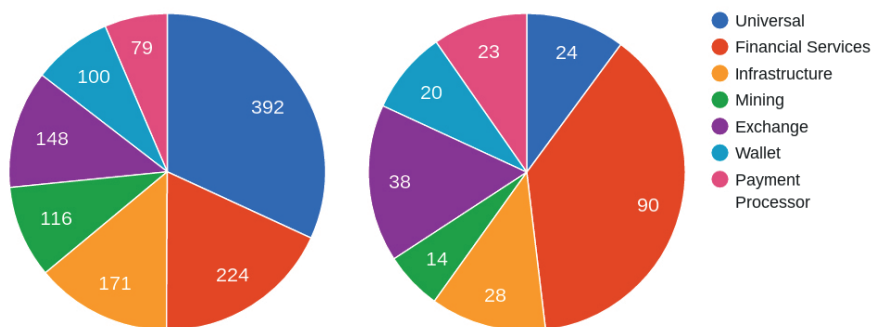


Source: <http://www.coindesk.com/research/state-bitcoin-blockchain-2016/>

The company that has received the most venture capital (VC) investment to date is Circle, which has raised 136 million USD with the intention of offering Bitcoin financial services to consumers worldwide. Another company, 21 Inc., has raised 121 million USD with the focus on building a full-stack infrastructure for Bitcoin, from hardware to software. One of their released products is a small retail computer dedicated to Bitcoin mining, software development, and services, with an innovative marketplace enabled by Bitcoin microtransactions.⁵⁶ Following in order of VC investments, Coinbase is a large currency exchange and merchant platform with 100 employees and 116 million USD in venture capital funding. Blockstream is a company focused on development of the core Bitcoin protocol and accelerating innovation in cryptocurrencies, open assets and smart contracts, and has raised 76 million USD. A few of the next largest companies in terms of venture funding are⁵⁷ Digital Asset Holdings (60 million USD), with a focus on bringing blockchain to the traditional banking industry; BitFury (60 million USD), a Bitcoin mining company; and Chain (44 million USD), a company that is building blockchain software infrastructure.

56. <http://www.coindesk.com/21-inc-launches-bitcoin-micropayments-marketplace/>
 57. <http://www.coindesk.com/bitcoin-venture-capital/>, retrieved July 2, 2016

FIGURE 12. Venture Capital by Industry Sector and Money in \$m (L) and Number of Companies (R)



Source of data: <http://www.coindesk.com/bitcoin-venture-capital/> retrieved September 8, 2016

The Depository Trust & Clearing Corporation (DTCC) – a firm at the center of Wall Street’s trading infrastructure, settling the vast majority of US securities transactions– is building a blockchain-based solution. The corporation announced in March 2016 that they will build a blockchain proof-of-concept for the 2.6 trillion USD repurchase agreement market, in collaboration with Digital Asset Holdings.⁵⁸

The US-based Bitcoin Foundation is the largest and oldest (September 2012) non-profit organization, with the stated mission to support education, engage in advocacy, increase adoption, and encourage the development of Bitcoin and blockchain technology worldwide.⁵⁹ It is supported by many of the largest companies in the industry and a large number of individual members from all over the world.

The Chamber of Digital Commerce is a Washington DC-based trade association launched in July 2014 with the goal of promoting acceptance and use of digital assets and related technologies through education, advocacy, and working closely with policy makers, regulatory agencies, and industry.⁶⁰

At least 17 countries have national Bitcoin and blockchain associations, and The World Bitcoin Association, based in Switzerland, aims to unite all nonprofit Bitcoin organizations around the world and to spread Bitcoin and other cryptocurrencies.⁶¹ Some notable nonprofit organizations that accept Bitcoin for donations are the Electronic Frontier Foundation, Freedom of the Press Foundation, Greenpeace Fund, Khan Academy, Mozilla Foundation, Tor Project, Wikileaks, and Wikimedia

58. <http://www.wsj.com/articles/bitcoin-technologys-next-big-test-trillion-dollar-repo-market-1459256400>

59. <https://bitcoinfoundation.org/>

60. <http://www.digitalchamber.org/>

61. <http://worldbitcoin.info/>

Foundation.⁶² Some of the biggest charities that accept Bitcoin for donations are the American Red Cross, Save The Children, BitGive Foundation, and Direct Relief.⁶³

A new type of organization enabled by blockchain technology is the DAO. The aim is to build organizations of humans and machines without any centralized management. A DAO uses the decentralized trust model of the blockchain and has the ability to send currency and information and to form smart contracts. The most successful nascent projects aiming to build DAOs on the Bitcoin blockchain are the decentralized marketplace OpenBazaar, which launched in April 2016,⁶⁴ and the decentralized currency exchange Bitsquare, which launched later the same month.⁶⁵ Other projects are also under development to build DAOs for ridesharing, cloud storage, and prediction markets.

Another DAO project that has received a lot of attention is The DAO, which was launched on the Ethereum blockchain at the end of April 2016. Its aim was to function as a kind of decentralized crowdfunded investor-directed venture capital fund, used to fund child-DAO projects in a decentralized way. The DAO attracted about 14% of all Ethereum tokens, together worth over 150 million USD from over 11,000 investors. However, a flaw in The DAO allowed a hacker to gain control of around a third of all Ethereum tokens managed by The DAO.⁶⁶ This prompted the Ethereum community to perform a hard fork to essentially roll back the history in an attempt to recover the funds lost due to the flaws in The DAO. This controversial decision was mostly successful, but in the process, one of the most important features of a public blockchain, namely its alleged immutability was compromised. A split of the Ethereum community occurred into users of the forked version of the Ethereum blockchain and a smaller part of the community that continued using the unforked version of the blockchain, naming it Ethereum Classic.⁶⁷

3.3 Banks and Financial Institutions

In the last few years, the blockchain ecosystem has grown significantly. Large banks and financial institutions are exploring how they can adopt the technology underpinning Bitcoin to reduce costs, cut out intermediaries, and increase efficiencies in the backend of the financial industry.⁶⁸ A report by Santander InnoVenture estimated that blockchain technology can reduce infrastructure cost in the financial industry by 15–20 billion USD per year by 2022.⁶⁹ The total cost that banks and financial services have for clearing and settlements today has been estimated at 80 billion USD per year by the blockchain

62. https://en.bitcoin.it/wiki/Donation-accepting_organizations_and_projects

63. <http://bravenewcoin.com/news/donating-bitcoin-to-charities-is-on-the-rise/>

64. <https://blog.openbazaar.org/openbazaar-is-open-for-business/>

65. <https://bitsquare.io/blog/beta-version-launched/>

66. <http://www.coindesk.com/understanding-dao-hack-journalists/>

67. <http://www.coindesk.com/ethereum-hard-fork-creates-competing-currencies-support-ethereum-classic-rises>

68. <https://www.uschamber.com/above-the-fold/blockchain-technology-2016-the-year-the-blockchain>

69. <http://santanderinnoventures.com/fintech2/>

startup SETL.⁷⁰ The hope of the financial industry is that they will be able to reduce processing costs, speed up settlement times, and reduce the risk of human errors and fraud using blockchain technology. Blockchain technology has the potential to enable instant value transfer and settlement 24/7, cryptographically secured transactions with full provenance and chains of custody, immutability, perfect auditability, selective privacy, business automation through smart contracts, and automatic reconciliation of information between all parties involved. Many banks and financial institutions have been exploring blockchain technologies in the last couple of years for these reasons.⁷¹

R3 is a New York startup that leads a consortium of over 40 banks (with a combined market capitalization exceeding 600 billion USD) that are exploring and implementing the use of blockchain technology⁷² (Figure 13). In early March 2016, they finished a trial of five different blockchain ledgers with 40 of the banks involved and tested smart contracts to perform business logic for issuance, secondary trading, and the redemption of financial instruments.⁷³

FIGURE 13. R3 Blockchain Consortium Member Banks



Source: <http://www.coindesk.com/research/state-bitcoin-blockchain-2016/>

UBS, Deutsche Bank, Santander, and BNY Mellon, four of the world’s largest banks, stated on August 24, 2016, that they are collectively developing a new form of digital

70. <http://www.bloomberg.com/gadfly/articles/2016-03-23/wall-street-banks-will-be-the-weakest-link-in-the-blockchain>
 71. <http://bitfury.com/content/5-white-papers-research/public-vs-private-pt1-1.pdf>
 72. <http://uk.businessinsider.com/blockchain-r3-membership-hits-42-as-it-looks-to-non-banks-2015-12>
 73. <http://blogs.wsj.com/cio/2016/03/02/key-blockchain-vendors-cloud-providers-square-off-in-major-test/>

cash, called the utility settlement coin (USC).⁷⁴ The aim is a new industry standard for clearing and settlement based on blockchain technology.

Former JP Morgan executive Blythe Masters is leading Digital Assets Holding, a blockchain startup with the stated mission of improving efficiency, security, compliance, and settlement speed while reducing costs for the financial industry. The company is already valued at over 100 million USD after having raised 52 million USD in funding from banks and financial institutions and signing a contract worth 10.5 million USD with ASX Ltd. to speed up the settlement in Australia's stock market using blockchain technology.⁷⁵

Nasdaq has developed its own blockchain solution, Linq, for which it announced its first issuance of a private security on December 30, 2015.⁷⁶ It is a permissioned distributed ledger for native issuance, allocation, corporate action, auctions, transactions, and the settlement of digital bearer tokens, which are capable of representing any unregistered securities. Nasdaq has also partnered with Estonia's e-Residency program to facilitate blockchain-based e-voting and corporate governance of companies on Nasdaq's Tallinn Stock Exchange.⁷⁷

Microsoft has been working actively on speeding up blockchain adoption for enterprises, governments, and individuals since November 2015 by offering easy access to several different blockchain implementations through their Blockchain as a Service (BaaS), which was built on their Azure cloud computing platform. In June 2016, Microsoft launched Project Bletchley on this platform with the aim of addressing the openness of the platform, performance, scale, support, and stability and to integrate features for identity, key management, privacy, security, management, and interoperability.⁷⁸ Chain (the company) has developed an open source blockchain solution called Chain Open Standard 1 for enterprise solutions in collaboration with VISA and Nasdaq.⁷⁹ It is a permissioned ledger designed to meet the scale, security, privacy, and regulatory requirements of the financial services industry. Chain also offers a hosted cloud computing environment for rapid prototyping and testing of blockchain applications by its clients.

Another key player for building blockchain solutions for enterprises is the Hyperledger Project, which is a collaborative Linux Foundation open source initiative that was announced in December 2015. The 30 founding members are⁸⁰ ABN AMRO,

74. https://www.db.com/newsroom_news/UBS_-Utility_Settlement_Coin_concept_on_blockchain_gathers_pace_24.08.2016.pdf

75. <http://www.bloomberg.com/news/articles/2016-01-21/blythe-masters-firm-raises-cash-wins-australian-exchange-deal>

76. <http://ir.nasdaq.com/releasedetail.cfm?ReleaseID=948326>

77. <http://www.nasdaq.com/press-release/nasdaqs-blockchain-technology-to-transform-the-republic-of-estonias-eresidency-shareholder-20160212-00058>

78. <http://www.cbronline.com/news/cloud/hybrid/microsofts-project-bletchley-to-speed-up-blockchain-adoption-through-azure-200616-4927624>

79. <http://www.prnewswire.com/news-releases/chain-and-global-financial-firms-unveil-open-standard-for-blockchain-300260512.html>

80. <http://www.linuxfoundation.org/news-media/announcements/2016/02/linux-foundation-s-hyperledger-project-announces-30-founding>

Accenture, ANZ Bank, Blockchain, BNY Mellon, Calastone, Cisco, CLS, CME Group, ConsenSys, Credits, The Depository Trust & Clearing Corporation (DTCC), Deutsche Börse Group, Digital Asset Holdings, Fujitsu Limited, Guardtime, Hitachi, IBM, Intel, IntellectEU, J.P. Morgan, NEC, NTT DATA, R3, Red Hat, State Street, SWIFT, Symbiont, VMware, and Wells Fargo.

The involvement by central banks is also growing. By request from the Bank of England, researchers at University College London have created the cryptocurrency RSCoin, with a monetary policy designed to be centralized and controlled by the central bank.⁸¹ Moreover, the Dutch central bank stated in their annual report that they will develop a working prototype called DNBcoin based on blockchain technology.⁸² The central bank of Barbados have published a paper in which they explore the possible future need for the central bank to hold an amount of bitcoin as part of its portfolio of foreign reserves to protect against the destabilization of its currency.⁸³ Reports about digital currencies and blockchain have also been published by the ECB 2012⁸⁴ and 2015⁸⁵, Fed 2014⁸⁶, BIS 2015⁸⁷, UK HM Treasury 2015⁸⁸, and the IMF 2016.⁸⁹ Some of their conclusions are mentioned in later parts of this report regarding regulatory concerns and possible socioeconomic impacts.

Some in the Bitcoin community have expressed skepticism regarding the ability of banks and financial institutions to implement secure private permissioned blockchains, instead of building on an open, public, borderless, decentralized, and permissionless blockchain such as Bitcoin that has been working and hardened on the open Internet for seven years. Public blockchains living on the open Internet tend to grow stronger and more resilient over time, as the network protocol software is frequently updated to counter and withstand every attack vector it is constantly bombarded with. It is like training an antifragile immune system in the most hostile environment. Private blockchains would not face this same pressure to evolve and grow resilient in response to constant attacks since they are kept in a protected network environment. One of the strongest points of contention is also how data security can be maintained in a blockchain without using proof-of-work as the consensus algorithm.⁹⁰

81. Danezis, G., & Meiklejohn, S. (2015). Centrally banked cryptocurrencies. <http://arxiv.org/pdf/1505.06895v2.pdf>

82. <https://www.linkedin.com/pulse/dutch-central-bank-experiment-blockchain-based-simon-lielieveldt>

83. <http://www.centralbank.org.bb/news/article/8827/should-cryptocurrencies-be-included-in-the-portfolio-of-international-reserves>

84. <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>

85. <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>

86. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2544331

87. <http://www.bis.org/cpmi/publ/d137.htm>

88. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/414040/digital_currencies_response_to_call_for_information_final_changes.pdf

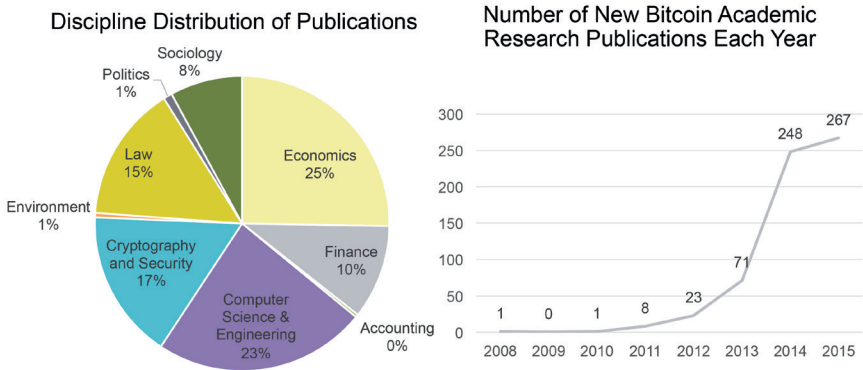
89. <https://www.bitcoinnews.ch/wp-content/uploads/2013/12/sdn1603.pdf>

90. <http://www.truthcoin.info/blog/private-blockchains/>

3.4 Research and Education

The interest from academic researchers all over the world to study Bitcoin and blockchain technology has been growing rapidly. There are now over 600 academic papers published in the fields of economics, computer science and engineering, cryptography and security, law, finance, sociology, environment, and politics (Figure 14).

FIGURE 14. Academic Research Interest



Source: <http://www.coindesk.com/research/state-bitcoin-blockchain-2016>

Several universities have launched courses about cryptocurrencies, and a few have established ambitious digital currency initiatives. The University of Nicosia, which is the largest private university in Cyprus, became the first accredited university in the world to launch a master’s degree program in digital currency in the spring of 2014.⁹¹ The program is offered both online and on campus to students worldwide. It was also the first university in the world to accept Bitcoin for tuition and other fees. The University of Cumbria in the United Kingdom offers two programs linked to the study of cryptocurrencies and complementary currencies, which can be paid for in Bitcoin. New York University and Duke University are two top-ranked universities that began to offer courses on cryptocurrencies in September 2014.⁹² Princeton University offers a free seven-week Massive Open Online Course (MOOC) on Bitcoin and cryptocurrency technologies through Coursera, which was attended by 30,000 students the first time it was given in September 2015. Princeton has also made available a free 300-page peer-reviewed textbook to accompany the course material.⁹³ Stanford University

91. <http://www.unic.ac.cy/digitalcurrency>
 92. <http://www.coindesk.com/top-us-colleges-begin-offering-bitcoin-courses/>
 93. <https://freedom-to-tinker.com/blog/randomwalker/the-princeton-bitcoin-textbook-is-now-freely-available/>

offers a lab course on Bitcoin engineering that teaches how to build Bitcoin-enabled versions of Internet services, such as Twitter, Instagram, WordPress, and Google – and they may offer a MOOC in the near future.⁹⁴ The free Internet learning platform Khan Academy offers one of the most popular MOOCs on the subject of Bitcoin.⁹⁵

The MIT Media Lab launched an ambitious digital currency initiative in April 2015 directed by former White House advisor Brian Forde. The goal of the initiative is to bring together experts, students, governments, nonprofits, and the private sector to research and test concepts on security, stability, scalability, privacy, and economics to support existing and future policy and standards.⁹⁶

94. <http://bitcoin.stanford.edu/>

95. <https://www.khanacademy.org/economics-finance-domain/core-finance/money-and-banking/bitcoin/v/bitcoin-what-is-it>

96. <https://www.media.mit.edu/research/highlights/media-lab-digital-currency-initiative>

4. Blockchain Developments in Sweden

During the past few decades, Sweden has experienced growth and notable international success in the international tech scene. Companies such as Ericsson, Spotify, Skype, Klarna, and Mojang have fueled the technology sector, attracting capital and talent and leading the interest and engagement in the digital transformation. Following the successes of the international so-called unicorns (companies with more than 1 billion USD valuations), an ecosystem of startups, incubators, accelerators, investors, and policy makers has arisen in Sweden.

Financial technologies and communication technologies have become areas of interest to many entrepreneurs. There has also been significant interest in file-sharing and peer-to-peer communication technologies, partly because of the interest awakened by the Swedish Pirate Bay. It is therefore not surprising that when the founder of the Swedish Pirate Party, Rick Falkvinge, was one of the first thought leaders in Swedish politics to post an article about Bitcoin on his website in May 2011, it rapidly gained attention.⁹⁷ Since then, both praise and criticism of Bitcoin and blockchain technology have been spread to the Swedish public by enthusiasts and journalists as well as businesses and governmental agencies.

In this chapter, blockchain developments and organizations in Sweden today are described. An overview of how the technology has been adopted by Swedish companies and organizations is presented, and the increasing interest from banks and financial institutions and academia is outlined.

4.1 Companies and Organizations

Several different stakeholders are involved in blockchain-related activities in Sweden – ranging from startups that are building blockchains or applications on top of blockchains to companies that accept digital currencies in payments and organizations that work to support the system. In terms of publicly disclosed venture capital investments

97. <http://falkvinge.net/2011/05/29/why-im-putting-all-my-savings-into-bitcoin/>

in companies that focus on blockchain technology, Sweden is in fourth place worldwide, after the United States, the Netherlands, and the United Kingdom.⁹⁸

One of the earliest players to receive significant attention in the media is KnCGroup, including its trademarked subsidiary KnCMiner. It specialized in the development of Bitcoin mining processors and hosted at most about 17% of all the computing power in the Bitcoin network. The first Swedish company in the group was founded in 2013⁹⁹ and experienced spectacular growth, developing and selling mining equipment for Bitcoin. After that, the group invested in large Bitcoin mining data centers in Boden in northern Sweden. During the first business year, it reached a turnover of more than 0.5 billion SEK. The company is however a good example of how fast moving the sector is. Despite its successes, and despite a recent venture capital injection of 220 million SEK to help finance new infrastructure, the parent company filed for bankruptcy on May 27, 2016, stating that the main reasons were Swedish energy taxes and vast competition from China during the last few months.^{100 101}

Other businesses with business models based on developing layers on top of blockchain are just starting to gain traction. A Swedish example of that is Strawpay, which was founded in early 2014. Its primary focus is on developing technologies for micro-payments of Bitcoin so that businesses can easily accept small Bitcoin payments with instant transactions. Another example is ChromaWay, which announced a proof of concept blockchain solution in June 2016 for land registration, in partnership with the Swedish National Land Survey (Lantmäteriet), consulting firm Kairos Future, and telecommunications company Telia.¹⁰² ChromaWay has also developed a mobile payment platform in collaboration with Estonia's LHV Bank that enables its users to send and receive EUR instantly and free of charge, based on colored coins technology on the Bitcoin blockchain.¹⁰³

Businesses can also use blockchain technology to prevent the manipulation of data. An example is the Swedish audit and accounting firm Wint, which announced in late 2015 that they have implemented blockchain technology to prevent history falsification of accounting data.¹⁰⁴

Simplifying the access to blockchain-based currencies, Swedish Bitcoin exchanges have emerged that help individuals and businesses exchange between Bitcoin and local currency. BTCX Express started in 2012 and now has 20,000 Swedish customers, according to the company.¹⁰⁵ Safello is another Swedish Bitcoin exchange that started in 2013 and is currently operating in over 30 countries.¹⁰⁶

98. <http://www.coindesk.com/bitcoin-venture-capital/>, retrieved March 26, 2016

99. <http://www.kncminer.com/>

100. <http://digital.di.se/artikel/bitcoinkursen-knackte-knc-miner--ansoker-om-konkurs>

101. <http://www.creandum.com/in-startups-sometimes-things-arent-meant-to-be/>

102. <https://bitcoinmagazine.com/articles/sweden-conducts-trials-of-a-blockchain-smart-contracts-technology-for-land-registry-1466703935>

103. <http://chromaway.pr.co/126406-cuber-first-blockchain-product-to-win-a-major-banking-award>

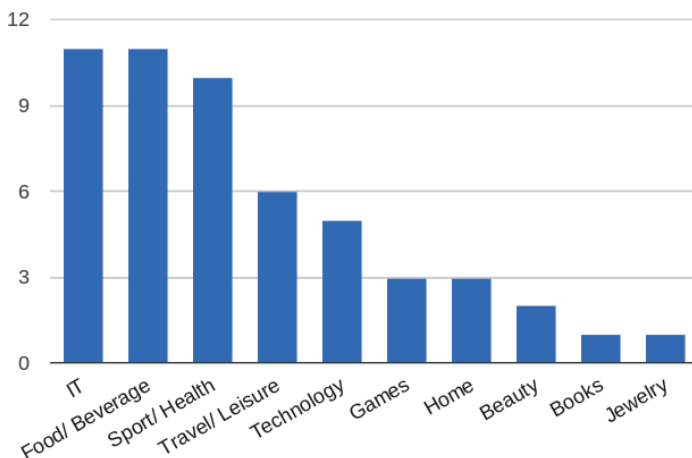
104. <http://blogg.wint.se/2015/12/02/sa-garanterar-vi-att-ingen-andrar-i-bokforingen-i-efterhand/>

105. <http://www.dagensjuridik.se/2015/03/svenskt-bitcoinbolag-gar-till-domstol-vagrar-lamna-uppgifter-om-kunder-till-skatteverket>

106. <https://safello.com/>

The access to digital currencies has enabled companies and organizations to start accepting Bitcoin as payment for their goods and services. However, only 53 companies in Sweden have (as of March 2016) announced that they accept Bitcoin as payment – a relative small number of businesses involved in the Bitcoin ecosystem compared to other countries. In comparison, the Netherlands, which has a population that is 1.7 times larger and a similar socioeconomic background to Sweden, has 4.8 times more businesses that accept Bitcoin as payment than Sweden. Denmark is close behind Sweden with 0.87 times the number of businesses accepting Bitcoin, even though the population of Denmark is almost half of Sweden’s.^{107 108} In Sweden, the majority of businesses accepting Bitcoin are in the IT, food/beverage, and sports/health sectors (Figure 15). The electronic store Webbhallen is the largest business in Sweden that accepts Bitcoin as payment, and they have been doing so since 2014.¹⁰⁹ Most of the companies in the IT sector provide virtual private network services, web tools, and web design, whereas the businesses in the food/beverage and sports/health sectors accept payments online or in physical stores for different goods and services.

FIGURE 15. Number of Businesses per Sector Accepting Bitcoin in Sweden



Source of data: <http://www.bitcoin.se/handlare> and <https://coinmap.org> retrieved March 26, 2016

In addition to investors and active companies, other organizations have formed that focus on applications of blockchain technology. One such organization is the Swedish Bitcoin organization, called “Svenska Bitcoinföreningen.” Its primary purpose is to

107. <http://www.bitcoin.se/handlare>, retrieved March 26, 2016

108. <https://coinmap.org/>, retrieved March 26, 2016

109. <http://www.ehandel.se/stor-svensk-e-handlare-tar-nu-emot-bitcoin-i-kassan,3870.html>

promote the use of Bitcoin in Sweden. In addition, a growing number of meetups, seminars, and even blockchain-related awards are being established.

4.2 Banks and Financial Institutions

The financial technologies sector is growing rapidly in Sweden, with venture capital investments of 266 million USD in Stockholm alone during 2014, which accounts for 32% of the total amount of venture capital and private equity investments in Sweden during the same period. The interest for blockchain technologies among banks and financial institutions is also increasing.

Two of Sweden's largest banks, Nordea and SEB, are involved in the New York-based R3 40+ bank consortium, as previously described in Chapter 3.3. Nordea is the largest financial group in northern Europe, with 10 million private and 500,000 corporate and institutional customers.¹¹⁰ Nordea has a handful of people working full time on projects related to blockchain technology, according to Erik Zingmark, Deputy Head of Transaction Products and Head of Cash Management, who is responsible for blockchain-related work at the bank.¹¹¹ According to Zingmark, this could be the biggest technology shift in the banking world in modern times, and huge operations transferring billions each day are in theory no longer needed, with enormous amounts of money at stake. Zingmark predicts that practical applications of blockchain technology can be in use within one to two years, provided regulators are supportive. SEB has 4 million private, 3,000 corporate and institutional customers, and 400,000 small and medium-sized enterprises (SMEs).¹¹² Nicholas Moch, Head of IT Governance at SEB, has stated that the number of people working on blockchain technology at the firm is in the double digits.¹¹³ Two of the other largest banks in Sweden, Swedbank and Handelsbanken, have stated that they have people working actively with blockchain technology, without giving further details. Swedbank has 7 million private and over 500,000 corporate customers,¹¹⁴ and Handelsbanken has 850 branches in 25 countries.¹¹⁵

Sweden was the first country in the world in May 2015 to have a Bitcoin tracking exchange-traded note (ETN) launched on the Nasdaq Stockholm.¹¹⁶ The ETNs available, "Bitcoin Tracker One" and "Bitcoin Tracker Euro," make it possible to invest in the Bitcoin market price through regular stock markets globally.¹¹⁷ The ETNs are provided by XBT Provider AB, which was originally founded by KnCGroup, the parent company

110. <http://www.nordea.com/>, retrieved March 28, 2016

111. <http://digital.di.se/artikel/storbankerna-sluter-upp-bakom-blockkedjan>

112. <http://sebgroupp.com/>, retrieved March 28, 2016

113. <http://digital.di.se/artikel/storbankerna-sluter-upp-bakom-blockkedjan>

114. <https://www.swedbank.com/>, retrieved March 28, 2016

115. <https://www.handelsbanken.se/>, retrieved March 28, 2016

116. <http://www.coindesk.com/swedens-nasdaq-exchange-approves-bitcoin-based-etn/>

117. <http://www.xbtprovider.com/>, retrieved September 5, 2016

of KnCMiner. It is backed and guaranteed by Global Advisors (Jersey) Limited (GAJL), which acquired it from KnCGroup in June 2016.

4.3 Research and Education

Swedish researchers have started to conduct research on blockchain technology and Bitcoin in particular. A search in the Swedish research archive database DiVA in March 2016, using the search term “Bitcoin,” generated 39 papers, of which 36 were academic publications. And 35 of the papers were student theses, ranging from bachelor’s to master’s degree levels from different universities in Sweden. One paper was a peer-reviewed article published in 2013, and one was a doctoral thesis from 2015, both from KTH Royal Institute of Technology.¹¹⁸ The search term “block chain” generated one additional hit, a student thesis from Linköping University, published in 2014. No courses purely on blockchain technology and cryptocurrency are currently available at Swedish universities. Only one lecture called “Bitcoin and blockchain technology” in a cryptology course at Linköping University was found for 2016.¹¹⁹

118. <http://www.diva-portal.org/>, retrieved March 26, 2016

119. <http://www.icg.isy.liu.se/en/courses/tsit03/>

5. Regulatory Barriers and Opportunities

With the rapid development of blockchain and its different applications, the question arises as to the need to legislate with regard to the technology and its impact. Traditional currencies, financial services, and property ownership are regulated by legal codes that differ between jurisdictions. Blockchain technology, however, is based on a permissionless open source protocol and can be constructed to be agnostic to regional jurisdictions due to its decentralized nature.¹²⁰ This poses new challenges for legislators worldwide.

An Internet communication protocol consists of a set of shared rules for how to send and receive messages over a network, a type of language used by computers to communicate with each other. In this sense, different applications of blockchain, for example, cryptocurrencies such as Bitcoin, are strictly regulated through the rules specified and enforced by its own infrastructure. The only way to take part in the network is by following the rules specified in the protocol. Bitcoin, for example, is an attempt to regulate through computer code rather than through legal and bureaucratic institutions.¹²¹ Just as the Internet provided permissionless information exchange across the globe, blockchain technology may have the same impact on transactions of value, for example, money, financial instruments, and property. With this development, questions arise regarding what regulation is needed to enforce rights, solve conflicts, and protect individuals and organizations in relation to technological development.

This chapter describes and analyzes the aspects that are important for understanding regulatory concerns regarding cryptocurrencies and blockchain technology, such as uses for illegal purposes, irreversibility of transactions, anonymity, and how states and government agencies are tackling regulatory issues so far.

5.1 Criminal Uses of Cryptocurrency

The first regulatory developments that have been observed for blockchain technology have mainly concerned the usage of Bitcoin. Bitcoin became infamous as it was used

120. <https://www.wired.com/2016/03/must-understand-bitcoin-regulate/>

121. <https://coincenter.org/2015/01/bitcoin-regulated/>

as the preferred currency on the pioneering dark web drug marketplace Silk Road, which launched in 2011 and was shut down by the FBI in 2013.¹²² The dark web is a collection of thousands of websites that can only be accessed using anonymity tools, such as TOR and I2P, which hide the IP addresses of users.¹²³ It has become a harbor for different illicit practices because of its opaque nature. Digital currencies have come into favor among dark market users, as they are perceived to offer anonymity and facilitate trade between sellers and buyers.

An early report from the FBI in 2012¹²⁴ expressed concerns that Bitcoin may be used as a tool for money laundering and other criminal activities. The FBI report described how Bitcoin could pose new challenges for law enforcement with regard to the detection of suspicious activity and identification of users in connection to illicit activities.

An important feature of blockchain transactions is that they are irreversible. There is no recourse to reverse a transaction if the receiver commits a fraud, for example, by not producing the agreed-upon goods or service. When using credit cards, customers are to some extent protected against the loss of money from fraudulent merchants; payments can be reversed by credit card companies. With Bitcoin, as an example, there is no third party that takes on that responsibility, which actualizes the need for potential internal or external regulation.

Since Bitcoin transactions are irreversible, the currency has become popular with fraudsters. Cryptocurrencies can also facilitate for extortionists and kidnappers to receive ransom. A phenomenon that has received a lot of media coverage in the last year is ransomware viruses that encrypt the files on infected computers and ask for bitcoins in return for the decryption key.¹²⁵ Hospitals, schools, and public institutions seem to be either particularly targeted or vulnerable to this lucrative criminal enterprise. Ransomware has existed since 1989 but grew explosively in late 2013. Cryptolocker, the first ransomware that asked for payment in Bitcoin, extorted 27 million USD with an estimated 250,000 victims in just three months.¹²⁶ This gave rise to several copycats, such as Cryptowall 3.0, which is estimated to have extorted 325 million USD from hundreds of thousands of victims around the world,¹²⁷ and Locky, which infected 250,000 computers in just three days.¹²⁸ The ransomware typically asks for a few hundred USD paid in bitcoins to unlock the infected computers. Kevin Beaumont, a British analyst that kept track of the Locky virus called it “a genuine cybersecurity incident” and a “masterpiece of criminality.”¹²⁹ To come to grips with these threats, a

122. <http://www.wired.com/2015/04/silk-road-1/>

123. <https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/>

124. http://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf

125. <http://www.ibtimes.co.uk/cisco-ransomware-supervillain-cybersecurity-none-our-pcs-will-be-safe-again-1564094>

126. <http://www.zdnet.com/article/cryptolockers-crimewave-a-trail-of-millions-in-laundered-bitcoin/>

127. <https://www.cryptocoinsnews.com/ransomware-racket-nets-developers-325-million-in-bitcoin-report/>

128. <http://www.forbes.com/sites/thomasbrewster/2016/02/18/ransomware-hollywood-payment-locky-menace/>

129. <https://medium.com/@networksecurity/you-your-endpoints-and-the-locky-virus-b49ef8241bea>

general improvement in computer security and backup practices would be needed to enhance the immune systems of computers connected to the Internet.

5.2 The Complexity of Blockchain Regulation

Technological developments often move faster than laws and regulation adapt. Bitcoin and blockchain technology is not easy to fit under current regulations as a currency, financial instrument, financial institution, or other disparate category. Rather, it is an integrative technology that potentially can serve several of those roles. Arguably, Bitcoin can be said to represent a new asset class that shows a uniquely low correlation to traditional asset classes, making it interesting as a hedge in investment portfolios.¹³⁰ However, existing laws do not necessarily need to be changed to accommodate blockchain technology and cryptocurrency. It may be sufficient to clarify through regulatory guidance how already existing regulations apply to the different use cases of blockchain technology and cryptocurrencies. Moreover, this kind of guidance would not require the long process of new legislation, and would suggest that existing regulations already apply for any new technology.

Similar situations have occurred in the past when new technologies have not easily fit into the existing regulatory framework. A good example is the Voice over Internet Protocol (VoIP), which started to gain traction and was adopted for mass market consumers by Skype in 2003. Skype argued that it was not a telecommunications company and therefore should not be regulated as one.¹³¹ Skype stressed that they had simply developed a piece of software and released it directly to users. The users running the software created a peer-to-peer communications network that existed independently of the company that developed the software. The same applies to Bitcoin and other open source blockchains. However, it is not one company that runs the processes, but volunteers from all over the world that contribute to the development. Just like the Skype software implemented a VoIP protocol for voice communication, blockchain software implements a protocol for another type of communication.

5.3 Regulating the Anonymity of Cryptocurrencies

Bitcoin is not anonymous, but pseudonymous. For every transaction, the sender's address, the receiver's address, and the value transacted is permanently registered, publicly viewable, and searchable by anyone on the blockchain via a long list of available block explorers¹³² (one of the most popular being <https://blockchain.info>). However, information about the identity of the person or company that owns a certain

130. <http://www.forbes.com/sites/laurashin/2016/06/02/4-reasons-why-bitcoin-represents-a-new-asset-class/>

131. <http://www.coindesk.com/bitcoin-regulation-lessons-early-days-skype/>

132. https://www.reddit.com/r/Bitcoin/comments/3fvoxm/a_list_of_block_explorers_more_than_10/

address is unknown unless voluntarily disclosed or discovered somehow, and each entity can own as many addresses as it wants.

One way to obfuscate specific bitcoins transaction history is to form transactions where they are mixed with bitcoins from others. Other methods include exchanging Bitcoin into other more privacy centric cryptocurrencies, such as Dash or Monero, which have additional privacy features built in.¹³³

Privacy is an essential characteristic of money and is closely tied to the concept of fungibility, which means that each unit of currency is exchangeable for any other regardless of its history. It does not matter where funds have come from, if they have been generated through legal or illicit activities, they still carry the same value. In Bitcoin, all transactions are stored publicly and permanently on the blockchain. This means that anyone can see the balance and transaction history of any Bitcoin address. This raises questions about Bitcoin's fungibility.¹³⁴ Insufficient privacy could potentially result in a loss of fungibility, where the value of older bitcoins could decrease if they have a provable transaction history tied to illegal purchases, and new bitcoins with a clean transaction history could be valued higher.¹³⁵ Bitcoins are less anonymous than cash, but more anonymous than credit/debit cards and bank accounts, where the owner of each specific account can be traced.

Financial privacy is a requirement by law in many jurisdictions, for example, through financial privacy acts and bank secrecy acts. Businesses might not want their competitors to find out who their suppliers are. They might also be cautious not to reveal information about their markup and pricing strategies. Private individuals might want to keep, for instance, their bills to the psychiatrist private.

Several proposals for how to improve privacy in Bitcoin have been introduced. One is stealth addresses, which would allow bitcoins to be received without revealing all other transactions sent to the same address.¹³⁶ Another proposal that is being explored is Confidential Transactions, which would keep the amounts transferred in a blockchain transaction visible only to participants in the transaction.¹³⁷ These privacy features would not only benefit Bitcoin but also the blockchain technology that is implemented in the regulated banking and financial industry, where privacy for transactions is required by law. It could also make illegal uses of blockchain technology harder to track.

5.4 Transparency and Accountability

While some forces call for more anonymity – not the least among those with a libertarian affinity, who initiated Bitcoin as an invention – others wish to build in

133. <https://news.bitcoin.com/meet-top-3-coins-cryptocurrency-anonymity-race/>

134. <https://bitcoinmagazine.com/articles/is-bitcoin-headed-for-a-break-in-fungibility-1450823559>

135. <http://investmentwatchblog.com/bitcoin-is-being-challenged-by-a-perceived-difference-in-fungibility-between-old-and-new-units/>

136. <https://blog.coinjar.com/2014/01/16/stealth-addresses-what-are-they-and-do-i-need-one/>

137. <https://www.elementsproject.org/elements/confidential-transactions/>

more transparency and traceability in the technology. In most jurisdictions, there are well-established rules and regulations around banks, financial institutions, and payment systems. Accountability, transparency and traceability are all fundamental aspects of a working societal control structure and a regulated market. For instance, individual privacy has to be balanced against crime-prevention and crime-solving measures. The strive to enable regulatory compliance is one of the key driving factors behind private blockchain solutions being experimented with and brought about in contemporary implementations at this stage. For public blockchain technology to be maturely integrated into societal functions, rules will need to be amended, and measures for ensuring transparency, and accountability will need to be actualized in the technology.

Using the inherent links between addresses and transactions, cluster analysis techniques can be used to link together financial transactions and their entities in the blockchain. Using one or more addresses known to be owned by one entity, the goal is to find out which other addresses in the blockchain that belong to the same entity. To do this, a set of assumptions (heuristics) are made about how Bitcoin wallet software handles transaction and address reuse. In one demonstration of these techniques, Blockstream testing engineer Jonas Nick was able to find 70% of all bitcoin addresses belonging to the same bitcoin wallet, given knowledge about one of its addresses.¹³⁸

Several companies in the blockchain ecosystem are focusing on building tools to analyze blockchain for compliance and law enforcement purposes. Chainalysis, Coinalytix, and Elleptic are some of the companies building real-time blockchain analytics platforms to help businesses stay compliant with anti-money laundering regulations, to make risk assessments, and to determine which entity a transaction originates from.

A new cryptocurrency being developed called Zcash is based on the zerocash¹³⁹ protocol, which uses zero knowledge proofs to enable transactions on a public blockchain, where the sender, the recipient, and amount of transactions remain private by default – but with the ability to voluntarily disclose transactions using separate view keys. This project, if successful, has the potential to provide cryptocurrency with confidential transactions, including the option of selective transparency, such as to enable audits.

One option to protect the senders of money is multisignature escrow transactions, which are built into the blockchain protocol and are currently being further developed with layers of applications.¹⁴⁰ The normal approach to this is to use a multisignature transaction that requires signing with any two out of three private keys. The buyer sends bitcoins to a Bitcoin multisignature address for which the buyer holds one private key, the seller holds one private key, and a third party arbitrator holds the third private key. This way, the money can be held in escrow until the seller has fulfilled their obligations. If the buyer and seller are satisfied, they can together sign a transaction

138. https://www.reddit.com/r/Bitcoin/comments/4b9ylx/bitcoin_privacy_theory_and_practice_jonas_nick/

139. <http://zerocash-project.org/>

140. <https://en.bitcoin.it/wiki/Multisignature>

using their private keys. When there is a dispute, the escrow agent investigates and decides which of the two parties receives the money. A transaction is then signed using the third private key together with the private key of either the buyer or the seller, or potentially a percentage split of the money to each party.

5.5 Blockchain Regulations to Date

To address the complexities of blockchain technology, formal regulations are being issued on the national and regional levels. Most of the regulations to date have focused on Bitcoin, other digital currencies, and their handling organizations.

In October 2012, the European Central Bank (ECB) published a report in which it classified virtual currencies into three categories, depending on whether they have no trade, unidirectional trade, or bidirectional trade with the regular economy.¹⁴¹ The ECB concluded that the Electronic Money Directive (2009/110/EC) and the Payment Services Directive (2007/64/EC) could not be applicable to Bitcoin because it does not fulfill all the criteria outlined in the directives to meet the definition of electronic money, since there is no responsible issuer behind cryptocurrencies and they are not issued as a claim on the issuer.¹⁴² This means that the regulation of cryptocurrencies in the EU is left for each member state to decide.

In March 2013, the first regulatory guidance was issued in the United States by the Financial Crimes Enforcement Network (FinCEN) of the US Treasury, in which Bitcoin and digital currencies that are not legal tender under any sovereign jurisdiction were classified as “virtual currencies.”¹⁴³ FinCEN declared that the users of virtual currency are not money services businesses (MSB) under FinCEN’s regulations and therefore not subject to MSB registration, reporting, and recordkeeping regulations. Thus, a person who accepts real currency in exchange for virtual currency, or vice versa, is not a dealer in foreign exchange under FinCEN’s regulations, and therefore the Bank Secrecy Act (BSA) is not applicable. However, a person that creates units of convertible virtual currency – for example, through mining – and sells those units to another person for real currency or its equivalent was deemed a money transmitter and, as such, subject to regulation. FinCEN also claimed regulatory authority over American entities that manage Bitcoin in a payment processor setting or as an exchanger, requiring them to disclose large transactions and suspicious activity, comply with money laundering regulations, and collect information about their customers as traditional financial institutions are required to do.¹⁴⁴ In August 2013, a judge in Texas ruled that Bitcoin is “a currency or a form of money” and, as such, subject to the court’s jurisdiction under applicable laws.

141. <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>

142. <http://lecocqassociates.com/publication/virtual-currencies/>

143. https://www.fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html

144. http://www.abajournal.com/magazine/article/some_basic_rules_for_using_bitcoin_as_virtual_money/

In August 2013, the German Ministry of Finance characterized Bitcoin as a unit of account, a kind of private money, subject to capital gains tax if held less than one year.¹⁴⁵ Finland issued regulatory guidance on Bitcoin soon after in September 2013, specifying a capital gains tax on Bitcoin and the taxing of bitcoins produced by mining as earned income. The Swedish Tax Agency classified Bitcoin as a capital investment object in May 2014, with requirement to pay capital gains taxes on realized gains, similar to commodities.¹⁴⁶ However, Sweden's financial supervisory authority (Finansinspektionen) has regarded Bitcoin as a means of payment since the end of 2012, with the requirement that businesses that trade with Bitcoin are registered and follow regulations to prevent money laundering.¹⁴⁷ Over 30 countries had issued regulatory guidance by the end of 2013 and beginning of 2014 on Bitcoin and what taxes were applicable.¹⁴⁸ Few governments have announced any intention to prohibit the use of Bitcoin and other cryptocurrencies, but many have warned that Bitcoin is not an official currency and that it is highly volatile, highly speculative, and not entitled to any legal claims or guarantees of conversion. In December 2013, the People's Bank of China declared that banks and payment companies were prohibited from dealing with Bitcoin, but the country's citizens were still free to buy and sell it.¹⁴⁹ Canada has been one of the more welcoming jurisdictions, with a report published in June 2015 by the Canadian Standing Senate Committee on Banking, Trade, and Commerce, following investigations and several senate hearings since March 2014. The report called for a regulatory light touch on Bitcoin and digital currencies to minimize actions that might stifle the development of these new technologies.¹⁵⁰ In Switzerland – where blockchain companies that offer exchange and wallet services are often regulated as banks – 24 members of parliament have proposed a motion to reduce the regulatory burden on blockchain startups to promote growth and innovation.¹⁵¹ Hong Kong has decided not to regulate trading in virtual commodities, primarily because it is not seen as posing a threat to Hong Kong's financial system due to the lack of widespread adoption, while criminal activities and fraud using digital currencies fall under existing legal statutes.¹⁵²

Bitcoin and other cryptocurrencies are legal to use in most countries in the world, but there are a few exceptions (Figure 16). Countries that have explicitly banned Bitcoin are Bangladesh, Bolivia, Ecuador, and Iceland.

145. <http://www.spiegel.de/international/business/germany-declares-bitcoins-to-be-a-unit-of-account-a-917525.html>

146. <http://www.bitcoin.se/2014/05/02/skatteverket-om-kapitalvinstbeskattning-av-bitcoin/>

147. <http://www.svd.se/fi-ser-penningvatrisk-med-bitcoin>

148. https://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country, retrieved April 8, 2016

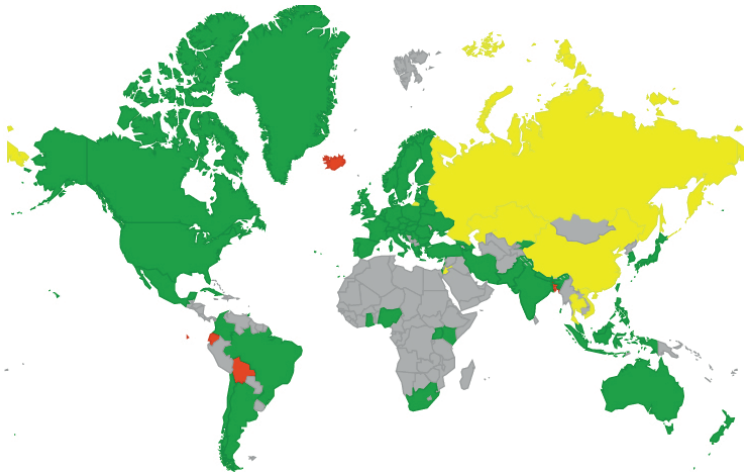
149. <http://www.bloomberg.com/news/articles/2013-12-05/china-s-pboc-bans-financial-companies-from-bitcoin-transactions>

150. <http://www.parl.gc.ca/Content/SEN/Committee/412/banc/rms/12jun15/home-e.htm>

151. <https://news.bitcoin.com/switzerland-eases-bitcoin-regulations/>

152. <http://www.coindesk.com/hong-kong-bitcoin-legislation-not-necessary/>

FIGURE 16. Bitcoin Legal Status, green = permissive, yellow = contentious, red = hostile, and grey = unknown



Source of data: bitlegal.io, wikipedia.org, coindesk.com

The Central Bank of Iceland issued a statement in March 2014 explaining their opinion, namely, that purchasing bitcoins violates the Icelandic Foreign Exchange Act no. 87/1992, which restricts citizens from transferring foreign currency across borders.¹⁵³ The Central Bank of Bolivia declared in May 2014 that it is illegal to use any kind of currency that is not issued and controlled by a government or an authorized entity.¹⁵⁴ The Central Bank of Bangladesh issued a statement in September 2014 about how trading in Bitcoin and other digital currencies could lead to a punishment of up to 12 years in prison, invoking provisions of the Foreign Currency Control Act of 1947 and the Money Laundering Control Act of 2012. The National Assembly of Ecuador voted to ban decentralized digital currencies such as Bitcoin in July 2015 while proposing to develop its own digital currency.¹⁵⁵

In June 2015, New York State Department of Financial Services (NYDFS) launched a licensing regime for virtual currency businesses in the state of New York and businesses involving any New York resident. For the license application, highly detailed levels of information are required, which market players have argued pose great entry barriers for new market entrants. The application, for example, requires detailed biographical information, photographs, financial statements, and fingerprints (to be submitted to the FBI and Criminal Justice Services) for each applicant and person affiliated to the

153. <http://www.cb.is/publications-news-and-speeches/news-and-speeches/news/2014/03/19/Significant-risk-attached-to-use-of-virtual-currency/>

154. <http://www.coindesk.com/bolivas-central-bank-bans-bitcoin-digital-currencies/>

155. <http://www.coindesk.com/ecuador-bans-bitcoin-legislative-vote/>

company. It also needs to include a background report prepared by an independent investigatory agency for each individual applicant, each principal officer, principal stockholder, and principal beneficiary of the applicant. Further requirements include details of all banking arrangements, all written policies and procedures, organization charts detailing management structure, a list of all of the applicant's affiliates, and an organization chart illustrating the relationship among the applicant and all affiliates.¹⁵⁶ The application fee is 5,000 USD, and additional fees for processing additional applications related to the license may be incurred. When the regulation came into effect in August 2015, at least 15 Bitcoin companies ceased doing business in New York State and with residents of New York, while at least eight companies decided to apply for a Bitlicense.¹⁵⁷ Bitstamp, one Bitcoin exchange that decided to apply for the license, estimated the cost to be roughly 100,000 USD, including time allocation and legal and compliance fees.¹⁵⁸ MonetaGo, another Bitcoin exchange, said that the BitLicense application they submitted was 500 pages long.¹⁵⁹ It is worth noting that in March 2016, only one company had been granted a Bitlicense, while 21 companies had ongoing applications.¹⁶⁰

In October 2015, the European Court of Justice ruled that Bitcoin transactions should be exempt from the value added tax (VAT), in response to a request by Swedish tax authorities.¹⁶¹ The ruling effectively recognized Bitcoin as a legitimate means of payment in Europe, putting it in the same category as other currencies for tax purposes. According to a report released by the SWIFT Institute in November 2015, the EU is years away from implementing a consistent framework for cryptocurrency regulation.¹⁶² The report notes the lack of convincing arguments to include cryptocurrencies under the EU's current legal frameworks, set by the revised Directive on Payment Services (PSD2) and the fourth European anti-money laundering directive (AMLD4), since cryptocurrencies do not fit the requirement of a responsible issuer to fit the definition of electronic money.

In February 2016, a Commonwealth Working Group on Virtual Currencies released a report prepared by representatives from Australia, Barbados, Kenya, Nigeria, Singapore, Tonga, the Commonwealth Telecommunications organization, the World Bank, INTERPOL, and the UN Office on Drugs and Crime. It encouraged its 53 member countries to consider the application of their existing legal frameworks to virtual currencies and that they, where appropriate, should adapt them or enact new legislation to regulate virtual currencies.¹⁶³ It also called for developing and improving the capacity of law enforcement in areas of digital forensics and encouraged the establishment

156. <http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf>

157. <http://www.coindesk.com/bitlicense-round-up-whos-left-standing-in-new-york/>

158. <http://www.coindesk.com/real-cost-applying-new-york-bitlicense/>

159. <http://www.coindesk.com/new-york-bitcoin-scene-divided-as-bitlicense-deadline-looms/>

160. <http://www.coindesk.com/months-bitlicense-bitcoin-still-startups-await-approval-new-york/>

161. <http://www.reuters.com/article/us-bitcoin-tax-eu-idUSKCN0SG0X920151022>

162. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2665973

163. http://thecommonwealth.org/sites/default/files/press-release/documents/P14195_ROL_Virtual_Currencies_D_Tait_V5_LoRes.pdf

of industry associations within their jurisdictions to support the development of a responsible and sustainable virtual currency industry.

The status for Bitcoin in Russia is contentious. Russia's Ministry of Finance presented a draft bill in March 2016 that would ban production and circulation of bitcoins, with punitive damages ranging from million ruble fines to seven years in prison. The bill was later turned down by the Ministry of Justice, which cited the lack of appropriate justification for the criminalization of cryptocurrencies and their public danger; the draft was too broadly worded in regards to the definition of e-currencies as "money surrogates."¹⁶⁴ It remains to be seen if a revised bill will be submitted.

As the uptake of digital currencies and the evolution of new blockchain applications are ongoing, regulators are continuously following the developments to be able to respond appropriately. Since the users of the systems (e.g., the owners of bitcoins) are rewarded when the system works as intended (and the value of their digital assets remains or increases), many users in the network actively contribute to the strengthening of the infrastructure and its regulations. In collaboration with official regulators, their engagement in the network could be harnessed to decrease the applications of blockchain for illicit use.

164. <http://www.coindesk.com/russias-bitcoin-ban-draft-bill-withdrawn/>

6. Political and Economical Implications

The Internet enables global and nearly instant exchange of information. With the extension of blockchain technology, direct communication of value and money would also be enabled. Businesses agreements can take place without intermediaries, and peer-to-peer transactions can take place directly. Previously, reaching a global market was reserved for larger corporations, but now Internet and blockchain payment networks allow even single individuals to reach the global market with their services and products. This rapid technological development offers the potential for growth for actors of different sizes in the markets and for policy makers who seek to stimulate innovation and entrepreneurship.

6.1 Lowered Transaction Cost

The creation of institutions is often described in economic theory as a measure to reduce transaction costs. These costs encompass all kinds of factors that challenge, hinder, slow down, or drive up the cost for a transaction between two parties. The term cost includes not only the monetary value but also the time, difficulty, and other disturbances that may arise in connection to a transaction.¹⁶⁵ Transaction costs can be divided into the costs connected to a transaction before, during, and after a transaction. The costs before a transaction are associated with the task of finding a suitable counterparty and for conducting supply, quality, and price comparisons. The costs during the transaction stem from designing, implementing, and executing a contract. Control costs arise after the transaction has taken place and include the enforcement of the contract and the supervision of the parties' contractual compliance.¹⁶⁶

Factors that add to increased transaction costs also include information asymmetries between sellers and buyers, as well as the uncertainty of ownership regarding whether the counterpart is the true possessor of the good being sold. Together, they

165. Groenewegen, J., Spithoven, A. H. G. M., & Van den Berg, A. (2010). *Institutional economics: An introduction*. Hampshire: Palgrave Macmillan

166. <http://www.diva-portal.org/smash/get/diva2:812816/FULLTEXT01.pdf>

reduce the efficiency of the market, and the stakeholders in transactions therefore look for ways to reduce these barriers and transaction costs.

Through blockchain implementations, transaction costs can be reduced as the need for trusted intermediaries to relay transactions is eliminated along with the need for sellers of goods and services to trust that buyers can deliver a legitimate payment. The blockchain network in its entirety acts as the trusted party in the transaction. Blockchain currencies can also reduce the need for and cost of currency conversions in cross-border transactions.

For merchants, Bitcoin – and maybe other blockchain currencies in the future – has the potential to contribute to increased profit margins by reducing transaction fees, fraud, chargebacks, and fees for specialized payment terminals, while lowering the risk of physical robberies.

A global searchable database of all transactions enabled by blockchain technology also has the potential to lower transaction costs (incurred in the form of search and information costs) and policing and enforcement costs. Autonomous agents constructed by bundles of smart contracts acting on the blockchain offer the possibility of eliminating agency and coordinating costs and can perhaps even lead to highly distributed enterprises with little or no centralized management.¹⁶⁷

6.2 Transparency in Society

Many proponents of libertarian ideals celebrate the decentralizing power of blockchain technology, highlighting how its technology has the potential to decrease the need for and reliance on the state. However, the technology can also be used to improve existing systems of governance through strengthening the societal functions and elements of the welfare state.

Blockchain technology can for example increase the transparency between governmental agencies and citizens. Fraud and error in payments and the costs of protecting citizens' data can be reduced while enabling the secure sharing of data between different entities. This can contribute to the formation of information marketplaces, reduce market friction, facilitate the interaction of small and medium-sized businesses (SMEs) with local and national authorities, and promote growth and innovation possibilities for SMEs.¹⁶⁸ Reduced transaction costs for SMEs in dealing with local and national governments can enable SMEs to move more freely in the market and to face lower operating costs.

Sir Mark Walport, Chief Scientific Adviser to the UK government has stated the following:

167. <https://hbr.org/2016/05/the-impact-of-the-blockchain-goes-beyond-financial-services>

168. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

Distributed ledger technology provides the framework for government to reduce fraud, corruption, error and the cost of paper-intensive processes. It has the potential to redefine the relationship between government and the citizen in terms of data sharing, transparency and trust. It has similar possibilities for the private sector.¹⁶⁹

Blockchain technology can also help assure that welfare support is more efficiently distributed. If the technology were applied in the registration and payment processes for government benefits, fraud and error could be prevented. Vulnerable citizens could be offered easier access to government services and reach a level of fuller financial inclusion.¹⁷⁰ Business licensing, registration, insurance, and pension data could also be registered in a blockchain ledger.

Blockchain solutions could be applied both nationally and across regions for taxation management. For example, VAT standards and protocols could be managed through a blockchain, which could enable real-time tracking of payments and address various threshold differences in VAT applicability across EU member states. The administrative burden of companies and tax authorities could be decreased through automatic and easily auditable digital records of all transactions. Credit risk could be assessed more accurately, reducing the losses incurred by insolvency and improving the monitoring of systemic risks.

Blockchain technology could support and strengthen the distribution of international aid. One of the Swedish International Development Cooperation Agency's (SIDA) most prioritized areas is anti-corruption,¹⁷¹ and monitoring fund disbursements in operations and countries is high on the agenda. The blockchains' functionality, with irreversible and reliable transfers of digital goods without intermediaries, could serve as an important tool for SIDA and donors globally. Funds can directly reach end users, surpassing limitations and restrictions set up on currencies and banking services in some countries. The misappropriation of funds for purposes other than the intended ones can be reduced, and in addition, funds could be used more efficiently as the transaction costs, with money transfers over the blockchain, could be more cost-efficient than current remittance systems. Blockchain technology could thus further support the Swedish government in its stated mission to work towards the Sustainable Development Goals set out by the United Nations (UN) in 2015, thereby reducing corruption and achieving development objectives.¹⁷²

In fact, some blockchain proponents argue that the largest impact for blockchain technology might be realized in developing countries where the financial infrastructure is poor, a large part of the population is unbanked, and the dependence on remittances

169. <http://bravenewcoin.com/news/british-prime-minister-and-cabinet-advised-to-start-using-distributed-ledger-technology/>

170. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

171. <http://www.sida.se/English/how-we-work/approaches-and-methods/our-work-against-corruption/>

172. <http://www.regeringen.se/regeringens-politik/globala-malen-och-agenda-2030/>

from other countries is large. However, many obstacles need to be overcome before this can be a reality.¹⁷³ Because of the requirements of technical expertise and access to technical infrastructure, it is likely that blockchain technology, to a larger extent, will be adopted in advanced economies first.

Another area, which might benefit from blockchain technology is in job search and matching. With the growing global movement of labor, it has become increasingly difficult for employers to verify the qualifications of job candidates. The process of verifying that a candidate in fact has the degree or certificate he or she claims from an educational institution is in many cases hard, if not impossible. In the MIT Media Lab, a group of researchers has started exploring how digital graduation certificates could be registered on the blockchain.¹⁷⁴ This has until now been done only on a local scale but the group has released the code, which is open source, for others to follow suit. If universities and institutions world-wide would adopt the technology and practice, easier verification of academic qualifications globally could be enabled. If an institution would shut down, due to wars or political conflicts, there would still be a reliable registry over the certificates that the educational institution has issued. Job applications would become more reliable, and the transition between educational institutions would be simplified. The increased trust in qualifications from foreign educational institutions would potentially lower the barriers to entry into new job markets for immigrants, and search costs in recruitment and staffing could be decreased. It would also be easier to detect fraudulent institutions, for example, issuing questionable certificates to candidates without necessary qualifications.

Sustainability is becoming an increasingly important topic for businesses, both due to the requirements of customers and for the demands for more sustainable business practices worldwide. Before reaching the end consumer, goods often travel vast distances from producers, assemblers, distributors, transporters, and storage facilities to suppliers in different areas. The creation and exchange of goods often have negative environmental and societal effects: exploitative extraction, hazardous work conditions (sometimes involving child labor and slavery), forgery, environmental effects, and the waste of valuable material at the end of product life cycles. Stakeholders in the value chain and those affected by the transaction are demanding more sustainable production and greater transparency around supply chains. Making the traceability of goods more secure and having more salient information in production and in supply chains could be enabled through blockchain technology.¹⁷⁵ By tagging different inputs, for example minerals, materials, or chemicals, and assigning them with digital certificates on blockchain, they can be followed in a step-by-step, transparent, audible way, enabling more informed purchases along the supply chain and for the customer. Organizations that could spearhead such initiatives might be fair trade organizations, for example, aiming to increase transparency and accountability. Practices could also

173. <https://www.saveonsend.com/blog/bitcoin-money-transfer/>

174. <http://certificates.media.mit.edu>

175. <https://www.provenance.org/whitepaper>

be enforced by organizations that use conflict minerals or other contested inputs in their production. Policies could be formed to encourage manufacturers to use blockchain for storing production data and for increasing the transparency in the production.

Product traceability could improve the security and efficiency in health, pharmaceuticals, energy, financial services, food, aerospace, telecommunications, IT, transportation, utilities, agriculture, and oil and gas.¹⁷⁶ For example, many emerging economies are struggling with the extensive markets offering counterfeit medicine, and they are in need of reliable systems to certify the authenticity of the medicines sold. Likewise, with increased global flows and the exchanges of other goods and services, the demand for accountability is on the rise.

6.3 Evolving Governance Systems

With the rapid technological development of the past few years, which has further connected events, individuals, and systems globally, the interest in technical support and solutions for governance of global issues is growing. Businesses, nations, and global governance institutions are seeking governance mechanisms that can be adjusted for the modern world.

Blockchain technologies enable governance models where centralization of decision making and hierarchical structures are replaced by mechanisms of decision making by distributed consensus. Projects have already been developed for virtual cryptonations where governance services are entirely based on blockchain technology. These entities are borderless, voluntary organizations that offer alternatives in legal, social, diplomacy, and security services to traditional nation states. The notion behind them is that every owner of a private key can take part in a decision-making process, vote, sign legal contracts, and have access to services that traditionally are provided under the purview of traditional governments.

Several countries are starting to explore how digital technology could be applied to connect citizens to governmental services and to make business processes more efficient. Estonia, for example, has been at the forefront of digitizing governance and has over a thousand government e-services. Estonia is the first country in the world to offer a supranational e-Residency program, partly supported by blockchain technology. The project was started in 2014 by government officials with the aim of having 10 million e-Estonians by 2025.¹⁷⁷ In May 2016, over 10,000 Estonian e-Residents had established over 500 new companies and had become owners of over 1,000 companies registered in Estonia.¹⁷⁸ Kaspar Korjus, Estonia's e-Residency program director, explained the situation as follows:

176. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

177. <https://taavikotka.wordpress.com/2014/05/04/10-million-e-estonians-by-2025/>

178. <https://e-estonia.com/estonia-hits-the-10-000-e-resident-milestone/>

In Estonia, we believe that people should be able to freely choose their digital/public services best fit to them, regardless of the geographical area where they were arbitrarily born. We're truly living in exciting times when nation states and virtual nations compete and collaborate with each other on an international market, to provide better governance services.¹⁷⁹

E-Residency allows entrepreneurs and freelancers from all over the world to establish location-independent businesses online, apply for a bank account, conduct e-banking, get access to international payment service providers, declare taxes, sign documents and contracts remotely, and get easier access to EU markets.

The Estonian e-Residency program, in partnership with the virtual nation Bitnation, will use blockchain technology to offer a blockchain based public notary to e-Residents.¹⁸⁰ The partnership provides a legally binding worldwide proof of existence and integrity of contractual agreements, which can empower entrepreneurs and e-Residents around the world. The Bitnation public notary allows Estonian e-residents and Bitnation world citizens to notarize their marriages, birth certificates, business contracts, and other documents on the Bitcoin blockchain. Bitnation CEO and founder Susanne Tarkowski Templehof has said, "Bitnation is doing for identity and statehood, what Bitcoin is doing for money." Bitnation, as the world's first blockchain-powered virtual nation, provides "DIY governance services" and has received international attention for providing refugee emergency response, world citizenship IDs, pioneering marriage certificates, land titles, birth certificates, and more on blockchain. A long-term ambition by Bitnation is to provide dispute-resolution services using blockchain technology. The digital ledger technology company Guardtime, which has been working with the Estonian government since 2011, announced a partnership in March 2016 with the Estonian eHealth Foundation for securing health records used by the Estonian eGovernment infrastructure.¹⁸¹

E-residency governance services such as the ones spearheaded by Estonia and Bitnation have the potential to change the way people think about nations and citizenship. Also, in the event of natural disaster or war, where normal governmental services in a geographical region might cease to exist, property rights, contracts, and documents stored on a worldwide distributed blockchain ledger would still be intact and could potentially be recognized as an internationally authoritative record. Perhaps in the future, this could also apply to physical property (e.g., land titles).

In countries where election processes are corrupt and voters face security challenges, blockchain technology could provide voters with the safety of voting from their own homes or remote areas and still have a democratic influence. The same voting mechanisms as proposed for national elections are also of interest to shareholders

179. <http://www.ibtimes.co.uk/bitnation-estonian-government-start-spreading-sovereign-jurisdiction-blockchain-1530923>

180. <https://bitnation.co/blog/pressrelease-estonia-bitnation-public-notary-partnership/>

181. <http://www.coindesk.com/blockchain-startup-aims-to-secure-1-million-estonian-health-records/>

in publicly traded companies. Instead of missing out on the opportunity to vote or using a proxy, shareholders could directly vote in crucial company decisions through blockchain-based systems.

6.4 The Impact on National Currencies

If the predictions of many of the early adopters of blockchain technology are right, blockchain currencies could in time offer a competitive alternative to nation state currencies. Thus, through market competition, they could potentially have an impact on nation states' and central banks' ability to control monetary policy and set interest rates. Nation state currencies have significant competitive advantages due to network effects, but those could slowly be eroded with the continuance of negative interest rates, rapid monetary inflation, and increases in compliance costs and in debt levels.

The national currencies used in the world lost the last traces of backing by gold via the Bretton Woods system in 1971, when the unilateral cancellation of the direct convertibility of the United States dollar to gold took place.¹⁸² Terminating the restriction on monetary policy provided by a fixed link to a scarce physical commodity effectively meant that the central banks in the world were free to print as much or as little new money as they deemed appropriate (often euphemistically called quantitative easing). Expanding the money supply (primarily through credit expansion) through lowering interest rates gives incentives for increased borrowing and consumption and provides disincentives for saving. This has led to a situation where nearly 97% of all circulating money in the economy is now credit (IOUs) created by commercial banks on people's bank accounts, as explained by the Bank of England.¹⁸³ Most economists today argue that this system stimulates economic activity and creates more jobs. An opposing view on this – which adherents of the Austrian economic school hold and which the monetary policy of Bitcoin was originally based on – is that many jobs that are created through monetary expansion (diluting the purchasing power of savers) do not reflect the desire of society and cause inefficiencies in the economy.¹⁸⁴

Most cryptocurrencies have strictly regulated and predictable inflation. The amount of money circulated is predetermined in the protocol, controlled through computer code, and cannot be altered by anything less than a majority consensus in the community. This is quite different from the systems of quantitative easing that central banks deploy. The amount of bitcoins that will be issued is limited to 21 million, in this sense, making it similar to limited supply commodities like gold. The value of cryptocurrencies as mediums of exchange is set on the global free market based on supply and demand, where the supply side is strictly regulated through code and known at all times by all participants. If you purchase one bitcoin, you know for sure that you have at least one 21 millionth of the entire Bitcoin money supply that will ever exist.

182. <https://history.state.gov/milestones/1969-1976/nixon-shock>

183. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2499418

184. <https://mises.org/library/can-quantitative-easing-lift-economic-growth>

Like physical banknotes, bitcoins are a form of bearer instruments (not IOUs like the entries in digital bank accounts), meaning that holding the asset equates to owning the asset, and transfer of the asset equates to an instant change of ownership. Bitcoin and other cryptocurrencies are thus bearer instruments that can be settled digitally across large distances in an instant, without the limitations of physical notes requiring the transaction parties to be in the same physical location. Swapping two different native digital bearer assets on a blockchain can be done in a single-step operation without intermediaries. This unique property of cryptocurrencies as digital bearer instruments could be a key reason that central banks would want to issue their own cryptocurrencies.¹⁸⁵

In general, for something to be considered as money, it needs to function as a medium of exchange, a measure of value, and a way to store value. At least nine characteristics are important in this regard: limited quantity, durability, portability, divisibility, ease of recognition, ease of storage, fungibility, difficulty in terms of counterfeiting, and widespread use.¹⁸⁶ Some current features of Bitcoin that increase its chances of being adopted as a global currency are its low transaction costs, high anonymity, and no inflationary pressure. Meanwhile, features that could hamper its adoption include the absence of a legal tender status, the difficulty of obtaining bitcoins by the general public, high educational barriers, the absence of Bitcoin denominated credits, deflationary pressure, high price volatility, and cyber security issues.¹⁸⁷

Bitcoin as a currency can be thought of as price deflationary. If Bitcoin becomes a generally accepted currency, the value of bitcoins would theoretically increase over time. This means that the prices of goods and services would fall in terms of bitcoins if the productivity of the economy continued to increase, as more goods and services then would increase demand for bitcoins while the total supply of bitcoins would remain essentially unchanged. As stated above, the total number of bitcoins is limited and will never exceed 21 million. Actually, bitcoins can also be destroyed, simply by losing the keys controlling the address where they are stored or by sending them to an address that is not controlled by anyone. Anyone will still be able to see these inoperative bitcoins in the blockchain forever, but no one will ever be able to move them. The loss of bitcoins increases the deflationary nature of Bitcoin slightly, but this is of less importance than the overall growth of demand for bitcoins as the user base grows.

Economists influenced by Keynesian economic theory have argued that the price deflation of goods and services is bad for primarily three reasons.¹⁸⁸ First, it provides an incentive to save rather than to consume, and it reduces the incentive to borrow money. Second, the real debt burden of borrowers will increase over time; and third, they argue that nominal wage cuts would be difficult to implement. According

185. <https://medium.com/chain-inc/why-central-banks-will-issue-digital-currency-5fd9c1d3d8a2>

186. <https://tradeblock.com/blog/refuting-the-ecb-the-9-characteristics-that-make-bitcoin-money/>

187. <https://ec.europa.eu/jrc/en/publication/digital-agenda-virtual-currencies-can-bitcoin-become-global-currency>

188. <http://krugman.blogs.nytimes.com/2010/08/02/why-is-deflation-bad/>

to Keynesian economics, it is desirable to push down lending rates and expand the money supply to provide incentives for increased borrowing and increased consumption to increase economic activity and to create more jobs.

Bitcoin does not allow for inflationary control in a normal sense and is essentially deflationary in its nature. Most economists today would likely argue that both those features could be regarded as problematic if it were to be used as a national currency. However, it would of course be possible to create new blockchain-based cryptocurrencies with inflationary features. The main remaining question is about Bitcoin's potential impact in relation to fiat currencies: If the above issues pose a problem with Bitcoin as currently formulated and if it then could affect traditional currencies in a potentially harmful way, could this threat be regulated or controlled somehow?

First of all, Bitcoin is not a national state currency. In fact, it is not the same thing as a traditional currency at all – at least not more than e-mail is the same thing as national postal services. There are overlapping concepts for sure, but they do not completely cover each other's area of usability. There is most likely a role for each to play. Some proponents (e.g., those in libertarian circles) would like Bitcoin to completely take over the global financial market and act as the one and only currency for all value transactions. But most likely, due to the above issues and others (e.g., the influence of growing fragmentation in the cryptocurrency space), it will not be used in general as a complete replacement of fiat currencies. Thus, the issue of the lack of control over Bitcoin for any specific national state should not pose a larger problem than the actual lack of control that the specific state already has over any other foreign currency.

Bitcoin could potentially play a huge role in value transactions over the Internet, which of course could affect the role of other currencies in that aspect. The built-in efficiency of blockchain currencies such as Bitcoin could definitively spawn interest in streamlining the efficiency of traditional currencies, associated transactions, and service costs. Bitcoin could act as an enabling catalyst to the already ongoing digitization and streamlining of global trade. New growing industry areas, such as the Internet of Things, are currently seeking lower thresholds, micro transactions, and simpler trusted point-to-point value transactions. It could be argued that this trend of globalization is affecting the possibilities of inflationary control in local currencies, since increased accessibility to global trade further interconnects the involved economies. Regional market demand and supply could be less affected by regional regulatory influence if it is being increasingly interconnected with, and affected by, global demand and global supply. This is not a direct effect on currencies from Bitcoin in itself, since, if it exists, it is an effect connected to the Internet, globalization, and digitization in general. The remaining question is that if Bitcoin and similar cryptocurrencies coexist with traditional state currencies, solving different needs, would the deflationary nature of Bitcoin then be a problem? The incentives to borrow bitcoins could be low, but it is hard to see a threat in that when normal currencies can be borrowed instead. It could of course provide an incentive to save money in bitcoins rather than to consume, and in that way, it could also compete with traditional ways of saving. However, in a growing

global market, that kind of competition between assets of different kinds and from external sources is already present.

6.5 Challenges and Risks with Blockchain-Based Systems

Blockchain technology could enable efficiency improvements and contribute to more transparent governance mechanisms. However, a range of challenges are also connected to the widespread adoption of the technology, which needs to be considered.

Using a public blockchain is not without risk. Even Bitcoin should be considered as an immature experiment at this stage, and undiscovered bugs in the distributed system could potentially be exploited. As a currency, bitcoin and other cryptocurrencies are very volatile, driven mainly by speculation, and any promises of future exchangeability is dependent on it actually gaining traction in terms of demand derived from usability. The road to that kind of maturity is long, and many failures will occur along the way. Storing cryptocurrencies safely is also far from trivial and necessitates a high level of technical knowledge and understanding about information security. Ownership of cryptocurrencies requires safe handling and unique access to information in the form of private keys. If that information were lost through forgetfulness, computer failure, or theft, all digital assets controlled by those keys would also be lost without recourse. In an immature system, those requirements are imposed on the end user, which creates thresholds and induces problems. In a more mature system, ease of use and the needed security and stability could be built into evolved general practice and into tools to provide a higher abstraction layer.

Currently, more than 50% of the mining network is located in China. A majority of the mining hash rate is essentially in control of security and verification, and it constitutes the major voting power in terms of future development. This uneven distribution of computing power on a global basis evokes the question of whether a national actor could make policy decisions that could affect the entire network.

Blockchain technology and cryptocurrencies, as with other global digital phenomena, have evolved faster than they can be studied and adopted by most authorities, institutes, and companies. This fast and dynamic technology evolution may benefit society, but it can lead to societal costs in terms of technostress, exclusion, and segregation.

Concerns have particularly been raised regarding unclear regulation and guidance in the rapidly growing FinTech sector. If regulation is too strict or does not adjust fast enough, this could have negative effects on Sweden's growth and global competitiveness.¹⁸⁹ However, sometimes the lag of legislation in relation to technological developments can actually be positive, as it allows a deeper understanding of the real implications of the technology. Even if blockchains distributed nature is lauded by many, there might be situations where the lack of a trusted third party can be a

189. <http://digital.di.se/artikel/fintech-kraver-tydligare-spelregler>

disadvantage. In order to fully trust a system, at least one trusted intermediary who can make adjustments and regulate the system is often needed, for instance, when an automatic system has failed or when someone has maliciously exploited a previously unknown bug in a collaboratively designed solution. Anonymity and other inherent features raise new means to break laws and international agreements. Rules evolving in a global and completely distributed democratic fashion have a tendency to not fit into the regulatory requirements of states and other jurisdictions. However, organizations, companies, and people within those jurisdictions still have to abide by local rules. A system controlled by a trusted entity also abiding by the rules could therefore be potentially more effective than a publicly distributed system and could ensure that its use is kept within bounds and that it does not evolve outside of expected limits. Similarly, a privately controlled system could also be more optimized for the intended use than a large and general system. For those reasons among others, DAOs and similar solutions built on public blockchains – such as Bitcoin – would work well in theory but could perhaps end up being of small practical use and thus marginal phenomena as a whole.

Private blockchains would be able to provide the means for trusted central control. However, what can be achieved with private blockchain solutions may as well be implemented using more conventional database technologies. As an example, blockchain consortium R3 abandoned blockchain solutions and chose an alternative implementation of a private distributed ledger. The hype of Bitcoin has spread to a vast number of blockchain solutions for which it would have been easier to use a traditional database. Securing data by distribution is nothing new in itself. Git (the distributed versioning control system used by the Linux development community and many other open source communities) is a good example.

Another risk posed by blockchain technology is that it can challenge national security. RAND Corporation conducted an analysis in 2015 on the national security implications and the feasibility of deployment of virtual currency schemes by non-state actors, including terrorist or insurgent groups aiming to increase their political and/or economic power.¹⁹⁰ The report explicitly examined the deployment of new virtual currencies by non-state actors as a medium for illicit transfer, fundraising, or money laundering, as opposed to exploiting already deployed virtual currencies, such as Bitcoin. It noted that the trend toward decentralized Internet services is a two-way street that could enable unprecedented global access to information and communication services and that could be both beneficial and harmful to national security interests. As the technology becomes more sophisticated, mature, and easy to use, unsophisticated non-state actors could have uninterrupted access to Internet services, even if a highly sophisticated state actor deploys active countermeasures. This could have implications for national firewalls, access to extremist rhetoric, the

190. http://www.smallake.kr/wp-content/uploads/2016/02/RAND_RR1231.pdf

possibility of nation state cyber attacks, and the ability to maintain uninterrupted and anonymous encrypted communications.

A common critique of the processing in the Bitcoin blockchain is that it requires vast amounts of energy consumption to mine bitcoins and to keep the system going. It is not known whether the energy cost would be defensible in the long run in comparison with a life-cycle assessment of fiat currencies. A private blockchain would not necessarily require the same energy expenditure, since it could be controlled by trusted intermediaries. A less wasteful alternative for public blockchain implementations has yet to be found.

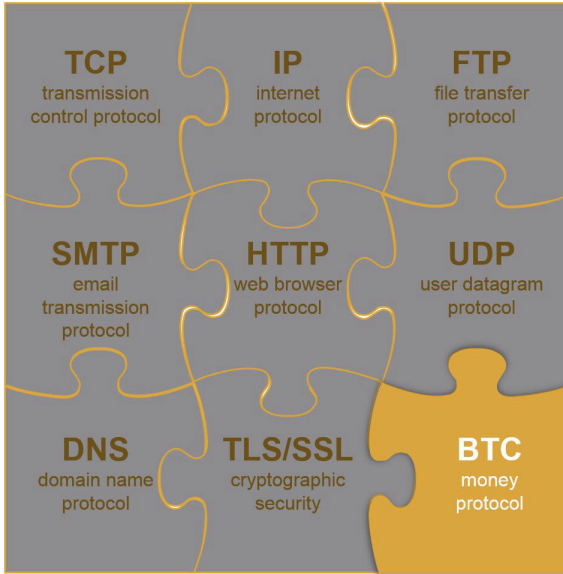
Bitcoin is frequently proposed as a trustable currency solution for developing countries, conflict zones, and areas where people are essentially unbanked. However, access to a stable network and power infrastructure is often not attainable in developing regions, which can instead be left behind by the fast uptake of technology. The necessary technology and knowledge transfer processes linking developing regions to more advanced economies are in many cases lacking.

7. Future Scenarios

Blockchain is sometimes compared to the invention of the Internet and the TCP/IP protocol. During the 1990s, expectations, investments, and the number of inventions were growing fast due to an increased understanding of the potential of the global network. The boom led to a speculative bubble, which burst into the Dot-Com Collapse of 2000. The IT boom and bust cycle left a plethora of startups, higher level protocols, concepts, and an infrastructure in its wake. These have since matured and grown into a complex network that fulfills and often exceeds many of the high expectations that fuelled the IT bubble. Today, these tremendous IT advances are taken for granted worldwide. TCP/IP remains a fundamental layer in the way it is being used on the Internet, but on top of it are higher abstraction level protocols. For instance, SMTP provides us with part of the worldwide email standard. A vast number of protocols, databases, and programming languages have been put together into content management systems and the like. These systems enable state-of-the-art solutions supplied on the World Wide Web of today. Looking at the whole system from the outside, these can be seen as abstraction layers; and for higher layers, it does not even matter if TCP/IP or something else is being used as the lower-level transport protocol. Similarly to TCP/IP, blockchain could be the next fundamental global layer of technology, providing us with a new vast number of possibilities built on top of it. Transaction of value is important in that context, but far from the only important possibility (Figure 17). With blockchain technology, the Internet could potentially be reengineered from the ground up to offer privacy, security, and inclusion. Attempts were made using cryptography to offer this as early as 1981, but they failed because intermediate third parties that could leak information could not be avoided at that time.¹⁹¹

191. http://www.huffingtonpost.com/don-tapscott/heres-why-blockchains-wil_b_10146610.html

FIGURE 17. Blockchain, the Missing Piece of the Internet Protocol Puzzle?



Source: <https://panteracapital.com/wp-content/uploads/The-Final-Piece-of-the-Protocol-Puzzle.pdf>

Considering the idea that we are currently at the early stages of a new possible IT boom nurtured by the blockchain technology development, it is hard to accurately extrapolate and make predictions concerning what the future abstraction layers will be. It is impossible to tell with certainty which solution will become “the golden standard” and which projects will have to be shut down along the way. To reach a deeper understanding, it can be helpful to conceptualize a future development based on the possibilities of the lower layer of blockchain technology that is already available. This chapter seeks to envision a future where blockchain technology has matured, become widely accepted, and grown into a fundamental technology for societal infrastructure. The chapter is not meant as a prediction, but as a basis for further analysis, where certain hypothetical implementations, applications, and consequences of such a scenario are explored.

7.1 Digitized Public Sector Scenario

The first exploration concerns how society could be affected by a greater implementation of blockchain technology. In 2016, digitization is already happening in most aspects of society. The driving factor behind this trend is that individuals and organizations benefit from connections and information flowing faster across physical boundaries. This facilitates interactions between fast-growing numbers of digital entities, not bound by physical limits. In this scenario, the concept of a mature digitized public

sector underpinned by blockchain technology is explored. In the envisioned society, people will spend more time in the digital world than they do in what will by then be called the physical space. Blockchain could potentially be used to better optimize and automate processes such as planning, organization, and decision making in public authorities and registries.

POPULATION REGISTRATION AND PERSONAL IDENTIFICATION

Sweden's personal ID number system was changed in late 21st century. Since then, each registered individual, organization, and other kind of entity is handed a unique personal identification number (PID). PIDs are constructed in a way that the supply cannot reasonably run out. There are billions of entities, most of which are non-human, since distributed automated algorithms are multiplying faster on their own. For people to interact with authorities and with each other within the jurisdiction of society, a PID is required. Using a PID as a seed, an unlimited number of asymmetric key pairs can be generated by or for the entity who owns it. Keys may also be revoked by either authorities or the owner. A web of trust concept, with entities – including authorities – signing each other's keys, creates bindings between public keys and their owners. This way, a PID can also act as a kind of master public key, automatically connected to more dynamic physical and virtual addresses, accounts, legal rights, and so on. PID numbers, signatures, interactions, and activities are stored in a blockchain. Thus, the blockchain is the basis for population registration and offers a built-in means for population registration certificates and virtual ID cards.

JURISPRUDENCE

General jurisprudence involves the study of legal source code. That is, legal code has turned into software legal code, where both laws and contracts are created through programming. The blockchain forms the legal system framework, as civil laws and regulations are written in code and signed and issued by corresponding authorities. All agreements are made as smart contracts in the blockchain, which are legally binding when signed by parties and included in the ledger and executed at all times according to the framework made up by laws and regulations that are also stored in the blockchain. Any binding interaction ever made within the jurisdiction of the blockchain law will be forever time-stamped and written into the history archives of the very same blockchain system. Most disputes are settled automatically by the pure distributed execution of the code. Those disputes that lead to court actions and trial verdicts are used to guide new legal practice and to fine-tune the legal source code in interpreting law.

PUBLIC INFORMATION, PRIVACY, AND INTEGRITY

The public sector blockchain is public, which guarantees that the principle of public access (Swedish: Offentlighetsprincipen) is upheld. By default, all interactions involving public sector entities are stored in clear text or unencrypted source code. When committed, each interaction automatically goes through the scrutiny of certified processes

and coding practices. When the stipulations of such processes and practices are not met, committed interactions are simply not accepted into the blockchain ledger and are thus not legally binding or accepted within the law code framework. All classified interactions are also committed, abiding by the very same rules – the difference being that they are encrypted as part of the process. Encrypted classified information always has a timed or event-based deadline, at which the encryption key is automatically published, making the information publicly available. What this means in layman terms is that authorities may still classify information, deeming it secret, but the decision to do so has to be done in blockchain as well, ensuring data integrity, traceability, and accountability for the future. Many concurrent methods are in use to ensure individual privacy and integrity. Knowing an entity's PID gives access to a lot of information about that entity and its activities. The vast number of possible PIDs makes it hard for anyone not involved with an entity to figure out its PID. Some sensitive information is kept encrypted such that it is readable by authorized eyes only, and some information is kept in sidechains or external archives. That provides the possibility of linking data in the system to, for instance, top secret data that has to be stored in an offline system or to move assets from the Swedish system to another authoritative linked system.

TAX AGENCY

Bookkeeping rules, like all other rules, have algorithmically been implemented in the blockchain. All financial interactions, asset exchanges, and all business events occur in the blockchain. This completely automates bookkeeping for all entities and has removed the need for fiscal years and reporting, since any financial statements or reports are readily available in real time. When digitizing taxation rules and moving them into blockchain, the system is constructed so that the appropriate tax deduction is made at each payment/exchange between entities depending on the nature of the interaction and continuously yields a flow from all taxed assets. Also the enforcement authority (Swedish: Kronofogden) has been fully automated, simply by restraining ownership of any asset in blockchain. This has been made possible since ownership is defined by which registered key – indirectly, the PID – is associated with an asset.

After digitizing its currency, the Krona, and implementing the new code law system, including automated taxation, Sweden ended up with a tax agency having relatively few employees and low administrative costs. Economic crime diminished into a minor issue. Since funds and assets are all accessible and accounted for via blockchain, inherently only using legal means, accounting fraud or tax evasion is simply not easily possible. The state did find it necessary though to install a handful of tax agents to continuously help in finding, analyzing, and closing the few loopholes in the organization registration and taxation system, which are periodically found and exploited by algorithmic trading companies.

With a long history of public sector infrastructure investments, the Nordic countries were among the first to invest in implementing a completely blockchain-based system. This made way for an efficient business climate; suddenly, entities from all over the world were inclined to move their assets and operations to the new jurisdiction,

accepting higher tax rates in exchange for the profitable gain of completely eliminating all administrative costs. The advantage and prosperity that followed in the region made it harder for other nations to follow swiftly, which gave the term tax haven a completely new meaning in the global debate.

BANKS AND LAW FIRMS

In the beginning of the blockchain boom, which was powered by the invention of cryptocurrencies, banks had to redefine their *raison d'être*. This had traditionally been the role of a trusted third party. Many people speculated that banks were to become obsolete in the upcoming digitized financial era where blockchain could eliminate the need for trusted intermediaries. However, after the whole maturing process and with the newly evolved legal system in place, banks are still essential to a prosperous society, though their roles have been altered. There is no money to be earned from transaction fees, running asset exchange platforms, selling derivatives, structured products, or any other middle man activities or oligopoly-based services that have been conveniently taken over by blockchain and decentralized commerce. The demand for financial services, such as loans and credits, overdraft agreements, safekeeping, escrow, and trade facilitating services, has nonetheless never been higher, due to the recent years' explosion of self-driving micro-businesses. But the previously unexpected main income for banks that survived the burst of the blockchain bubble is from providing real-time assistance in generating business agreement code. To create a controllable line of trust, only entities such as banks accredited by financial authorities have the right to sign legal agreement applications on behalf of their clients. The second largest income is from data banking and secure hosting of localized sidechains. During the time when law code was turning into real code, law firms started merging with engineering and programming companies to adapt. Later, banks started to acquire law firms to build and sustain their business agreement services. Now, there is no difference between them; bank APIs is where anyone would turn when in need of trusted and authority-accredited development services or agreement design services.

DEMOCRACY, GOVERNMENT, AND VOTING

Sweden has become a democracy in which every sentient entity that is mature enough and authorized for voting can participate. Since humans started using technology to improve their mental abilities, and since physical and virtual robots started coming close to mimicking human behavior, age as a means to determine maturity was deemed deprecated. Instead, a maturity test was implemented as smart contract code in blockchain, assessing the aspects of both psychology and knowledge. Any entity of any age and any kind has the right to take the test at any time. Test results are automatically stored in blockchain and immediately affect the rights attributed to the associated PID of the entity. So far, no other entities than humans have become eligible for voting, but some AIs are getting very close to passing those parts of the test. Instead of the ancient bottleneck governmental structure of the early decades of the 21st century, where authority was handled by a few people, blockchain technology

provided new means for a system that has the ability to keep up with real-time data flow and to continuously adapt to exponential development. A dynamically changing group of 100,000 people, representative of the voting population at all times, is collectively running the government. The number was chosen to vastly improve combined mental processing power and at the same time to give a true statistical representation of the will of the people, without actually involving everyone at all times. Government duty is a mandatory part of the requirements for all who choose to participate in politics by coming of age, taking the maturity test, and thereby making themselves eligible for voting. Every single authorized individual is participating part time whenever their PID is called upon by the governmental algorithm that is embedded in blockchain code. Participation most often involves reading up on a specific subject, analyzing the consequences of a particular decision, and voting for or against. Tasks are distributed by the governmental algorithm, and voting is done via blockchain. This makes the whole process completely transparent and protected from manipulation. Anyone can verify that each vote has been made only once. Anyone can verify the voting result. A participant can easily see his or her own vote and that it is accounted for. There are no politicians, but of course there is an open public debate discussing topics deemed relevant. The most respected discussion forum is implemented in blockchain, where articles and comments are signed by their authors and the whole debate history is recorded for all to follow. Collective effort controlled via blockchain also provide utilities, data analysis tools, and AI search agents for assisting in knowledge distribution and assessment.

7.2 The Hive Scenario

The next future scenario to explore, the Hive, is an idea relating to how people (and other entities) use the evolved Internet and blockchain technology as a communication platform and what that platform could look like. It could be regarded as a future replacement for the social media we see today (e.g., Facebook, LinkedIn, Twitter, Instagram, and Snapchat) and various messaging systems (e.g., Hangout, Messenger, and WhatsApp). The main difference is that the Hive is one single platform continuously evolving according to its users' wishes, completely distributed and neither owned nor controlled by any single entity. Due to its democratic, evolving nature, a platform like the Hive will most likely also include elements such as distributed marketplaces and auctions, replacing the platforms of today (e.g., Alibaba, Amazon, Ebay, Blocket, Craigslist, and Tradera).

BEEHIVE ORGANIZATION AND BUSINESS ADMINISTRATION

The Hive is a DAO. As such, there is no board of directors and no president. Central management, known as the Queen, is a set of business rules in code implemented as smart contracts in blockchain. The Queen code can evolve and change over time by the continuous addition of new smart contracts. Within the encoded mission statement framework rules, the Queen can rewrite its own code. It may for instance generate

revenue, employ other entities, and pay for its own code execution infrastructure. The Hive business rules, including the mission statement, can also be changed via democratic decision by participants, using the process of consensus forking. Since all code is open source and running transparently in blockchain, anyone at anytime can copy the full set of code, modify it, and start a new forked branch. Users, via current consensus rules, determine which branch to continue on. The winning branch inherits all funds and the legal status of the Hive.

PARTICIPATION AND COMMUNICATION

Users participate simply by signing their activities and submitting them to the Hive blockchain. Many different types of activities are defined by the Hive framework rules, ranging from communication activities (e.g., sending a message to another entity) to administrative activities (e.g., linking multiple authorization key tokens to each other and identifying them as belonging to the same user). There is no need for a central user database registry of usernames and passwords, nor user profiles or similar. Since all activities made by a user can be linked in time to that particular user, different kinds of views (e.g., timeline, profile, images, and message history) are just a matter of the visualization perspective of different searches through the data. Users validate each other through common activities, so a web of trust emerges in time that links users to their activities and provides a reputation network.

COST OF PARTICIPATION, CURRENCY, AND SPAM PREVENTION

Since no business runs and controls the system, no fees or mandatory costs are involved; neither are there any mandatory commercial ads or the like for financing the system. There is a built-in cryptocurrency in the Hive named Nectar (through which a vast number of third party providers are linked to the smart contract API), and the Queen is interconnected with other currencies, cryptocurrencies, and value systems. Value and assets of different kinds effortlessly change hands between entities in the exchange flow provided by the Nectar. Inherently, all users and all activities may be interlinked with more or less Nectar, including activities involving the Queen or other autonomous entities.

Each user is in control of his or her own connection points. This means that each user can exclusively decide which interfaces can be used (and by whom) to interact with them and associate those interactions with their own rule set. Since all those rules are available in the Hive blockchain, any other entity can scrutinize and may even simulate results before taking any interactive action. For example, a default cost in Nectar is involved in messaging, paid by the sender of any message. The default cost, which can be changed in special cases but is left as is by most entities, is set to such a low number that the impact for a normal user is negligible. Even when sending more messages than receiving on average, the cost would be inconsequential during a whole year. It is however set high enough to effectively prevent spam, since any entity trying to send messages to a vast number of users would very quickly face large summarized costs.

7.3 The Cooter Scenario

Next is a scenario exploring an extreme sharing economy based on blockchain technology. The vision entails a future in which nobody, not persons nor companies, owns their own vehicles (i.e., cars, motorcycles, boats, ships, trains, airplanes, trains, helicopters, and hovercrafts). Instead, whenever the need for personal transportation or delivery arises, Cooter (the conveniently named conveyance origin order transporter) is invoked and solves the need. Cooter, a blockchain-based system to control all vehicles and infrastructure, replaces privately owned transportation devices, post offices, taxi services, travel agencies, couriers, railway companies, and so forth.

THE CONVEYANCE HUB

During the second part of the 21st century, the total amount of autonomous vehicles exceeded the number of manually driven vehicles, and the gap continued to increase in an exponentially growing pace. By the end of the century, human drivers were finally completely forbidden due to their slow reactions, unpredictable behaviors, and inability to cope with all the simultaneous interactions and data streams needed for planning and reasonable safety. After that, traffic could be vastly optimized in terms of space, punctuality, cost, and travel times. A general traffic organizer, Cooter, was implemented as a computer-planning algorithm running on a distributed blockchain virtual machine. Cooter is the one and only manager of traffic, completely controlling specifically dedicated airspace, landspace, and seaspace, collectively named the transferspace, and driving everything within. Authorities can bind areas of transferspace via blockchain with restrictions for environmental reasons to minimize disturbing noise, and similarly, to force Cooter to take all requirements into account in its planning engine. This way, regulations on exhaust gas limitations, for example, can be directly controlled, instantly implemented, and fully and verifiably adhered to in real time. Invoking Cooter from a user perspective is easy. A signed blockchain message containing the requirements of what is to be moved, where, when, and other needs, is simply sent to Cooter. Various apps, web pages, and other user interfaces targeting different needs in different situations can be used to further simplify generating those requests. Requests are automatically processed in an optimal way by the planning engine, and funds are withdrawn from the origin address of each request.

Based on blockchain technology, Cooter runs with a vast amount of processing power (running on 100% renewable energy of course, since power distribution is also regulated through blockchain). Also, the code executes with total redundancy, since no single hardware failure, local power outage, or node error can affect the end result. Immutability and traceability of blockchain technology makes the system secure against hackers and external threats. The very same features also make it easy to track and investigate the exact cause within the system each time something unexpected happens. Effectively, failures and accidents diminish into a minimum. The users of the system find it puzzling and almost incredible that thousands of people used to die in traffic each year due to human errors. The fact that human control issues led to

decades of resistance against automated transportation seem even more questionable when looking in the rearview mirror.

VEHICLES AND INFRASTRUCTURE

Back in the days when vehicles used to be managed by people, they were also very well categorized, and different vehicles for different purposes were easily distinguished. Airplanes were airplanes, trains were trains, and cars were cars. Originating from a time when customized on-demand single-item production techniques (e.g., 3D printing) started taking over from mass production facilities, devices also started taking in a more unique form. The phenomena accelerated when humans no longer needed to make choices themselves; there are no simple categories of vehicles anymore. Vehicles and transportation devices come in all shapes and variants in different sizes and with different infrastructure for land, sea, and water, with hybrids of different kinds. Based on Cooter's calibrations for how to optimize the service in relation to the demand, new devices were automatically specified, manufactured, and put to use on the fly. Each machine is unique, with no design looking like another. The only few common denominators for all moving machines are the control and user interfaces, connected to Cooter via blockchain on one end and open for booking requests and other needs on the other end. Another commonality is an autonomous driving feature as a fallback when the Cooter connection is lost and for rare occasions when a traveler ventures outside of the Cooter transferspace. Being in full control of the transferspace and its infrastructure, Cooter can fill all available land, sea, and air in an optimal way at all times. Optimized in that way, transferspace itself never needs to take up more room than exactly what is needed. Since Cooter was implemented, more air, land, and water have been made available for nature and living space.

SHIPPING, COURIER, AND FREIGHT SERVICES

Since moving physical objects is not very much different from moving physical beings, Cooter handles these services as well. Small quadcopters can be used for delivering small items point to point, and larger drones of different kinds can deliver larger items. The system chooses the right conveyance method depending on size, timing, fragility, frequency, and so forth. A distributed planner makes the process highly efficient as it replaces multiple competing smaller entities that lacked the whole picture with all its different complexities and interdependencies.

7.4 Reflections Concerning Future Scenarios

In the digitized public sector scenario, a new personal identification numbering system using blockchain was explored. It was also expanded to allow more and different kinds of entities than the system of organization numbers and personal numbers of today. Using blockchain technology, it is possible to arrange public registers so that connected routines could be automated and more efficient. The application for a new company organization number could potentially be automated and finalized in minutes.

One country that has already recognized the potential of new types of digital id-registrations is Estonia, which has created the e-Estonia program, offering world citizens an e-Residency with digital identifications and the possibility of digitally entering contracts and starting organizations within their jurisdiction. More similar concepts will most likely be developed and offered by nations and organizations in the future. Blockchain technology could very well be only part of the technologies needed to make it plausible. Sweden has a long history of recognizing the value of early adoption and facilitation of technological inventions. New infrastructure has received support, such as the early broadband rollout all over the country. In a developing global digital market, the facilitation for algorithmic organizations could similarly affect economic growth in a jurisdiction.

A historic blockchain market bubble is mentioned in the public sector scenario. This can be seen as a reference to the IT bubble that burst around the turn of the millennium. Blockchain is a hyped term at the moment. For instance, vast amounts of venture capital are being funded into start-ups using blockchain and/or Bitcoin in their business ideas. As in the case of the IT bubble, there is always a risk that the hype can turn into a bubble based on expectations that are too high too early. Blockchain is in many ways not yet a mature technology. Bitcoin, which is currently the largest application, still has its demand mostly driven by speculation and not by actual usage. There have already been several big company failures, such as Mt. Gox in Tokyo, just recently KnC Miner in Sweden, and Bitfinex in August 2016. Many successes, mistakes, and failures are likely along the way until the technology matures and becomes more widely used.

The Hive scenario depicts how people may interact with each other in the future. The Internet has completely changed our communication habits. E-mail partly ousted the need for sending letters and vastly improved the speed and cost of everyday point-to-point written messaging. Web pages did the same, as anyone is now able to publish information and make it available to everyone else. Postal companies have been affected, and so have newspapers and other traditional media. People have also started interacting with more than written messages. File sharing has affected a whole industry of music and video. Blockchain and cryptocurrencies such as Bitcoin have similarly started to affect banks and financial institutes, and is a part of the global digitization affecting the entire financial system.

For communication platforms and data aggregation on the Internet, proprietary solutions have in some cases come further at the moment than globally shared and open protocols in terms of winning market shares. Larger players such as Google and Facebook still very much define the social media space globally. The underlying requirement has been that a trusted party handles shared data storage online for users that communicate with each other. These trusted companies also act as authorized central authorities for their users, setting up rules, fighting unwanted content, and so on. The Blockchain technology of today might not be mature enough to replace all these advantages enough to win over the market, but it definitively adds functionality and potential in that direction.

What blockchain enables in the concept of the Hive, compared to the large messaging and digital service platforms such as Facebook and Google, is that the platform does not have to be run as a private profit-driven company. Neither does it have to be run on centrally controlled computer resources. There are already interesting projects in DAO development, for example, making use of the Ethereum blockchain for related purposes. One simple example is EtherTweet, which is an already existing distributed proof-of-concept alternative to Twitter. Global search and point-to-point as well as group communication could be run in the future as shared code on globally shared computer processing infrastructure. However, the possibility of DAO implementations will most likely not remove private ventures. Instead, they will probably coexist to some extent, offering different pros and cons in different situations. Of course, problematic issues will also have to be handled when autonomous organizations grow more common. Sooner or later, distributed companies will start affecting privately held companies in different industries, which raises many questions. Since they do not have a specific geographic locality, where should they be taxable? How can rules and regulations be enforced in the DAOs and in which jurisdictions? Who is responsible for their actions, when there is nobody in central control and no known founder? Global digitization will most definitively continue to affect more aspects of our society, and blockchain technology will likely provide some of the enabling infrastructure in the transformation.

The Cooter scenario is another example of blockchain technology's potential in replacing intermediaries. It illustrates the possibilities of optimizing systems by using centrally distributed management, for instance, in a blockchain. Efficiency gains can be achieved when it replaces multiple competing sub-control systems. Thereby, blockchain technology provides a means for distributed central control without any single entity actually acting as the central control. Reasonable mechanisms for authorized regulatory input can be used and also verified via blockchain.

These future scenarios are all pretty extreme and explore far future extrapolations of what blockchain technology could be used for. Even though these explorations in some way relay a sci-fi feeling due to their nature, it does not mean that big breakthroughs due to blockchain technology have to be far away. The development we can see is happening here and now, and it is happening at an astoundingly fast pace.

Blockchain technology is developing in parallel with many other technological breakthroughs, and it is likely that they will converge, affect, and replace each other. The infrastructure of today's blockchain technology may very well form the basis for developments, improvements, and new solutions in the coming years. It is very possible that the technology will not even be called blockchain at the point at which it will be used on a larger scale or in other implementations built on top of it. Thus, in all likelihood, the future will not look like the one described in the scenarios; but hopefully, they can serve as inspiration or guidance in terms of the potential of these very first stages of the implementation of the new technology.

8. Policy Measures to Spur Further Innovation

Blockchain technology and its potential applications are not easily regulated by the existing legal frameworks. The technology can make significant contributions to the distribution of welfare, more efficient taxation, and transparency in international transfers, but it can also be used for creating economies largely outside of government control or for criminal activities. Policy makers need to balance the support of the ecosystem that can enable positive solutions with regulations that limit the potential negative consequences. Since an application of the technology (Bitcoin) at an early stage was used as a means for trading drugs and illicit goods online, it has not been uncommon among policy makers to advocate a ban of the usage of the technology. Since the technology consists of a decentralized global network using open source software, it is, however, practically impossible to shut down. Banning the usage might thus hinder the positive outcomes that the technology might contribute to, without actually preventing the negative usage.¹⁹² Governments that might attempt to shut down or hinder the uptake of the technology might even put themselves at a competitive disadvantage.

Deciding about the right balance between governance and regulation and between legal code and technical code will require multidisciplinary collaboration between IT experts, lawyers, data scientists, user groups, and policy makers. Platforms for these types of interactions, such as test beds, can be offered by policy makers who intend to spur innovation in the field. Opening up data sources in the public system and even allowing certain transactions to be directly stored and registered in blockchain technology can open the way for more cocreation and further advances. By openly sharing and publicizing the outcomes as well as the challenges of such initiatives, policy makers can contribute to broad learning and understanding of the technology.

Blockchain technology is still in its very early stages but offers possibilities for entrepreneurs, business leaders, and innovators that are interested in pursuing the creation of applications and further developing the technology. The common knowledge about the technology is still limited, and expertise in the field exists in silos. Policy makers could play an important role in increasing awareness of the technology and its potential for

192. http://mercatus.org/sites/default/files/GMU_Bitcoin_042516_WEBv2_0.pdf

enhanced transparency, accountability, and effectiveness in transactions. By sharing knowledge about blockchain technology, through reports, seminars, and match-making among relevant actors, the potential of the industry could be further unlocked. The universities in Sweden could play an important role in the development of the technology, just as they did in the early stages of the Internet, by allowing research and experimentation based on blockchain. Incubators or accelerators could be established to allow new initiatives making use of blockchain technology. Vinnova, Sweden's Innovation Agency, could issue grants specifically targeting the potential applications of blockchain, for example, for the welfare system and international aid transfers.

The development of blockchain infrastructure is also dependent on talent to develop the systems and to write the code needed for the different applications. Talent development through tailored education programs, advanced research, and facilitated global mobility programs can be of great value for Sweden in strengthening the national expertise in blockchain technology.

Municipalities could launch challenges and competitions to identify the most efficient and impactful applications of blockchain technology in society, thereby driving both the interest and engagement of different actors to identify both problems and potential solutions. As an example, the National Aeronautics and Space Administration (NASA) in the United States successfully organizes innovation challenges on an ongoing basis to engage external research institutes and the open community in solving challenges in technology development.¹⁹³

Another way of supporting innovation in and based on blockchain technology could be to prepare for a faster decision-making process, especially as development is not expected to slow down. Faster analysis of global change and proactive implementation of more dynamic processes could facilitate innovation that gives favorable environments and economic growth.

With regards to money-transmission licensing, governments can choose to either craft new policies completely focused on regulating virtual currency transmissions or to adjust existing regulations to also take blockchain alternatives into consideration. The existing regulatory barriers need to be revisited, but as the digital currencies are still at a very early stage, policy makers need to be cautious with regards to their usage to avoid hindering potentially positive developments and inadvertently spurring unwanted developments.

As the technology evolves, the government could play an important role in setting standards to ensure the robustness of the distributed ledger systems and to ensure a clear understanding of the accountability in the system. Security, privacy, and integrity will also have to be defined in the framework of standards to facilitate an efficient use of blockchain in coming applications. The standards will need to be adopted on an international basis, given blockchain's distributed character, and collaboration with international counterparts will be vital for interoperability.

193. <https://www.nasa.gov/offices/oct/openinnovation>

9. Conclusions

Blockchain has a transformative potential in terms of businesses and societal functions. The technology could in many areas allow the transition from centrally controlled hierarchical structures to decentralized peer-to-peer organization and interactions. Global network-distributed consensus algorithms can eliminate the need for trust between parties, offering the Internet an additional functionality level with significant implications.

Blockchain puts every user on the same level playing field as a peer in the network. It can be regarded as a global spreadsheet, or an incorruptible digital ledger, where not only financial transactions but also ownership rights and legal documents can be stored. Blockchain technology can also contribute to improved mechanisms for governance. If public institutions enable the registration of property titles, business licenses, educational degrees, birth certificates, and so forth utilizing blockchain technology, citizens could perform transactions that today require lawyers, notaries, banks, and government paperwork.

Blockchain technology promises to fundamentally change how data can be transacted, accessed, stored, and secured. The compromises of centrally controlled databases can become a thing of the past, and the critical computational infrastructure that controls vital societal functions, such as energy, water, sanitation, and defense, can be built without the risk of single points of failure or control.

As the technology is still in its nascent stages, regulations need to both enable innovations based on blockchain and to restrict potential illicit use. The government agencies that at first point of departure could benefit from monitoring the developments are financial regulatory bodies and tax authorities. With the current momentum and development trend in blockchain technology, nations that remove barriers for experimentation around smart contracts and peer-to-peer solutions may benefit from the progress of entrepreneurs and ventures built on top of blockchain. Countries that hinder its development may lose out on the first-mover advantage to jurisdictions that are more permissive.

Blockchain technology is complicated, requiring an advanced understanding of computer science, peer-to-peer network technology, cryptography, and economics. Few people in the world currently have a good understanding of how this technology functions; systems and nations that might benefit the most lack the capacity in many

cases to take full advantage of the technology's potential. The technology is free and open for anyone to use, build upon, improve, and come up with new applications and use cases. It will likely take many years, and many improvements to the user experience are needed, until we see mainstream adoption of more mature blockchain technology.

Even if many of the benefits of blockchain lie in its decentralized structure, new bodies might be needed to assure standards in terms of how data is added to the system and how contracts are written. This role could potentially be filled by the same financial intermediaries responsible for storage of information involving transactions today.

The ecosystem around blockchain is developing rapidly among early adopters, which includes developers, activists, and technology enthusiasts. If this development could also be applied to core societal functions at an early stage, it could contribute to reducing information asymmetries and transactions costs, benefitting citizens directly. To enable the potential of the technology to be fully harnessed, businesses, entrepreneurs, government agencies, and individuals should be encouraged to follow the development of this new technology and to explore the new functions that it enables. The insights may contribute to better organized societal functions, more cost-efficient transactions, better protection of data, and innovations for nations and entities on the quest to stay globally competitive. The technology obviates the need for trusted intermediaries as well as the need to trust counterparties in economic transactions. Blockchain represents a breakthrough in computer science that enables a robust decentralized global system for the verification of actual transactions that are auditable by anyone in real time. If it continues to evolve similarly to the progress that has been witnessed for other Internet protocols, it will most likely be highly impactful for businesses and society

Om författarna

David Bauman

Tre års arbete med blockchain som HW Development Manager hos KnC Group VD och grundare av Xelmo AB. Grundare av Theedge Solutions samt Refo. Civilingenjörsexamen i industriell ekonomi och mekatronik vid Kungliga Tekniska Högskolan.

Pontus Lindblom

Fem års studier av Bitcoin och blockkedjeteknik. Civilingenjörsexamen i teknisk biologi och disputerad forskare vid Linköpings Universitet.

Claudia Olsson

VD och Grundare Exponential Holding AB, Associate Faculty Singularity University European David Rockefeller Fellow vid Trilateral Commission. Tidigare ämnessakkunnig vid Utrikesdepartementet. Civilekonomexamen Handelshögskolan i Stockholm. Studier i industriell ekonomi vid Kungliga Tekniska Högskolan, INSA Lyon samt Universitat Karlsruhe, Graduate fran Singularity University Graduate Studies Program.

Acknowledgements

We wish to extend a thank you to all the kind supporters and sources of wisdom and knowledge that have made this report possible. We are grateful to Johan Eklund, Pernilla Heed, and Pernilla Norlin from the Swedish Entrepreneurship Forum. They have made this report possible and have provided valuable insights throughout the process. We are also most grateful to H. R. H. Prince Daniel and Magnus Billing for their encouragement in writing this report. We would also like to thank Vitalii Demianets, Anna Fellander, Stefan Folster, Jeremias Kangas, Trace Mayer, Anish Mohammed, Susanne Tarkowski Tempelhof, Robin Teigland, Johan Toll, Charlotta Tullila Persson, and Roger Ver, who have shared their understanding of the field. This report would not have been possible without the support from Ulrika Englund, Maximilian Richter, and Sophia Wallin, who provided outstanding input in the writing process. It has been a true pleasure to meet and learn from all the visionary thought leaders in the writing process.

References

- ABA Journal (2013). Some basic rules for using 'bitcoin' as virtual money. Retrieved September 5, 2016, from http://www.abajournal.com/magazine/article/some_basic_rules_for_using_bitcoin_as_virtual_money
- Ali, R., Barrdear, J., Clews, R., & Southgate, J. (2014). The economics of digital currencies. Bank of England Quarterly Bulletin, Q3. Retrieved September 5, 2016, from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2499418
- Back, A. (2002). *Hashcash-a denial of service counter-measure*.
- Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., et al. (2014). Enabling blockchain innovations with pegged sidechains. Retrieved September 5, 2016, from <https://www.blockstream.com/wp-content/uploads/2014/10/sidechains.pdf>
- Badev, A. I., & Chen, M. (2014). Bitcoin: Technical background and data analysis - FEDS Working Paper No. 2014-104. Retrieved September 5, 2016, from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2544331
- Barlow, J. P. (2016). A Declaration of the Independence of Cyberspace. Retrieved September 20, 2016, from <https://www.eff.org/cyberspace-independence>
- Baron, J., O'Mahony, A., Manheim, D., & Dion-Schwarz, C. (2015). *National Security Implications of Virtual Currency*.
- Rand Corporation. Retrieved September 5, 2016, from http://www.smallake.kr/wp-content/uploads/2016/02/RAND_RR1231.pdf
- Beaumont, K. (2016). You, your endpoints and the Locky virus. Retrieved September 5, 2016, from <https://medium.com/@networksecurity/you-your-endpoints-and-the-locky-virus-b49ef8241bea>
- Bie, N. (2016). The Bitcoin Formula: Energy / Time = Truth. Retrieved September 5, 2016, from <https://webonanza.com/2015/10/12/the-bitcoin-formula-energy-time-truth/>
- BIS (2015). Digital currencies. Retrieved September 5, 2016, from <http://www.bis.org/cpmi/publ/d137.pdf>
- Bitcoin - GitHub. Retrieved September 5, 2016, from <https://github.com/bitcoin>
- Bitcoin ATM Map (2016). Countries. Retrieved September 5, 2016, from <https://coinatmradar.com/countries/>
- Bitcoin Charts (2011). Markets. Retrieved March 22, 2016, from <http://bitcoincharts.com/markets/>

REFERENCES

- Bitcoin Charts (2013). Bitcoin Network. Retrieved September 5, 2016, from <https://bitcoincharts.com/bitcoin/>
- Bitcoin Foundation (2012). Retrieved September 5, 2016, from <https://bitcoinfoundation.org/>
- Bitcoin Magazine (2015). Blockchain Technology: The Key to Secure Online Voting. Retrieved September 5, 2016, from <https://bitcoinmagazine.com/articles/blockchain-technology-key-secure-online-voting-1435443899>
- Bitcoin Magazine (2015). Is Bitcoin Headed for a Break in Fungibility? Retrieved September 5, 2016, from <https://bitcoinmagazine.com/articles/is-bitcoin-headed-for-a-break-in-fungibility-1450823559>
- Bitcoin Magazine (2016). Sweden Conducts Trials of a Blockchain Smart Contracts Technology for Land Registry. Retrieved September 5, 2016, from <https://bitcoinmagazine.com/articles/sweden-conducts-trials-of-a-blockchain-smart-contracts-technology-for-land-registry-1466703935>
- Bitcoin News (2016). Is Ghana Showing the Most Interest in Bitcoin?. Retrieved September 5, 2016, from <https://news.bitcoin.com/ghana-interested-bitcoin/>
- Bitcoin News (2016). Meet the Top 3 Coins in the Cryptocurrency Anonymity Race. Retrieved September 5, 2016, from <https://news.bitcoin.com/meet-top-3-coins-cryptocurrency-anonymity-race/>
- Bitcoin News (2016). Switzerland Won't 'Obstruct' Bitcoin Startups. Retrieved September 5, 2016, from <https://news.bitcoin.com/switzerland-eases-bitcoin-regulations/>
- Bitcoin Wiki (2014). Altcoin. Retrieved September 5, 2016, from <https://en.bitcoin.it/wiki/Altcoin>
- Bitcoin Wiki (2015). Donation-accepting organizations and projects. Retrieved September 5, 2016, from https://en.bitcoin.it/wiki/Donation-accepting_organizations_and_projects
- Bitcoin Wiki (2015). Multisignature. Retrieved September 5, 2016, from <https://en.bitcoin.it/wiki/Multisignature>
- Bitcoin.se (2012). Handlare. Retrieved March 26, 2016, from <http://www.bitcoin.se/handlare/>
- Bitcoin.se (2014). Skatteverket om kapitalvinstbeskattning av Bitcoin. Retrieved September 5, 2016, from <http://www.bitcoin.se/2014/05/02/skatteverket-om-kapitalvinstbeskattning-av-bitcoin/>
- Bitcoinfees.21.co (2016). Bitcoin Fees for Transactions. Retrieved September 5, 2016, from <https://bitcoinfees.21.co/>
- Bitfury (2016). Public versus Private Blockchains Part 1. Retrieved September 5, 2016, from <http://bitfury.com/content/5-white-papers-research/public-vs-private-pt1-1.pdf>
- Bitnation (2015). Estonia E-residency Program & Bitnation Public Notary Partnership. Retrieved September 20, 2016, from <https://bitnation.co/blog/pressrelease-estonia-bitnation-public-notary-partnership/>

- BitScan (2015). How to: establish proof-of-existence on the bitcoin blockchain. Retrieved September 5, 2016, from <https://bitscan.com/articles/how-to-establish-proof-of-existence-on-the-bitcoin-blockchain>
- Bitsquare (2016). The decentralized bitcoin exchange. Retrieved September 20, 2016, from <https://bitsquare.io/blog/beta-version-launched/>
- Blockchain.info (2016). Bitcoin Hashrate Distribution. Retrieved September 6, 2016, from <https://blockchain.info/pools>
- Bloomberg (2015). China Bans Financial Companies From Bitcoin Transactions. Retrieved September 5, 2016, from <http://www.bloomberg.com/news/articles/2013-12-05/china-s-pboc-bans-financial-companies-from-bitcoin-transactions>
- Bloomberg (2016). Blythe Masters Firm Raises Cash, Wins Australian Contract. Retrieved September 5, 2016, from <http://www.bloomberg.com/news/articles/2016-01-21/blythe-masters-firm-raises-cash-wins-australian-exchange-deal>
- Bloomberg (2016). Wall Street is Blockchain's Weak Link. Retrieved September 5, 2016, from <http://www.bloomberg.com/gadfly/articles/2016-03-23/wall-street-banks-will-be-the-weakest-link-in-the-blockchain>
- Bol, S., & Ceric, A. (2014). Bitcoin-ett hållbart betalningsmedel?: En transaktionskostnadsanalys av Bitcoin som betalningsmedel jämfört med traditionella betalningsmedel. Retrieved September 5, 2016, from <http://www.diva-portal.org/smash/get/diva2:812816/FULLTEXT01.pdf>
- Brave New Coin (2015). Donating Bitcoin to Charities Is On the Rise. Retrieved September 5, 2016, from <http://bravenewcoin.com/news/donating-bitcoin-to-charities-is-on-the-rise/>
- Brave New Coin (2016). British Prime Minister and Cabinet advised to start using distributed ledger technology. Retrieved September 5, 2016, from <http://bravenewcoin.com/news/british-prime-minister-and-cabinet-advised-to-start-using-distributed-ledger-technology/>
- Brito, J., Castillo, A. (2016). Bitcoin: A Primer for Policymakers. Retrieved September 5, 2016, from http://mercatus.org/sites/default/files/GMU_Bitcoin_042516_WEBv2_0.pdf
- Business Insider (2015). Blockchain: R3 membership hits 42, as it looks to non-banks. Retrieved September 5, 2016, from <http://uk.businessinsider.com/blockchain-r3-membership-hits-42-as-it-looks-to-non-banks-2015-12>
- Buterin, V. (2014). Ethereum White Paper. Retrieved September 5, 2016, from <https://github.com/ethereum/wiki/wiki/White-Paper>
- Buterin, V. (2014). On Stake. Retrieved September 5, 2016, from <https://blog.ethereum.org/2014/07/05/stake/>
- Bytecoin (2015). Alternatives for Proof of Work, Part 1: Proof Of Stake. Retrieved September 5, 2016, from <https://bytecoin.org/blog/proof-of-stake-proof-of-work-comparison/>

REFERENCES

- Central Bank of Barbados (2015). Should Cryptocurrencies be included in the Portfolio of International Reserves. Retrieved September 5, 2016, from <http://www.centralbank.org.bb/news/article/8827/should-cryptocurrencies-be-included-in-the-portfolio-of-international-reserves>
- Central Bank of Iceland (2014). Significant risk attached to use of virtual currency. Retrieved September 5, 2016, from <http://www.cb.is/publications-news-and-speeches/news-and-speeches/news/2014/03/19/Significant-risk-attached-to-use-of-virtual-currency/>
- Chamber of Digital Commerce (2014). Retrieved September 5, 2016, from <http://www.digitalchamber.org/>
- ChromaWay (2016). Cuber first blockchain product to win a major banking award! Retrieved September 5, 2016, from <http://chromaway.pr.co/126406-cuber-first-blockchain-product-to-win-a-major-banking-award>
- Coin Center (2016). Is Bitcoin Regulated? Retrieved September 5, 2016, from <http://coincenter.org/entry/is-bitcoin-regulated>
- CoinCap (2016). Retrieved September 5, 2016, from <https://coincap.io/>
- CoinDesk (2014). Andreessen at CoinSummit: Bitcoin Today is the Internet in 1994. Retrieved September 5, 2016, from <http://www.coindesk.com/marc-andreessen-balaji-srinivasan-discuss-bitcoin/>
- CoinDesk (2014). Bitcoin and Regulation: Lessons from the Early Days of Skype. Retrieved September 5, 2016, from <http://www.coindesk.com/bitcoin-regulation-lessons-early-days-skype/>
- CoinDesk (2014). Bolivia's Central Bank Bans Bitcoin. Retrieved September 5, 2016, from <http://www.coindesk.com/bolivias-central-bank-bans-bitcoin-digital-currencies/>
- CoinDesk (2014). Ecuador Bans Bitcoin, Plans Own Digital Money. Retrieved September 5, 2016, from <http://www.coindesk.com/ecuador-bans-bitcoin-legislative-vote/>
- CoinDesk (2014). Top US Colleges Begin Offering Bitcoin Courses. Retrieved September 5, 2016, from <http://www.coindesk.com/top-us-colleges-begin-offering-bitcoin-courses/>
- CoinDesk (2015). BitLicense: Who Has Applied and Who Has Left New York? Retrieved September 5, 2016, from <http://www.coindesk.com/bitlicense-round-up-whos-left-standing-in-new-york/>
- CoinDesk (2015). Hong Kong Official: Bitcoin Legislation Not Necessary. Retrieved September 5, 2016, from <http://www.coindesk.com/hong-kong-bitcoin-legislation-not-necessary/>
- CoinDesk (2015). New York Bitcoin Scene Divided As BitLicense Deadline Looms-. Retrieved September 5, 2016, from <http://www.coindesk.com/new-york-bitcoin-scene-divided-as-bitlicense-deadline-looms/>
- CoinDesk (2015). Sweden's Nasdaq Exchange Approves Bitcoin-based ETN. Retrieved September 5, 2016, from <http://www.coindesk.com/swedens-nasdaq-exchange-approves-bitcoin-based-etn/>

- CoinDesk (2015). The Real Cost of Applying for a New York BitLicense. Retrieved September 5, 2016, from <http://www.coindesk.com/real-cost-applying-new-york-bitlicense/>
- CoinDesk (2016). 21 Inc Launches Bitcoin Micropayments Marketplace. Retrieved September 5, 2016, from <http://www.coindesk.com/21-inc-launches-bitcoin-micropayments-marketplace/>
- CoinDesk (2016). Bitcoin Startups Stuck in Limbo as BitLicense Process Drags On. Retrieved September 5, 2016, from <http://www.coindesk.com/months-bitlicense-bitcoin-still-startups-await-approval-new-york/>
- CoinDesk (2016). Bitcoin Venture Capital Funding. Retrieved July 2, 2016, from <http://www.coindesk.com/bitcoin-venture-capital/>
- CoinDesk (2016). Blockchain Startup to Secure 1 Million e-Health Records in Estonia. Retrieved September 5, 2016, from <http://www.coindesk.com/blockchain-startup-aims-to-secure-1-million-estonian-health-records/>
- CoinDesk (2016). Ethereum Hard Fork Creates Competing Currencies. Retrieved September 20, 2016, from <http://www.coindesk.com/ethereum-hard-fork-creates-competing-currencies-support-ethereum-classic-rises/>
- CoinDesk (2016). Russia's 'Bitcoin Ban' Faces Uncertain Future After Draft Bill Withdrawn. Retrieved September 5, 2016, from <http://www.coindesk.com/russias-bitcoin-ban-draft-bill-withdrawn/>
- CoinDesk (2016). State of Bitcoin and Blockchain 2016. Retrieved September 5, 2016, from <http://www.coindesk.com/research/state-bitcoin-blockchain-2016/>
- CoinDesk (2016). State of Bitcoin and Blockchain 2016. Retrieved September 5, 2016, from <http://www.coindesk.com/research/state-bitcoin-blockchain-2016/>
- CoinDesk (2016). Understanding The DAO Attack. Retrieved September 20, 2016, from <http://www.coindesk.com/understanding-dao-hack-journalists/>
- CoinJar (2014). Stealth Addresses – What are they and do I need one? Retrieved September 5, 2016, from <https://blog.coinjar.com/2014/01/16/stealth-addresses-what-are-they-and-do-i-need-one/>
- Coinmap.org (2015). Map of Bitcoin accepting venues. Retrieved March 26, 2016, from <https://coinmap.org/>
- CoinTelegraph (2016). Understanding Smart Property. Retrieved September 5, 2016, from https://cointelegraph.com/news/understanding_smart_property
- Commonwealth (2015). Working Group on Virtual Currencies. Retrieved September 5, 2016, from http://thecommonwealth.org/sites/default/files/press-release/documents/P14195_ROL_Virtual_Currencies_D_Tait_V5_LoRes.pdf
- Computer Business Review (2016). Microsoft's Project Bletchley to speed up blockchain adoption. Retrieved September 5, 2016, from <http://www.cbronline.com/news/cloud/hybrid/microsofts-project-bletchley-to-speed-up-blockchain-adoption-through-azure-200616-4927624>
- Consumer Information (2013). Disputing Credit Card Charges. Retrieved September 5, 2016, from <https://www.consumer.ftc.gov/articles/0219-disputing-credit-card-charges>

REFERENCES

- Creandum (2016). In startups, sometimes things aren't meant to be. Retrieved September 5, 2016, from <http://www.creandum.com/in-startups-sometimes-things-arent-meant-to-be/>
- Cryptocoins News (2015). Ransomware Racket Nets Developers \$325 Million in Bitcoin. Retrieved September 5, 2016, from <https://www.cryptocoinsnews.com/ransomware-racket-nets-developers-325-million-in-bitcoin-report/>
- Dagens Juridik (2015). Svenskt bitcoinbolag går till domstol - vägrar lämna uppgifter om kunder till Skatteverket. Retrieved September 5, 2016, from <http://www.dagensjuridik.se/2015/03/svenskt-bitcoinbolag-gar-till-domstol-vagar-lamna-uppgifter-om-kunder-till-skatteverket>
- Dai, W. (1998). B-Money. Retrieved September 5, 2016, from <http://www.weidai.com/bmoney.txt>
- Danezis, G., & Meiklejohn, S. (2015). Centrally banked cryptocurrencies. arXiv:1505.06895 Retrieved September 5, 2016, from <http://arxiv.org/pdf/1505.06895v2.pdf>
- Deutsche Bank (2016) Utility Settlement Coin. Retrieved September 20, 2016, from https://www.db.com/newsroom_news/UBS_-Utility_Settlement_Coin_concept_on_blockchain_gathers_pace_24.08.2016.pdf
- Di Digital (2016). Bitcoinkursen knäckte KNC Miner – ansöker om konkurs. Retrieved September 5, 2016, from <http://digital.di.se/artikel/bitcoinkursen-knackte-knc-miner--ansoker-om-konkurs>
- Di Digital (2016). Fintech kräver tydligare spelregler. Retrieved September 5, 2016, from <http://digital.di.se/artikel/fintech-kraver-tydligare-spelregler>
- Di Digital (2016). Storbänkerna sluter upp bakom blockkedjan. Retrieved September 5, 2016, from <http://digital.di.se/artikel/storbankerna-sluter-upp-bakom-blockkedjan>
- Diffie, W., & Hellman, M. (1976). "New directions in cryptography". *IEEE transactions on Information Theory*, 22(6), 644-654
- DiVA (2004). Retrieved March 26, 2016, from <http://www.diva-portal.org/>
- e-Estonia (2016). Estonia hits the 10 000 e-resident milestone. Retrieved September 5, 2016, from <https://e-estonia.com/estonia-hits-the-10-000-e-resident-milestone/>
- ECB (2012). Virtual Currency Schemes. Retrieved September 5, 2016, from <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>
- ECB (2015). Virtual currency schemes - A Further Analysis. Retrieved September 5, 2016, from <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>
- Ehandel.se (2014). Stor svensk E-handlare tar nu emot Bitcoin i kassan. Retrieved September 5, 2016, from <http://www.ehandel.se/stor-svensk-e-handlare-tar-nu-emot-bitcoin-i-kassan,3870.html>
- Elements Project (2016). Confidential Transactions. Retrieved September 5, 2016, from <https://www.elementsproject.org/elements/confidential-transactions/>
- EU Commission (2015). The Digital Agenda of Virtual Currencies. Can BitCoin Become a Global Currency. Retrieved September 5, 2016, from <https://ec.europa.eu/jrc/en/publication/digital-agenda-virtual-currencies-can-bitcoin-become-global-currency>

- Falkvinge, R. (2011). Why I'm Putting All My Savings Into Bitcoin. Retrieved September 5, 2016, from <http://falkvinge.net/2011/05/29/why-im-putting-all-my-savings-into-bitcoin/>
- FBI (2012). Bitcoin Virtual Currency. Retrieved September 5, 2016, from https://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf
- FinCEN (2016). Guidance FIN-2013-G001. Retrieved September 5, 2016, from https://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html
- Forbes (2011). Solving the \$190 billion Annual Fraud Problem. Retrieved September 5, 2016, from <http://www.forbes.com/sites/haydnshaughnessy/2011/03/24/solving-the-190-billion-annual-fraud-scam-more-on-jumio/>
- Forbes (2016). 4 Reasons Why Bitcoin Represents A New Asset Class. Retrieved September 5, 2016, from <http://www.forbes.com/sites/laurashin/2016/06/02/4-reasons-why-bitcoin-represents-a-new-asset-class/>
- Forbes (2016). As Ransomware Crisis Explodes, Hollywood Hospital Coughs Up \$17,000 In Bitcoin. Retrieved September 5, 2016, from <http://www.forbes.com/sites/thomasbrewster/2016/02/18/ransomware-hollywood-payment-locky-menace/>
- Groenewegen, J., Spithoven, A. H. G. M., & Van den Berg, A. (2010). *Institutional economics: An introduction*. Hampshire: Palgrave Macmillan
- Handelsbanken (2011). Retrieved March 28, 2016, from <https://www.handelsbanken.se/>
- Harvard Business Review (2016). The Impact of the Blockchain Goes Beyond Financial Services. Retrieved September 5, 2016, from <https://hbr.org/2016/05/the-impact-of-the-blockchain-goes-beyond-financial-services>
- He, D., Habermeier, K. F., Leckow, R. B., Haksar, V., Almeida, Y., et al. (2016). Virtual Currencies and Beyond: Initial Considerations - International Monetary Fund. Retrieved September 5, 2016, from <https://www.bitcoinnews.ch/wp-content/uploads/2013/12/sdn1603.pdf>
- Hodges, A. (2012). *Alan Turing: the enigma*. Random House.
- Huffington Post (2016). Here's Why Blockchains Will Change the World. Retrieved September 5, 2016, from http://www.huffingtonpost.com/don-tapscott/heres-why-blockchains-wil_b_10146610.html
- International Business Times (2015). Bitnation and Estonian government start spreading sovereign jurisdiction on the blockchain. Retrieved September 5, 2016, from <http://www.ibtimes.co.uk/bitnation-estonian-government-start-spreading-sovereign-jurisdiction-blockchain-1530923>
- International Business Times (2016). Ransomware is the supervillain of cybersecurity and none of our PCs will be safe again. Retrieved September 5, 2016, from <http://www.ibtimes.co.uk/cisco-ransomware-supervillain-cybersecurity-none-our-pcs-will-be-safe-again-1564094>
- InvestmentWatch (2016). Bitcoin is being challenged by a perceived difference in fungibility. Retrieved September 5, 2016, from <http://investmentwatchblog.com/>

REFERENCES

- bitcoin-is-being-challenged-by-a-perceived-difference-in-fungibility-between-old-and-new-units/
- Johnston, D. (2013). *The General Theory of Decentralized Applications*, Dapps. Retrieved September 5, 2016, from <https://github.com/DavidJohnstonCEO/DecentralizedApplications>
- Khan Academy (2013). Bitcoin: What is it. Retrieved September 5, 2016, from <https://www.khanacademy.org/economics-finance-domain/core-finance/money-and-banking/bitcoin/v/bitcoin-what-is-it>
- KnCMiner (2013). Retrieved September 5, 2016, from <http://www.kncminer.com/>
- Krugman, P. (2010). Why Is Deflation Bad? Retrieved September 5, 2016, from <http://krugman.blogs.nytimes.com/2010/08/02/why-is-deflation-bad/>
- Lecocqassociate (2016). Virtual Currencies. Retrieved September 5, 2016, from <http://lecocqassociate.com/publication/virtual-currencies/>
- Lelieveldt, S. (2016). 'DNBcoin': the Dutch central bank experiment with a blockchain-based coin. Retrieved September 5, 2016, from <https://www.linkedin.com/pulse/dutch-central-bank-experiment-blockchain-based-simon-lelieveldt>
- Lerner, S. D. (2016). Rootstock Whitepaper - Bitcoin powered Smart Contracts. Retrieved September 5, 2016, from <https://www.weusecoins.com/assets/pdf/library/Rootstock-WhitePaper-Overview.pdf>
- Let's Talk Bitcoin (2015). Token Controlled Viewpoint (TCV). Retrieved September 5, 2016, from <https://letstalkbitcoin.com/blog/post/tcv>
- Linköping University (2016). TSIT03 Cryptology. Retrieved from <http://www.icg.isy.liu.se/en/courses/tsit03/>
- Linux Foundation (2016). Linux Foundation's Hyperledger Project Announces 30 Founding Members. Retrieved September 5, 2016, from <https://www.linuxfoundation.org/news-media/announcements/2016/02/linux-foundation-s-hyperledger-project-announces-30-founding>
- Ludwin, A. (2016). Why Central Banks Will Issue Digital Currency. Retrieved September 5, 2016, from <https://medium.com/chain-inc/why-central-banks-will-issue-digital-currency-5fd9c1d3d8a2>
- Merkle, R. C. (1987). *A digital signature based on a conventional encryption function*. *Conference on the Theory and Application of Cryptographic Techniques*. Springer Berlin Heidelberg
- Miller, V. S. (1985). *Use of elliptic curves in cryptography*. In *Conference on the Theory and Application of Cryptographic Techniques* (pp. 417-426). Springer Berlin Heidelberg
- Mises Institute (2014). Can Quantitative Easing Lift Economic Growth? Retrieved September 5, 2016, from <https://mises.org/library/can-quantitative-easing-lift-economic-growth>
- MIT (2016). Digital Certificates Project. Retrieved September 5, 2016, from <http://certificates.media.mit.edu/>
- MIT Media Lab (2015). The Media Lab Digital Currency Initiative. Retrieved September 5, 2016, from <https://www.media.mit.edu/research/highlights/media-lab-digital-currency-initiative>

- Nakamoto, S. (2008). Bitcoin P2P e-cash paper. Retrieved September 5, 2016, from <https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html>
- Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved September 5, 2016, from <https://bitcoin.org/bitcoin.pdf>
- Narayanan, A. (2016). The Princeton Bitcoin textbook is now freely available. Retrieved September 5, 2016, from <https://freedom-to-tinker.com/blog/randomwalker/the-princeton-bitcoin-textbook-is-now-freely-available/>
- NASA (2015). Open Innovation. Retrieved September 5, 2016, from <https://www.nasa.gov/offices/oct/openinnovation>
- Nasdaq (2015). Linq Enables First-Ever Private Securities Issuance. Retrieved September 5, 2016, from <http://ir.nasdaq.com/releasedetail.cfm?releaseid=948326>
- Nasdaq (2016). Nasdaq's Blockchain Technology to Transform the Republic of Estonia's e-Residency Shareholder Participation. Retrieved September 5, 2016, from <https://web.archive.org/web/20160416015329/http://www.nasdaq.com/press-release/nasdaqs-blockchain-technology-to-transform-the-republic-of-estonias-eresidency-shareholder-20160212-00058>
- New York State Department of Financial Services (2015). Regulatory Framework Virtual Currencies. Retrieved September 5, 2016, from <http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf>
- Nick, J. (2016). Bitcoin Privacy: Theory and Practice. Retrieved September 5, 2016, from https://www.reddit.com/r/Bitcoin/comments/4b9ylx/bitcoin_privacy_theory_and_practice_jonas_nick/
- Nordea Group (2002). Retrieved March 28, 2016, from <http://www.nordea.com/>
- OpenBazaar (2016). OpenBazaar is Open for Business. Retrieved September 20, 2016, from <https://blog.openbazaar.org/openbazaar-is-open-for-business/>
- Poon, J., & Dryja, T. (2016). The Bitcoin Lightning Network: Scalable Of-Chain Instant Payments. Retrieved September 5, 2016, from <https://lightning.network/lightning-network-paper.pdf>
- PR Newswire (2016). Chain and Global Financial Firms Unveil Open Standard for Blockchain. Retrieved September 5, 2016, from <http://www.prnewswire.com/news-releases/chain-and-global-financial-firms-unveil-open-standard-for-blockchain-300260512.html>
- Provenance (2015). Blockchain: the solution for transparency in product supply chains. Retrieved September 5, 2016, from <https://www.provenance.org/whitepaper>
- PwC (2016). Blurred lines: How FinTech is shaping Financial Services. Retrieved September 5, 2016, from <http://informes.pwc.es/fintech/assets/pwc-fintech-global-report.pdf>
- R3 (2016). A Distributed Ledger Designed for Financial Services. Retrieved September 5, 2016, from <http://r3cev.com/blog/2016/4/4/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services>
- Reddit (2015). A list of Block Explorers. Retrieved September 5, 2016, from https://www.reddit.com/r/Bitcoin/comments/3fvoxm/a_list_of_block_explorers_more_than_10/

REFERENCES

- Regeringen.se (2016). Globala målen och Agenda 2030. Retrieved September 5, 2016, from <http://www.regeringen.se/regeringens-politik/globala-malen-och-agenda-2030/>
- Reuters (2015). Bitcoin currency exchange not liable for VAT taxes. Retrieved September 5, 2016, from <http://www.reuters.com/article/us-bitcoin-tax-eu-idUSKCN0SGOX920151022>
- Rivest, R. L., Shamir, A., & Adleman, L. (1978). "A method for obtaining digital signatures and public-key cryptosystems". *Communications of the ACM*, 21(2), 120-126
- Safello (2013). Retrieved September 5, 2016, from <https://safello.com>
- Santander Innoventures (2015). The Fintech 2.0 Paper: rebooting financial services. Retrieved September 5, 2016, from <http://santanderinnoventures.com/wp-content/uploads/2015/06/The-Fintech-2-0-Paper.pdf>
- SaveOnSend (2015). Does Bitcoin make sense for international money transfer? Retrieved September 5, 2016, from <https://www.saveonsend.com/blog/bitcoin-money-transfer/>
- SEB (2008). Retrieved March 28, 2016, from <http://sebgroup.com/>
- Senate of Canada (2015). Digital Currency: You Can't Flip This Coin! Retrieved September 5, 2016, from <http://www.parl.gc.ca/Content/SEN/Committee/412/banc/rms/12jun15/home-e.htm>
- Sida (2014). Our work against corruption. Retrieved September 5, 2016, from <http://www.sida.se/English/how-we-work/approaches-and-methods/our-work-against-corruption/>
- Spiegel (2013). Germany Declares Bitcoins to Be a Unit of Account. Retrieved September 5, 2016, from <http://www.spiegel.de/international/business/germany-declares-bitcoins-to-be-a-unit-of-account-a-917525.html>
- Stanford (2013). Bitcoin Engineering CS251P Winter 2016. Retrieved September 5, 2016, from <http://bitcoin.stanford.edu/>
- SvD (2013). FI ser penningtvärrisk med bitcoin. Retrieved September 5, 2016, from <http://www.svd.se/fi-ser-penningtvattrisk-med-bitcoin>
- Swedbank (2011). Retrieved March 28, 2016, from <https://www.swedbank.com/>
- Szabo, N. (2005). Bit gold. Retrieved September 5, 2016, from <http://unenumerated.blogspot.co.uk/2005/12/bit-gold.html>
- Szabo, N. (2014). The dawn of trustworthy computing. Retrieved September 5, 2016, from <http://unenumerated.blogspot.com/2014/12/the-dawn-of-trustworthy-computing.html>
- Sztorc, P. (2016). Private Blockchains, Demystified. Retrieved September 5, 2016, from <http://www.truthcoin.info/blog/private-blockchains/>
- Taavikotka (2014). 10 million e-Estonians by 2025! Retrieved September 5, 2016, from <https://taavikotka.wordpress.com/2014/05/04/10-million-e-estonians-by-2025/>
- Todd, P. (2016). Soft Forks Are Safer Than Hard Forks. Retrieved September 5, 2016, from <https://petertodd.org/2016/soft-forks-are-safer-than-hard-forks>

- Top500.org (2016). China Races Ahead in TOP500 Supercomputer List. Retrieved September 5, 2016, from <https://www.top500.org/news/china-races-ahead-in-top500-supercomputer-list-ending-us-supremacy/>
- TradeBlock (2013). Refuting the ECB – The 9 Characteristics That Make Bitcoin Money. Retrieved September 5, 2016, from <https://tradeblock.com/blog/refuting-the-ecb-the-9-characteristics-that-make-bitcoin-money/>
- U.S. Chamber of Commerce (2016). Is 2016 the Year of the Blockchain? Retrieved September 5, 2016, from <https://www.uschamber.com/above-the-fold/blockchain-technology-2016-the-year-the-blockchain>
- UK Government (2015). Digital currencies: response to the call for information. Retrieved September 5, 2016, from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/414040/digital_currencies_response_to_call_for_information_final_changes.pdf
- UK Government Office For Science (2016). Distributed Ledger Technology: beyond block chain. Retrieved September 5, 2016, from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf
- University of Nicosia (2014). MSc in Digital Currency. Retrieved September 5, 2016, from <http://digitalcurrency.unic.ac.cy/>
- US Government History Office (2014). Nixon and the End of the Bretton Woods System, 1971–1973. Retrieved September 5, 2016, from <https://history.state.gov/milestones/1969-1976/nixon-shock>
- Valcke, P., Vandezande, N., & Van de Velde, N. (2015). The evolution of third party payment providers and cryptocurrencies under the EU's upcoming PSD2 and AMLD4. Retrieved September 5, 2016, from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2665973
- Varian, H. R. (2010). Computer mediated transactions. *The American Economic Review*, 100(2), 1-10. Retrieved September 20, 2016, from <http://people.ischool.berkeley.edu/~hal/Papers/2010/cmt.pdf>
- Washington Post (2015). Here's how Bitcoin charmed Washington. Retrieved September 5, 2016, from <https://www.washingtonpost.com/news/the-switch/wp/2013/11/21/heres-how-bitcoin-charmed-washington/>
- Wikipedia (2015). Legality of bitcoin by country. Retrieved April 8, 2016, from https://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country
- Wint (2016). Så garanterar vi att ingen ändrar i bokföringen i efterhand. Retrieved September 5, 2016, from <http://blogg.wint.se/2015/12/02/sa-garanterar-vi-att-ingen-andrar-i-bokforingen-i-efterhand>
- WIRED (1993). Crypto Rebels. Retrieved September 5, 2016, from <http://www.wired.com/1993/02/crypto-rebels/>
- WIRED (2014). Hacker Lexicon: What Is the Dark Web? Retrieved September 5, 2016, from <https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/>
- WIRED (2015). The Untold Story of Silk Road, Part 1. Retrieved September 5, 2016, from <https://www.wired.com/2015/04/silk-road-1/>

REFERENCES

- WIRED (2016). We Must Regulate Bitcoin. Problem Is, We Don't Understand It. Retrieved September 5, 2016, from <https://www.wired.com/2016/03/must-understand-bitcoin-regulate/>
- World Bitcoin Association (2013). Retrieved September 5, 2016, from <http://worldbitcoin.info/>
- World Economic Forum (2015). Deep Shift Technology Tipping Points and Societal Impact. Retrieved September 5, 2016, from http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf
- WSJ (2016). Bitcoin Technology's Next Big Test: Trillion-Dollar Repo Market. Retrieved September 5, 2016, from <http://www.wsj.com/articles/bitcoin-technologys-next-big-test-trillion-dollar-repo-market-1459256400>
- WSJ (2016). Key Blockchain Vendors, Cloud Providers Square Off in Major Test. Retrieved September 5, 2016, from <http://blogs.wsj.com/cio/2016/03/02/key-blockchain-vendors-cloud-providers-square-off-in-major-test/>
- XBT Provider (2015). Retrieved September 5, 2016, from <http://xbtprovider.com/>
- ZDNet (2014). CryptoLocker's crimewave: A trail of millions in laundered Bitcoin. Retrieved September 5, 2016, from <http://www.zdnet.com/article/cryptolockers-crimewave-a-trail-of-millions-in-laundered-bitcoin/>
- Zerocash (2014). Retrieved September 5, 2016, from <http://zerocash-project.org/>

Appendix One: Further Resources

Whitepapers

- [Bitcoin: A Peer-to-Peer Electronic Cash System](https://bitcoin.org/bitcoin.pdf)
<https://bitcoin.org/bitcoin.pdf>
- [Ethereum Whitepaper](https://github.com/ethereum/wiki/wiki/White-Paper)
<https://github.com/ethereum/wiki/wiki/White-Paper>
- [Enabling Blockchain Innovations with Pegged Sidechains](https://blockstream.com/sidechains.pdf)
<https://blockstream.com/sidechains.pdf>
- [The General Theory of Decentralized Applications, Dapps](https://github.com/DavidJohnstonCEO/DecentralizedApplications/blob/master/README.md)
<https://github.com/DavidJohnstonCEO/DecentralizedApplications/blob/master/README.md>
- [Rootstock – Bitcoin powered Smart Contracts](https://uploads.strikinglycdn.com/files/90847694-70f0-4668-ba7f-dd0c6b-0b00a1/RootstockWhitePaperv9-Overview.pdf)
<https://uploads.strikinglycdn.com/files/90847694-70f0-4668-ba7f-dd0c6b-0b00a1/RootstockWhitePaperv9-Overview.pdf>
- [Storj A Peer-to-Peer Cloud Storage Network](https://storj.io/storj.pdf)
<https://storj.io/storj.pdf>
- [Proof of Stake versus Proof of Work](http://www.bitfury.com/content/5-white-papers-research/pos-vs-pow-1.0.2.pdf)
www.bitfury.com/content/5-white-papers-research/pos-vs-pow-1.0.2.pdf
- [Chainpoint – A scalable protocol for recording data in the blockchain and generating blockchain receipts](https://tierion.com/chainpoint)
<https://tierion.com/chainpoint>

Reports

- [Virtual currency schemes - ECB \(2012\)](https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf)
<https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>
- [Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity - FBI \(2012\)](https://cryptome.org/2012/05/fbi-bitcoin.pdf)
<https://cryptome.org/2012/05/fbi-bitcoin.pdf>
- [On the origins of Bitcoin, stages of monetary evolution - Konrad S. Graf \(2013\)](http://nakamotoinstitute.org/static/docs/origins-of-bitcoin.pdf)
nakamotoinstitute.org/static/docs/origins-of-bitcoin.pdf

APPENDIX ONE: FURTHER RESOURCES

- **Bitcoin: Technical Background and Data Analysis - Fed (2014)**
<https://www.federalreserve.gov/econresdata/feds/2014/files/2014104pap.pdf>
- **Money is no object: Understanding the evolving cryptocurrency market - PwC (2015)**
<https://www.pwc.com/us/en/financial-services/publications/assets/pwc-cryptocurrency-evolution.pdf>
- **Beyond the Hype: Blockchains in Capital Markets - McKinsey (2015)**
https://www.weusecoins.com/assets/pdf/library/McKinsey%20Blockchains%20in%20Capital%20Markets_2015.pdf
- **National Security Implications of Virtual Currency - RAND Corporation (2015)**
https://www.rand.org/content/dam/rand/pubs/research_reports/RR1200/RR1231/RAND_RR1231.pdf
- **Virtual currency schemes, a further analysis - ECB (2015)**
<https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>
- **The Fintech 2.0 Paper: rebooting financial services - Santander InnoVentures (2015)**
<http://santanderinnoventures.com/wp-content/uploads/2015/06/The-Fintech-2-0-Paper.pdf>
- **Digital currencies: response to the call for information - HM Treasury UK Gov (2015)**
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/414040/digital_currencies_response_to_call_for_information_final_changes.pdf
- **Digital currencies - Bank for International Settlements (2015)**
www.bis.org/cpmi/publ/d137.pdf
- **Commonwealth Working Group on Virtual Currencies (2016)**
http://thecommonwealth.org/sites/default/files/press-release/documents/P14195_ROL_Virtual_Currencies_D_Tait_V5_LoRes.pdf
- **The Promise of Bitcoin and the Blockchain, Bretton Woods 2015 - Consumers' Research (2016)**
<http://bravenewcoin.com/assets/Industry-Reports-2016/Bretton-Woods-2015-White-Paper-The-promise-of-Bitcoin-and-the-Blockchain.pdf>
- **Blockchain Enigma Paradox Opportunity - Deloitte (2016)**
<http://bravenewcoin.com/assets/Industry-Reports-2016/Deloitte-Blockchain-Enigma-Paradox-Opportunity.pdf>
- **Virtual Currencies and Beyond Initial Considerations - IMF (2016)**
<https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf>
- **Distributed ledger technology beyond blockchain - UK Gov Chief Scientific Adviser (2016)**
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

- **How Can Cryptocurrency and Blockchain Technology Play a Role in Building Social and Solidarity Finance? - United Nations Research Institute for Social Development (2016)**
<http://bravenewcoin.com/assets/Industry-Reports-2016/UN-How-Can-Cryptocurrency-and-Blockchain-Technology-Play-a-Role-in-Building-Social-and-Solidarity-Finance-Brett-Scott.pdf>
- **Blockchain technology as a platform for digitization - Ernst & Young (2016)**
[https://webforms.ey.com/Publication/vwLUAssets/EY-blockchain-technology-as-a-platform-for-digitization/\\$FILE/EY-blockchain-technology-as-a-platform-for-digitization.pdf](https://webforms.ey.com/Publication/vwLUAssets/EY-blockchain-technology-as-a-platform-for-digitization/$FILE/EY-blockchain-technology-as-a-platform-for-digitization.pdf)
- **Embracing Disruption – Tapping the Potential of Distributed Ledgers to Improve the Post-Trade Landscape - DTCC (2016)**
https://www.finextra.com/finextra-downloads/newsdocs/embracing%20disruption%20white%20paper_final_jan-16.pdf
- **Consensus Immutable agreement for the Internet of Value - KPMG (2016)**
<https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/kpmg-blockchain-consensus-mechanism.pdf>

Books

- **Mastering Bitcoin: Unlocking Digital Cryptocurrencies**
– Andreas M. Antonopoulos
- **Bitcoin and Cryptocurrency Technologies (Princeton)**
- Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder
- **The Book Of Satoshi: The Collected Writings of Bitcoin Creator Satoshi Nakamoto**
– Phil Champagne
- **Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World**
– Don Tapscott and Alex Tapscott
- **Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money**
– Nathaniel Popper

Videos

- **This is how Bitcoin Works (2 min)**
<https://www.facebook.com/aljazeera/videos/10154385815638690/>
- **The real value of Bitcoin and crypto currency technology, blockchain explained (6 min)**
<https://www.youtube.com/watch?v=YIVAluSL9SU>

APPENDIX ONE: FURTHER RESOURCES

- [The Essence of How Bitcoin Works - Non-Technical \(5 min\)](https://www.youtube.com/watch?v=t5JGQXCTe3c)
<https://www.youtube.com/watch?v=t5JGQXCTe3c>
- [How Bitcoin Works in 5 Minutes - Technical \(5 min\)](https://www.youtube.com/watch?v=l9jOJk30eQs)
<https://www.youtube.com/watch?v=l9jOJk30eQs>
- [How Bitcoin Works Under the Hood - Technical \(22 min\)](https://www.youtube.com/watch?v=Lx9zgZCMqXE)
<https://www.youtube.com/watch?v=Lx9zgZCMqXE>

Först kom PC:n, sen kom internet, nu kommer blockkedjan! Inte sällan talas det om blockkedjan som en revolutionerande innovation som kommer att förändra sättet vi handlar, kommunicerar och hanterar information på. Men vad innebär detta mer konkret?

I *Blockchain – Decentralized Trust* presenteras blockkedjeteknikens funktion, utveckling och genomslag. Blockkedjeteknik möjliggör delning av information, tillgångar och värden mellan olika parter globalt, utan mellanhänder eller centrala aktörer. I rapporten undersöks möjliga konsekvenser av en utbredd framtida användning av blockkedjeteknik och ett antal spännande framtids-scenarier presenteras.

Rapporten är författad av David Bauman, entreprenör med mångårig erfarenhet av blockkedjan, Pontus Lindblom, disputerad forskare Linköping universitet och Claudia Olsson, vd och grundare Exponential Holding samt Associate Faculty Singularity University.



WWW.ENTREPRENORSKAPSFORUM.SE