XISCHÉ

REPORTS

STATE *of* PLAY

BLOCKCHAIN

THE BLOCKCHAIN MARKETPLACE WILL SOON BE WORTH $7.74 BILLION. THIS REPORT CHARTS THE ORIGINS OF BLOCKCHAIN, EXAMINES THE CURRENT ECOSYSTEM, AND PREDICTS THE SHIFTS AND LEADERS OF THE SECOND INTERNET REVOLUTION.

XISCHÉ & CO
strategy by design™

XISCHÉ & CO
strategy by design™

XISCHE IS A COLLECTIVE HELPING GOVERNMENTS, GLOBAL BRANDS, AND START-UPS RESEARCH, INNOVATE, COMMERCIALISE, AND TELL UNFORGETTABLE STORIES.

XISCHÉ
REPORTS

XISCHE REPORTS IS AN INVESTIGATIVE PRACTICE WITHIN THE COLLECTIVE, EXAMINING CHANGE IN THREE DOMAINS — FUTURE, INNOVATION, AND CULTURE. WE PUBLISH LONG-FORM, VISUAL, AND INTERACTIVE INSIGHTS.

Xische & Co.
POBox 500601
A-202, Building 4
Dubai Design District
T +9714 367 8184

www.xische.com

EDITOR-IN-CHIEF

Danish Farhan
Chairman, Xische Holdings

CONTRIBUTORS

Mary Ames
Author

Marri Janeka
Managing Editor

Zaineb Al Hassani
Editor

ACKNOWLEDGEMENTS

The *State of Play: Blockchain* report would not have been possible without the support and contribution of the entire strategy and consulting teams, including Wisam Amid, Liza Terry, Nakul Berry, Marri Janeka, Karl Pais, Kajal Kalan, and Laszlo Menyhart. We also thank Suhail Suleman for contributions to the design of the report.

We also thank the **Dubai Future Foundation** and the **Smart Dubai Office** for the opportunity to contribute to the Dubai Blockchain Strategy through our consulting arm, **Xische Strategy Practice**, and our communications agency, **Xische & Co**.

IN PARTNERSHIP WITH

دبـــي الذكية
SMART DUBAI

WITH THE SUPPORT OF

WBF WORLD BLOCKCHAIN FORUM INVESTMENTS & ICOs

FINTECH HIVE
DIFC

Image reused with permission under the Creative Commons Attribution-ShareAlike licence

CONTENTS

1. Battle for the Internet 8

2. Spark of Rebellion 13

- The quest for the anti-bank
- The Cypherpunks

3. Birth of Bitcoin 20

- Crash and breakthrough
- Who is Satoshi Nakamoto?
- A question of trust
- E-Gold: A cautionary tale
- Bitcoin goes to The Hill

4. So, What is Blockchain? 30

- Beyond Bitcoin
- Smart Contract breakthrough
- Ethereum and the World Computer
- The internet of transactions

5. The Age of Blockchain 45

- The Blockchain ecosystem
- The banks
- Boundary-crossing start-ups
- Bold governments

6. Why Nobody Will Care in Ten Years 65

- The DAO, parity, and the risks of being human
- Blockchain for every organisation
- A closing dose of reality

1. BATTLE FOR THE INTERNET

Perhaps the internet is fundamentally flawed. Like a marble statue, with a powerful blow to the heart of the stone, the veined masterpiece could crumble and fall.

Ninety percent of data on the internet has been created in the past two years.[1] We upload family photos to a photo-sharing app; save travel plans on a travel app; store notes and articles in a note-taking app. Almost every app we use asks us to save our debit or credit card details at some point. We trust others to keep our data secure, but there is no way to verify who else is accessing our data online. As soon as we upload our data, we cede control.

In the wrong hands, a little piece of data can go a long way. Early in 2017, an attack on Equifax, a credit-scoring firm in the US, compromised the account details and social security numbers of 143 million Americans.[2] Most of this data has already been sold to other black market firms who will use the stolen information to commit fraud.

Part 1: Battle for the Internet

As more of our data is stored in blackbox central databases, the success rate and impact of these data breaches will continue to scale. According to AT&T Vice President of Security Architecture Karthik Swarnam, "Cybercrime damages are expected to rise to $6 trillion annually by 2021."[3] With enough successful attacks, our trust in the internet will crumble.

But a fringe community of Libertarian programmers and activist hackers believe they have found a solution to restore trust in the internet, introducing a new paradigm for online transactions in the process.

What began as a passion project of tech diehards has transformed with breathtaking speed into a wave of innovation that is sweeping through the digital community. This movement is touching off a surge in new ventures, investments, and solutions that, if realised at scale, have the potential to fundamentally change how we interact with the internet.

How did an idea pioneered by anti-authoritarian punks and championed by drug dealers become the darling of governments, banks, and global corporations?[4]

The story of Blockchain is the story of a persistent human quest for trust, autonomy, and safety.

"Cybercrime damages are expected to rise to $6 trillion annually by 2021." With enough successful attacks, our trust in the internet will crumble.

Part 1: Battle for the Internet

"All money mankind has ever used has been insecure in one way or another." [5]

- NICK SZABO

Image reused with permission under the Creative Commons Attribution-ShareAlike licence

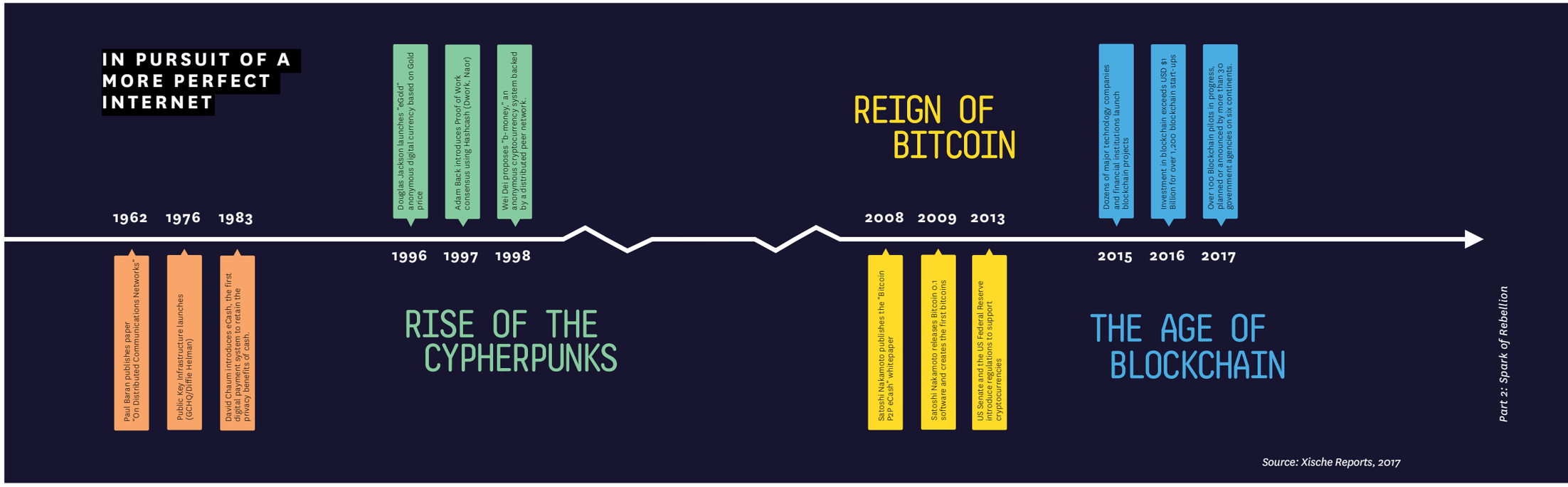
2. SPARK OF REBELLION

Threats to our data in the ether world parallel a more tangible threat that has dogged society for much of our modern history: the worth of money.

The mechanisms of commerce traditionally have been defined by social contracts enforced by a central authority. The mint issues coins that ascribe a certain value to things, trade is regulated and, for the most part, people's individual fortunes are secured. But who is to say if your coin is still valid if the rules change? You stockpile a treasure. One day, you could wake up to find a new governor in charge, one who prefers another coinage. All of a sudden, your amassed fortune is valueless.

To find a solution to our internet problem, the cryptocurrency pioneers of the 1980s and 1990s began by trying to solve our money problem. The hunt was on for a new currency that would be internationally recognised yet independent of the fortunes of the realm.

Part 2: Spark of Rebellion



Part 2: Spark of Rebellion

THE QUEST FOR THE ANTI-BANK

The first step towards a decentralised currency system was to find a way to make the exchange of money anonymous again.

Cash is a private exchange of a mutually-agreed value between two parties. Although you could withdraw cash from a bank, and the receiving party may in turn deposit the cash into another bank, the details of the purchase itself remain private. But with the rapid adoption of credit and debit cards, banks have quickly become repositories not just for our money, but also for data on how we spend our money. When we transact digitally using a debit or a credit card, our financial data is no longer private: we are entrusting the details of that exchange to our bank, the credit card company, and our friend's bank.

A method for private digital transactions would mirror the benefits of cash but with the speed and convenience of credit.

In 1983, David Chaum, recognised as one of the inventors of digital cash, introduced the first model for eCash, a digital payment system that retained the privacy benefits of cash. The eCash system allowed users to store bank-verified digital money on their home computer to pay for goods or services from participating merchants. The new system was able to make the relationship between the withdrawal and payment transactions anonymous, achieving the same level of privacy as traditional cash transactions.[6]

But Chaum's eCash system, along with similar schemes piloted during the mid-1990s by CyberCash, Digital Equipment (Compaq Computer), and IBM, fell short of the goal of an anonymous and decentralised currency system. To the consumer, the functional benefit of eCash was unclear. To the tech world, the system was still overly reliant on a central authority, since the bank remained singularly responsible for verifying each transaction.[7]

Meanwhile, a radical concept for the future of truly independent digital money was emerging.

THE CYPHERPUNKS

Whereas Chaum's eCash sought to transform fiat money into digital cash, the pioneers of cryptocurrency were pushing an even more revolutionary idea: a fungible currency for a purely digital community, de-linked from any federal monetary system.

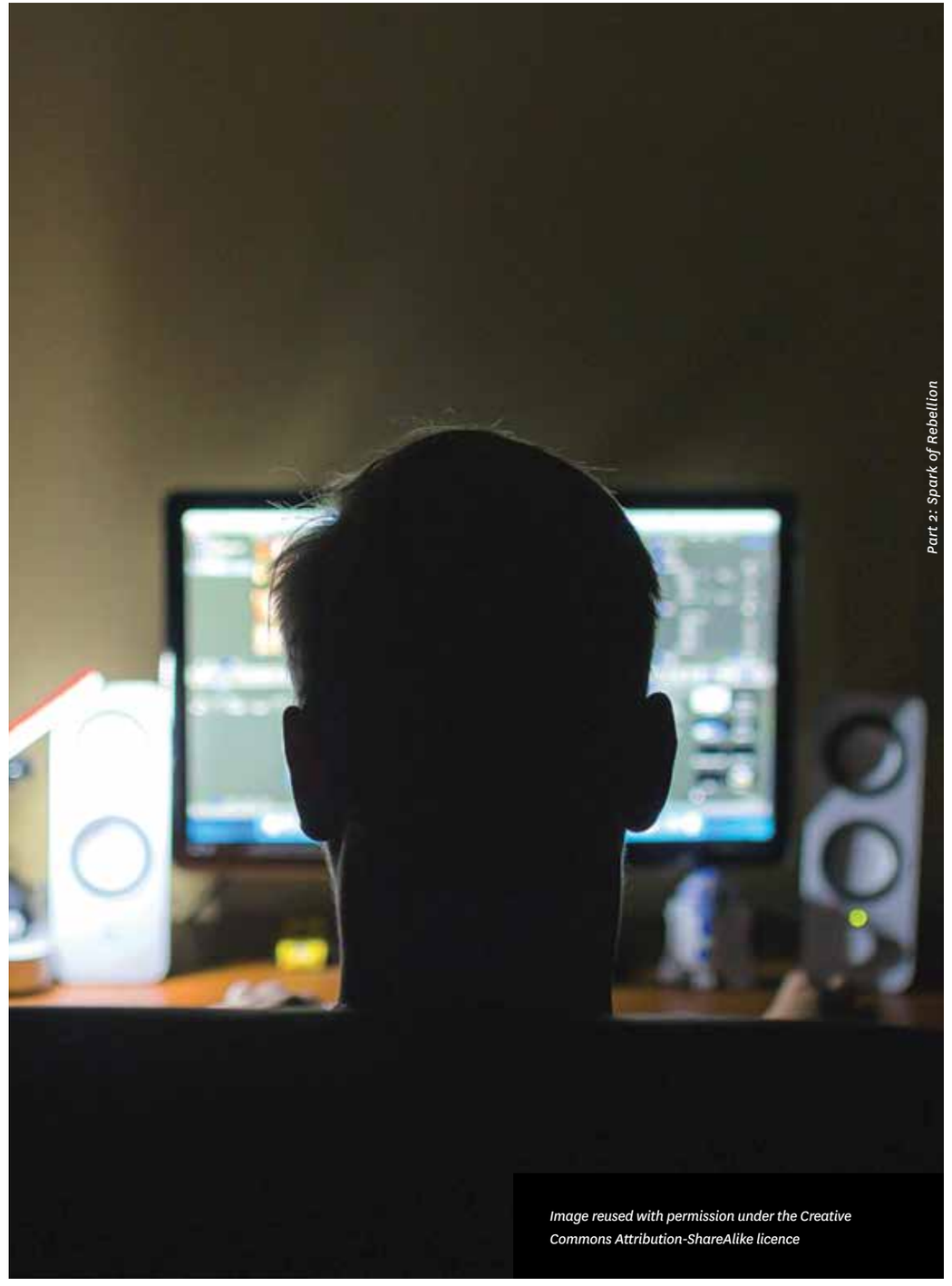
In a seminal essay published in 1998, Wei Dai, an intensely private computer engineer associated with Microsoft, described an anonymous cryptocurrency system backed by a distributed peer network that could facilitate both the creation and the exchange of digital 'b-money'.[8]

Dai was a member of the Cypherpunks, a loosely organised community of digital privacy advocates committed to realising the ideal of a decentralised and anonymous monetary system.

> "A community is defined by the co-operation of its participants, and efficient cooperation requires a medium of exchange — money — and a way to enforce contracts. Traditionally, these services have been provided by the government or government-sponsored institutions and only to legal entities... I describe a protocol by which these services can be provided to and by untraceable entities."
> - Wei Dai, 1998

Counted among them were Adam Back, Hal Finney, and Nick Szabo, who also briefly worked with Chaum at DigiCash, the successor to eCash. Building on each other's innovations, the Cypherpunks contributed essential pieces to the puzzle of a fully-realised cryptocurrency.[9]

The foundation for Dai's currency system was proposed by Adam Back a year earlier, in 1997, through a modification of the cryptographic principle of Hashcash.



Part 2: Spark of Rebellion

Hashcash was conceived in 1992 by Cynthia Dwork and Moni Naor as a means to cryptographically secure email messages. The programme appends a difficult-to-solve but easy-to-verify mathematical puzzle to the header of an email. The puzzle must be solved prior to sending the email, and solving it proves the sender has enough interest in the message being delivered to take the time to complete the puzzle.

Back's modified interpretation of Hashcash applied the same principles but used the puzzle as an incentive rather than a deterrent. According to Back, users could earn digital currency by solving the hash puzzles appended to pending transactions, earning at a rate corresponding to the time required to solve the puzzle. Worth is proportional to effort: a gold bullion is more valuable than a penny because it is harder to make. Dai theorised a mechanism similar to Back's Hashcash in his concept of b-money, a currency that could be created by anyone with a computer.

Still, Dai's proposal lacked the technical details to implement his theory. Without the means to turn idea into reality, interest in the pursuit began to wane. By the early 2000s, most computer programmers had given up hope on the Cypherpunks' dream for a cryptocurrency utopia.

"Anyone can create money by broadcasting the solution to a previously unsolved computational problem. The only conditions are that it must be easy to determine how much computing effort it took to solve the problem and the solution must otherwise have no value, either practical or intellectual. The number of monetary units created is equal to the cost of the computing effort in terms of a standard basket of commodities."

- WEI DAI, 1998

Image reused with permission under the Creative Commons Attribution-ShareAlike licence

3. BIRTH OF BITCOIN

CRASH AND BREAKTHROUGH

The Cypherpunks were motivated by the conviction that establishing a distributed and independent monetary system was essential to a secure and peaceful society.

As the world careened into the 2008 financial crisis, Cypherpunks' interest in devising an alternative currency system sparked again. This time, after nearly a decade marinating in the technology hive-mind, a fully fledged cryptocurrency system emerged — at the climax of a global financial meltdown.

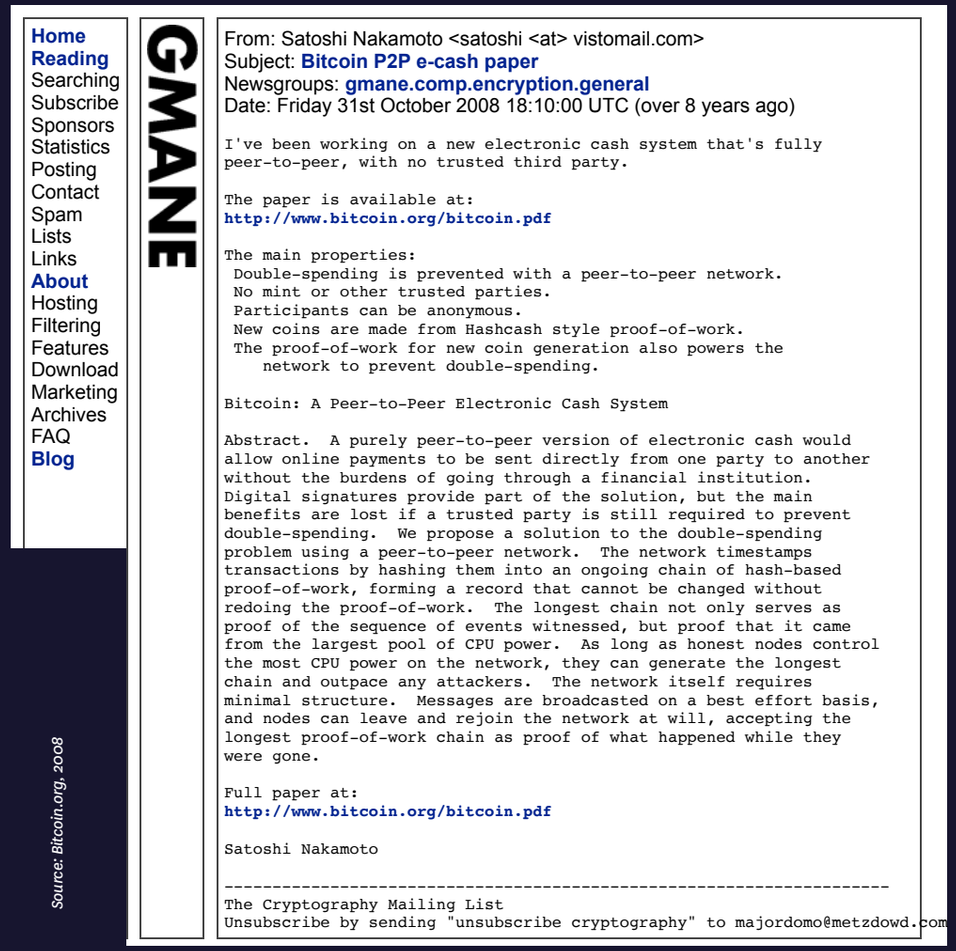
On October 31, 2008, one day after the chief of Merrill Lynch resigned in the wake of revelations that the investment bank was exposed to $7.9 billion in bad debt, an email from Nakamoto was sent to a mailing list of cryptography enthusiasts with the subject line, "Bitcoin P2P e-cash paper".[10] [11] [12]

The brief email described a new peer-to-peer digital currency system that utilised several of the foundational concepts pieced together by the Cypherpunks nearly a decade earlier: no central authority or mint, peer-to-peer authentication with Hashcash, and anonymous participation.

"I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party."

- SATOSHI NAKAMOTO, OCTOBER 31, 2008

Within three months, on January 9, 2009, Nakamoto released Version 0.1 of the Bitcoin software, launching both the software and the first units of the Bitcoin cryptocurrency.



Home
Reading
Searching
Subscribe
Sponsors
Statistics
Posting
Contact
Spam
Lists
Links
About
Hosting
Filtering
Features
Download
Marketing
Archives
FAQ
Blog

GMANE

From: Satoshi Nakamoto <satoshi <at> vistomail.com>
Subject: Bitcoin P2P e-cash paper
Newsgroups: gmane.comp.encryption.general
Date: Friday 31st October 2008 18:10:00 UTC (over 8 years ago)

I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.

The paper is available at:
http://www.bitcoin.org/bitcoin.pdf

The main properties:
 Double-spending is prevented with a peer-to-peer network.
 No mint or other trusted parties.
 Participants can be anonymous.
 New coins are made from Hashcash style proof-of-work.
 The proof-of-work for new coin generation also powers the
    network to prevent double-spending.

Bitcoin: A Peer-to-Peer Electronic Cash System

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without the burdens of going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as honest nodes control the most CPU power on the network, they can generate the longest chain and outpace any attackers. The network itself requires minimal structure. Messages are broadcasted on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Full paper at:
http://www.bitcoin.org/bitcoin.pdf

Satoshi Nakamoto

The Cryptography Mailing List
Unsubscribe by sending "unsubscribe cryptography" to majordomo@metzdowd.com

Source: Bitcoin.org, 2008

WHO IS SATOSHI NAKAMOTO?

An aura of mystery surrounds the creator of Bitcoin. Nakamoto is most probably a pseudonym of the person — or group of people — responsible for inventing the technology. Multiple investigations have failed to reveal Nakamoto's true identity, although many suspect the inventor may be one — or several — of the Cypherpunks who lay the groundwork for the Bitcoin system he pioneered.

Dai and Nakamoto exchanged emails in August 2008, several months before the publication of the Bitcoin whitepaper; Back and Nakamoto also allegedly emailed during that time. Hal Finney was the first person to use the Bitcoin software after Nakamoto launched it, and the first person after Nakamoto to mine bitcoins. And Nick Szabo began publicising his renewed efforts to build 'Bit Gold', a system with striking similarities to Bitcoin, in the spring of 2008, yet went inexplicably silent after Nakamoto's October announcement. More notable coincidences surrounding the birth of Bitcoin link Nakamoto to at least half a dozen other crypto-pioneers.[9] [13]

There is greater consensus behind Nakamoto's motivations. Like many of the Cypherpunks, Nakamoto displayed a distinctively Libertarian slant characterised by a mistrust of centralised authority and a desire to establish a financial system free from state regulation. The first mined bitcoin — known as the Genesis Block — contained a message from Nakamoto that directly referenced the ongoing financial crisis: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks".[14]

The message, entered in the comment section of the first bitcoin block, quotes a headline from *The Sunday Times*, "Chancellor Alistair Darling on brink of second bailout for banks. Billions may be needed as lending squeeze tightens." The reference has been taken as a critical commentary on the state of the financial markets.[15]

To Nakamoto, the Cypherpunks, and early Bitcoin adaptors, the 2008 financial crisis marked the demise of an outdated global financial institution and heralded the entrance of a new breed of monetary exchange for the digital age.

A QUESTION OF TRUST

Bitcoin was not the first attempt at a digital currency. Various digital currency projects had already been born and passed into obsolescence — including eCash and b-money — long before Nakamoto introduced his digital coin.

The success of any private currency hinges on trust. Participants need to believe that others will accept their coins in exchange for goods or services and the goods received will be worth the value exchanged. People will avoid a marketplace if its merchants are known swindlers.

Anonymous cryptocurrencies face an even higher hurdle. By design, purchase records are private, and buyer and seller identities are kept anonymous. Cryptocurrencies are seen as a haven for fraudsters, money launderers, and drug dealers.

To earn public trust, Bitcoin would need to do more than prove its coins are reliably redeemable. The platform would also need to demonstrate that the moral and ethical benefits of participation outweigh the risks associated with an anonymous digital currency.

E-GOLD: A CAUTIONARY TALE

One year before the release of Bitcoin, the public witnessed the fall-out of a years-long effort by the US federal government to dismantle an earlier digital currency, E-Gold.

Driven by a conviction that the US should never have left the gold standard, Douglas Jackson, a practicing oncologist and amateur economist, decided it was time for a radical rethink of money. With support from a software engineer, Jackson programmed, designed, and launched E-Gold in 1996, introducing an anonymous, nationless currency backed by gold.

By 2005, E-Gold had grown to more than 3.5 million customers in 165 countries, with 1,000 new accounts opening every day. E-Gold was second only to PayPal in the online payment industry.

But the dark side of an anonymous currency exchange would soon land Jackson behind bars. International criminals were using E-Gold for money laundering and to anonymously stash funds to finance illegal operations. Between 2003 and 2005, the FBI and the Secret Service used E-Gold to arraign a number of high-profile financial criminals. Jackson collaborated with the FBI until his own arrest in 2007 on federal charges of money laundering, conspiracy, and operating an unlicensed money transmitting business.[16]

In November 2008, less that one month after Nakamoto introduced Bitcoin to the Cypherpunk community, Jackson was sentenced to 36 months of supervised release, including six months of house arrest and electronic monitoring, and 300 hours of community service, and handed strict guidelines requiring E-Gold to adhere to all regulations for money transmitters should it ever re-launch.[16]

It took E-Gold most of a decade to gather enough traction to attract the attention of federal regulators. Bitcoin's fortunes changed when, after just five years of relative anonymity, the US government once again turned its eye to the emerging cryptocurrency market.

BITCOIN GOES TO THE HILL

On paper, Bitcoin should have shared E-Gold's fate. Like E-Gold, Bitcoin was the passion project of a fervent anti-bank idealist. Like E-Gold, Bitcoin developers spent much of its early life shoring up vulnerabilities and fixing glitches. And as an anonymous, international, digital currency, Bitcoin quickly became the coin of choice for criminals and black market traders.

But in US Senate hearings held in late 2013 on the future of cryptocurrencies, testimony from financial regulators, law enforcement, and federal officials signalled a surprising new openness to digital currencies.

Autumn 2013 had been a particularly fraught season for Bitcoin. In October, the FBI seized over 170,000 bitcoins when they shut down the infamous Silk Road digital black market. That autumn, hackers forced two bitcoin exchanges in Australia and Hong Kong to close up shop.[17]

"[Digital currencies] may hold long-term promise." [17]

- FORMER CHAIRMAN OF THE FEDERAL RESERVE BEN BERNANKE, NOVEMBER 2013

Image reused with permission under the Creative Commons Attribution-ShareAlike licence

The US Senate Committee on Homeland Security and Governmental Affairs, scheduled for November 18, and US Senate Committee on Banking, Housing, and Urban Affairs, scheduled for the following day, should have been cause for concern among Bitcoin investors. But rather than call for the shuttering of the platform, government officials offered a cautiously positive outlook.

Jennifer Shasky Calvery, the director of the Financial Crimes Enforcement Network (FinCEN), chose her words carefully: "Digital currencies could be used for money laundering, but ... this is no different from other financial instruments." Her measured testimony was a significant about-face from the federal ruling against Jackson six years earlier.

Ernie Allen, president of the International Centre for Missing and Exploited Children, suggested there was "broad-based agreement on its potential for social good". Even the Chairman of the Federal Reserve, Ben Bernanke, offered that digital currencies "may hold long-term promise".[18]

The gulf between the technologists and the policymakers on Capitol Hill had narrowed, and government regulators, who for decades had monitored the growth of the internet from the sidelines, were now embracing the technology for its potential for the public good.

Earlier that year, FinCEN, which is a division of the US Department of the Treasury, issued the first significant guidance for persons creating, obtaining, exchanging, accepting, and transmitting digital currencies. The document, which clearly defines the roles of the user, exchanger, and administrator of digital currencies and the financial reporting requirements for each, paved the way for open discussions on how best to regulate newly emerging cryptocurrencies, including bitcoin.[19]

With the cautious blessing of the US government, bitcoin was poised to enter the mainstream. Now only one roadblock remained: the banks.

The major banks and financial institutions followed Bitcoin's emergence with wary skepticism. Bitcoin's decentralised exchange and stateless currency was a direct challenge to the traditional banking model. And the Bitcoin market was notoriously volatile; bitcoin could fluctuate in value by as much as 50,000% in a single day. Investors were understandably wary.

Still, Bitcoin had a solution to a problem that had been dogging banks and exchanges for years. International trades can take up to three days to settle on a public market: Bitcoin trades were clearing in a matter of minutes. The banks wanted Bitcoin's technology to improve their own processes. Meanwhile, Bitcoin activists needed a signal from the banks to grant Bitcoin the legitimacy and trust it needed to smooth its volatile exchange.

Soon, major global financial and technology institutions were toying with Bitcoin and examining the mechanisms that allowed the distributed financial network to operate as it did.

And it was the underlying logic of Bitcoin — the Blockchain — that banks, governments, and start-ups saw the true potential for a digital re-awakening.

Part 3: Birth of Bitcoin

4. SO, WHAT IS BLOCKCHAIN?

The mining and exchange of a cryptocoin works like this:

Step 1
MINING

Assuming you don't have access to a faucet, or $4,000 to buy a bitcoin today, your participation in the exchange starts with 'mining' bitcoin, as if you were mining for gold to take with you on a shopping trip.

Bitcoin is mined today exactly as Wei Dai envisioned the process in 1998. Once your computer is connected to the Bitcoin network through a bitcoin wallet, you can start mining. Mining happens any time a bitcoin transaction is requested on your network. In order to complete the transaction, a unique hash needs to be assigned to each request. To create that hash, every computer connected to the network races to solve a short maths problem. The first computer to solve the problem — which generates the unique hash — receives an amount of bitcoin proportional to the complexity of the problem. The harder the problem is to solve, the more bitcoin you earn.

Step 2
SETTING UP YOUR WALLET

Now that you have some bitcoin, you probably want to spend it on something. First, you need to set up your wallet. Your wallet is a unique ledger assigned to you and protected through a public key infrastructure to keep your identity anonymous. The ledger tracks how many bitcoins you — and everyone else on your network — have to spend by recording every transaction ever made. Functionally, it is similar to the ledger of a traditional cheque book, except that it is readable by everyone on the network.

Step 3
REQUESTING A TRANSACTION

With your wallet full of bitcoin, now you're ready to spend.

Every exchange of bitcoin begins with a transaction request. When you request a transaction, a new 'block' is created (like a new row in your cheque book) that contains all of the details of the transaction. Your block is assigned a new hash that is mathematically verifiable as unique.

Step 4
VERIFYING A TRANSACTION

Once your block is created, each participant in the network verifies that all of the details for the transaction are correct. This is done by comparing the hashes of all of the previous transactions on the ledger (for example, when you first deposited money in your wallet).

This is the step that ensures you have enough bitcoin to complete the transaction, and that the party you are transferring funds to is able to receive them.

Step 5
PERFORMING THE TRANSACTION

Once every computer in the network verifies the transaction, it is cleared to proceed. The funds change accounts, and the public ledger is updated accordingly.

Step 6
STORING THE TRANSACTION DATA

When you began your transaction request, you created a new block that stored all of the details of the transaction. As soon as your transaction is completed, that block gets added to the public ledger. That ledger is viewable by everyone in the network, and it is made up of all of the blocks of every transaction that has ever taken place on the network.

Part 4: So, What is Blockchain?

Because each block is linked to a unique hash, the ledger cannot be altered: if someone were to go in and try to change the details of a past transaction, the hash would change (because the data changes), and as a result, that block and all following blocks would become invalid.

In this way, the exchange network is not only anonymous (using public key infrastructure) and decentralised (each participant in the network verifies each transaction), it is also tamper proof.

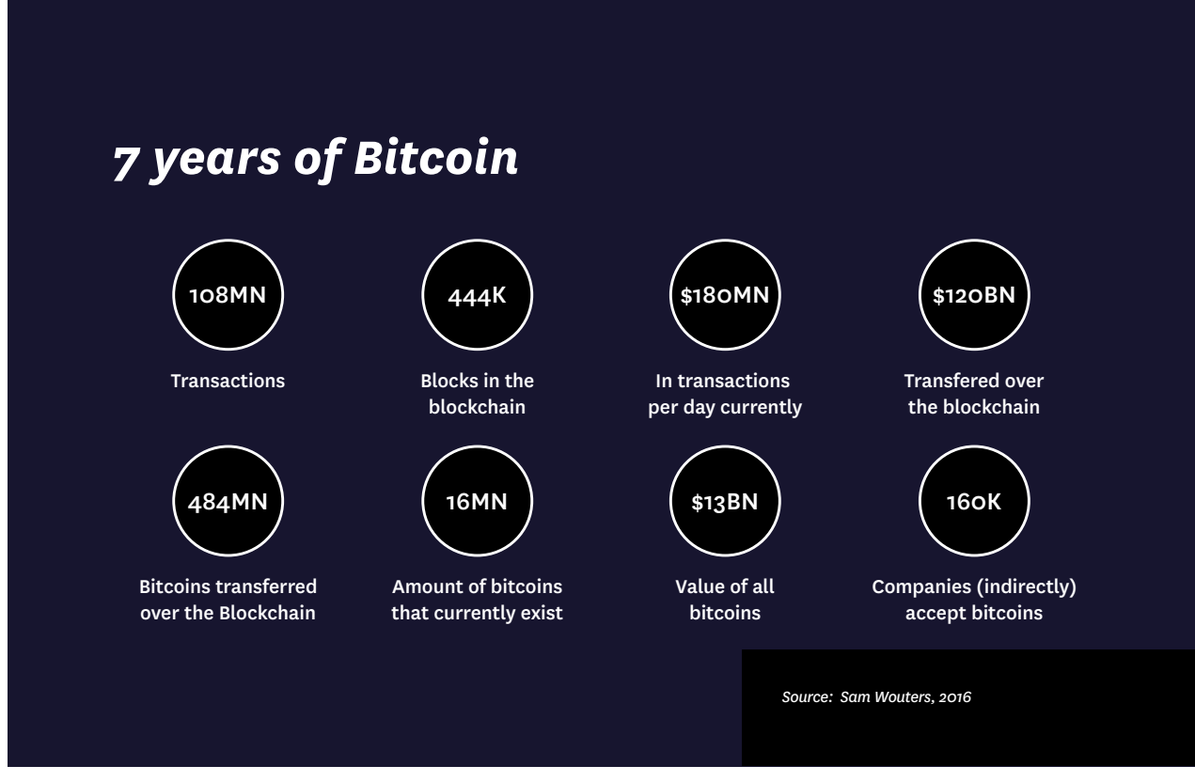
This public ledger of connected blocks bearing the complete and indelible transaction history of the network is called 'the Blockchain', and it is the undergirding technology on which the Bitcoin system operates.

BEYOND BITCOIN

When the banks finally lifted the hood on Bitcoin, they discovered a powerful new protocol that could fundamentally transform how their institutions utilised the internet for transactions.

Blockchain adds an extra layer of security for all participants in an ecosystem. Rather than rely on one centralised repository, Blockchain's decentralised model distributes decision-making power across a wide network of connected machines. To launch an attack, a malicious actor would need to divide his attention to overwhelm 51% of the network's distributed nodes, rather than focusing his efforts on a single main gate.

Blockchain's distributed ledger also enhances trust among participants on the network, which could include other banking institutions or customers themselves. Blockchain's hash protocol ensures that no record that has been stored on its ledger can be altered. Changing any data on the ledger would result in a new hash being created, which would invalidate the entire chain after the record in question. With an unalterable ledger, all participants in the network can be sure that each transaction has proceeded exactly and only as recorded.



Because the Blockchain ledger stores all historical transaction data on a distributed network, the requirements to complete a transaction can be verified near-instantly. If Bill previously gave $5 to Sue, and now Sue wants to give $3 to Evan, Evan's and Sue's banks don't need to independently go and check if Sue has $3 to give: as soon as Sue begins the transfer request, all of the parties on the network verify that Sue is able to send the money (and that Evan is able to receive it), by checking the Blockchain ledger. As soon as the request is verified, the value changes hands.

Using Blockchain, banks could cut trade processing times from three days to three minutes or less. Once they understood what the Blockchain could do, the banking world rolled up its sleeves.

THE INTERNET OF TRANSACTIONS

78830174330

1 Decentralised Network
Everyone in the network sits around a table, taking notes on everything that is happening.

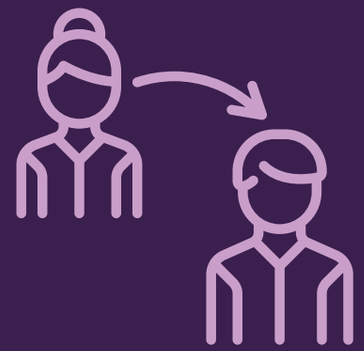
2 Transaction Request
Alice announces to the room that she wants to give her phone to Bob.

3 Verification
Everyone in the room races to check their notes to confirm that Alice is able to give her phone to Bob.

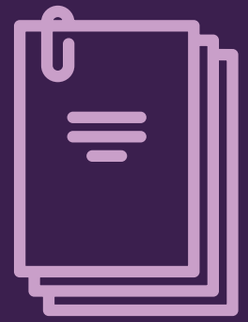
4 Hash Mining
The first person to mathematically prove that Alice is able to give her phone to Bob wins a prize.

5 Hash
The request is assigned a unique transaction number, based on the numerical proof.

6 Transaction
Alice gives her phone to Bob.



7 Block
Everyone records the transaction on their paper.



8 Blockchain
Everyone reviews each paper to ensure the information is correct. The paper is then sealed and added to the stack.

Source: Xische Reports, 2017

In March 2015, Nasdaq OSX, which oversees the Nasdaq stock exchanges, announced that it would begin testing a system using Bitcoin's Blockchain to oversee stock trades on the Nasdaq Private Market, a separate market for private companies. By managing pre-IPO trades on the Blockchain, CEOs would be able to instantly see who was buying and trading their stock. Before Nasdaq's pilot, pre-IPO companies were tracking this kind of data on Excel spreadsheets.[20]

Nasdaq's move highlighted a growing interest in Blockchain from the banking and technology sector. By the end of the year, over a half dozen financial and tech industry heavyweights — IBM, Cisco, the London Stock Exchange, and JP Morgan among them — were experimenting with building their own Blockchains.[20]

Bitcoin's Blockchain is revolutionary, but it is also imperfect. James Angel, a professor of finance at Georgetown University, compares Bitcoin to MySpace. While bitcoin as a currency is deeply flawed, according to Angel, its underlying technology can be adapted to fundamentally change the financial sector. Bitcoin's Blockchain set the ball in motion, but it is more likely that another platform will emerge as the true heavyweight.

"Bitcoin is like MySpace... it is paving the way for the Facebook or Twitter of Blockchain" [19]

— JAMES ANGEL

Image reused with permission under the Creative Commons Attribution-ShareAlike licence

Inspired by the Bitcoin Blockchain, IBM and Digital Asset Holders (DAH), a start-up founded by a former JP Morgan executive, began work on their own Blockchain as part of the Open Ledger Project, supported by Linux. They dubbed their blockchain 'Hyperledger'.[21]

In keeping with the Linux ethos, Hyperledger is open source: although IBM has contributed the bulk of the code for the Blockchain ledger, it is freely open and editable to others. Still more important for the future of Blockchain, Hyperledger is also a distributed ledger, and machines from many different organisations can participate in the network. As Marley Gray of Microsoft puts it, "Blockchain is essentially worthless within a single organisation. You have to have parties that are not yourself".[21]

By the close of 2015, with

"Blockchain is essentially worthless within a single organisation."

— MARLEY GRAY, MICROSOFT[20]

Blockchain being embraced by governments, banks, and the technology industry, it became clear that Bitcoin was only the beginning; the first use case of a technology that held the potential to radically transform the Internet.

SMART CONTRACT BREAKTHROUGH

As interest in Blockchain grew, developers began exploring the system's potential beyond financial transactions.

Although initially designed for monetary exchanges, early advocates recognised that the technology could be used to oversee the exchange of any contract of record. The title deed of a new home, the sale of a used car, the execution of a will, a driver's licence — even a ballot vote.

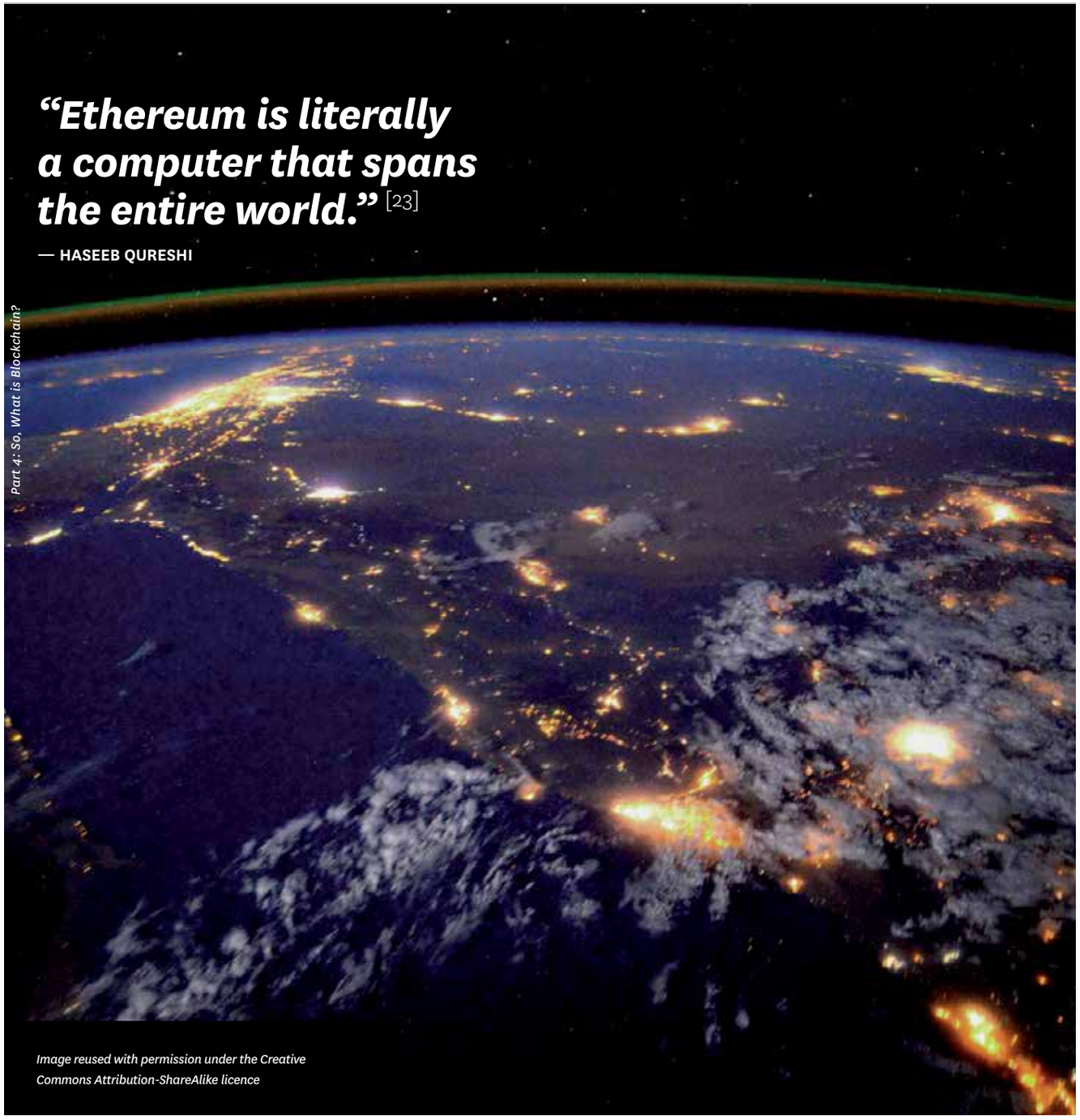
Not only can a Blockchain record the exchange of these contracts on an indelible ledger, it can, through a decentralised network, automatically execute contracts and eliminate the need for a middleman.

Take for example the purchase of a new home:

In most jurisdictions, finding your dream home, though you might search for months, only gets you to the starting line. Most buyers will take out a mortgage, which means you will need to have your mortgage loan pre-approved from the bank before making an offer, and your bank will require a credit score from a third party credit-rating firm. You will likely be closing with a real estate broker, not the current home owner. So once an offer is made, the validation process will proceed in duplicate with the brokers and bankers on each side of the transaction filing forms and reports. And there are any number of inspections that you, as the new owner, have the right to request. These inspections will need to be approved, conducted, and recorded. When you finally reach the settlement stage, your local government will step in to record transition of ownership. Then begins the lengthy process of registering for various utilities, phone lines, internet, cable, updating your address with the postal service, updating your voting address, and updating your address for food delivery apps.

A real estate application on Blockchain, utilising self-executing smart contracts, can condense this process to just a handful of steps, with banks, brokers, and the local government participating on a decentralised Blockchain network with a distributed ledger.

Part 4: So, What is Blockchain?



"Ethereum is literally a computer that spans the entire world." [23]

— HASEEB QURESHI

Image reused with permission under the Creative Commons Attribution-ShareAlike licence

ETHEREUM AND THE WORLD COMPUTER

Smart Contracts are open-ended: almost anything that can be transacted can be represented by a Smart Contract. The closest parallel to a Smart Contract is a website. Websites are used for the exchange of information, and all website developers follow a certain protocol when programming their sites. But the actual information on the site is infinitely variable.

Whereas Bitcoin restricted itself to one type of Smart Contract, for the purpose of the exchange of bitcoins, the team behind Ethereum saw an opportunity to develop a Blockchain that would support any potential transaction on a peer network. The language on which Ethereum is built is Turing-complete — meaning Ethereum is capable of doing just about anything that can be expressed in a computer programme. And because Ethereum rests on a Blockchain, the history of every transaction is stored on an enormous, distributed computer: the Ethereum Virtual Machine (EVM).[22] [23]

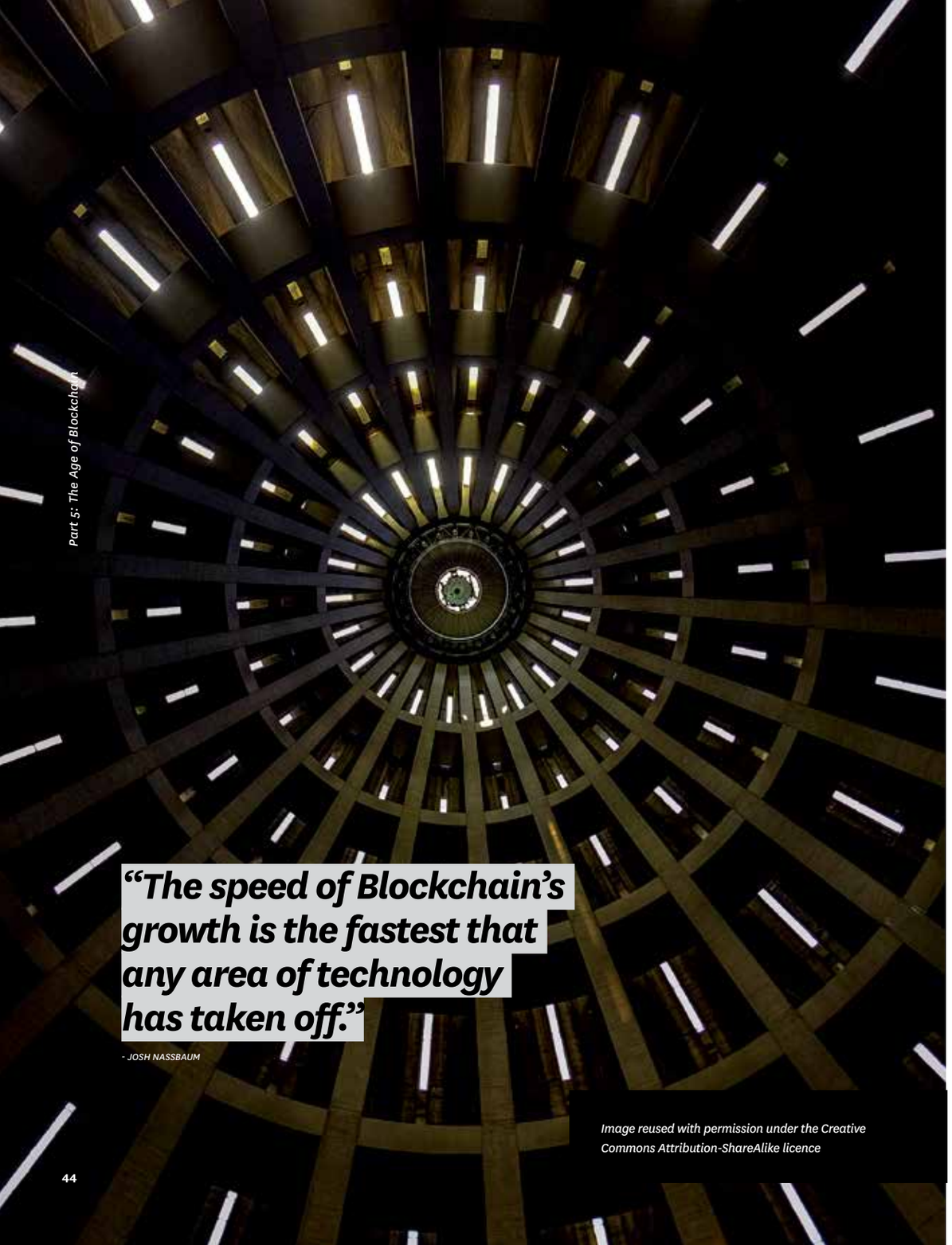
Ethereum has ignited a surge of interest in Smart Contracts and the supporting ecosystem of tools required to build Smart Contracts on the EVM. Ethereum's value has skyrocketed over the last six months.[24]

THE INTERNET OF TRANSACTIONS

Blockchain is not a ‘new’ internet, nor is it trying to replace the internet. By deploying a decentralised, hash-based protocol with an indelible ledger, Blockchain is offering a powerful alternative to the internet processes that have become routine since the widespread adoption of the World Wide Web.

By connecting centralised servers capable of storing massive amounts of data to a graphical user interface that allowed humans to easily read and interact with that data, the World Wide Web ushered in an internet of information that fundamentally changed the way we access and store information.

Blockchain has the potential to effect the same revolution, but for transactions. If its potential is realised correctly, we could trade stocks, buy homes, and play fantasy football on the Blockchain with the same security and ease with which we watch cat videos on YouTube.



"The speed of Blockchain's growth is the fastest that any area of technology has taken off."

- JOSH NASSBAUM

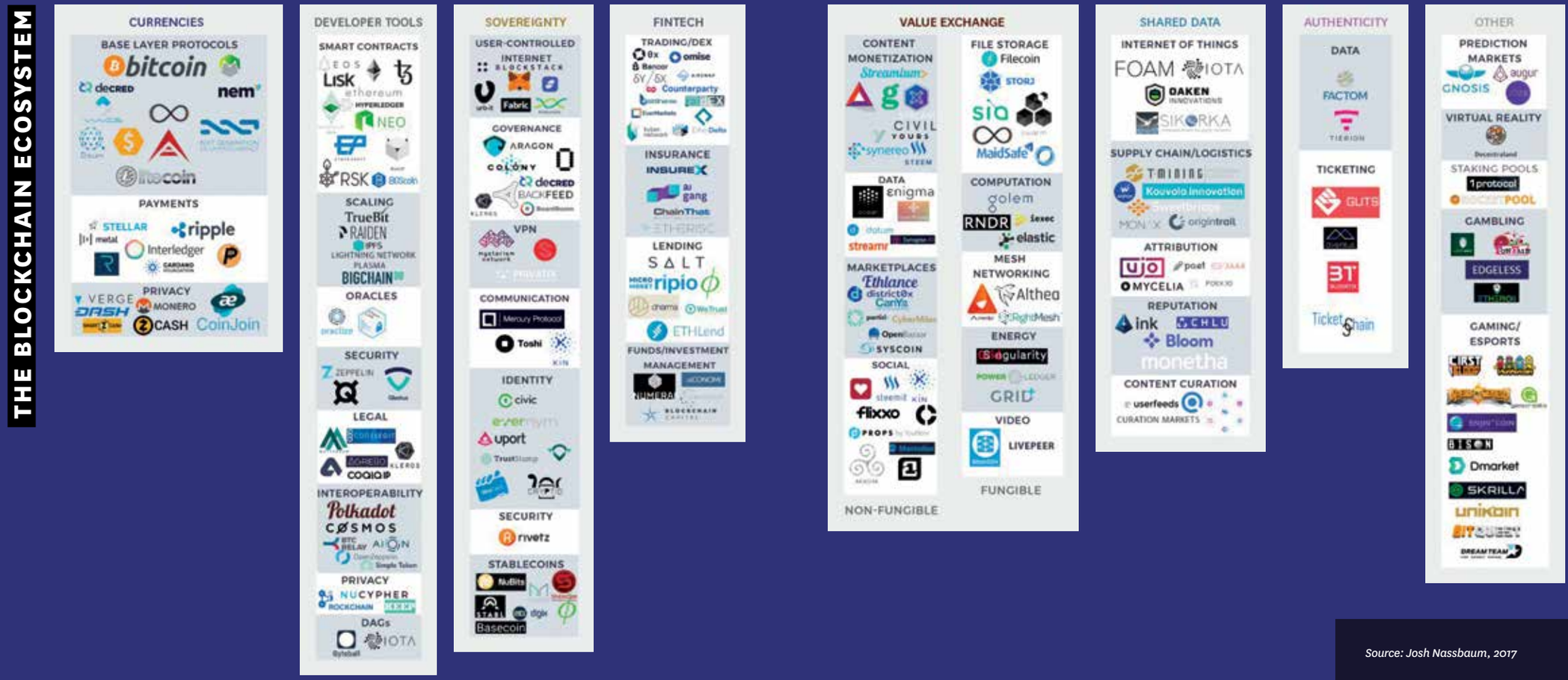
5. THE AGE OF BLOCKCHAIN

The dream of a self-regulated, secure, decentralised network sparked as an idea in the 1980s, grew into a quest in the 90s, was finally realised in the late 2000s, and truly came into its own by 2016.

Bitcoin is no longer the only Blockchain platform with wide-scale adoption. A comprehensive Blockchain ecosystem has emerged with astonishing momentum in the past five years. According to Blockchain specialist and venture capitalist Josh Nassbaum, "the speed of blockchain's growth is the fastest that any area of technology has taken off".[26]

THE BLOCKCHAIN ECOSYSTEM

To illustrate the scale of Blockchain's impact, Nassbaum has identified a Blockchain Project Ecosystem spanning eight major categories and 43 sub-categories that captures the depth and breadth of the Blockchain ecosystem.[26]



Source: Josh Nassbaum, 2017

— *Currencies*

Bitcoin was the first cryptocurrency to use the Blockchain. Since then, many more start-ups have entered this category to improve on the initial work of Bitcoin, or to create tailored products for specific use cases. Companies active in the Blockchain Currency category can be roughly segregated in to three sub-groups: base layer protocols, for projects such as Bitcoin that codify currency exchange protocols; payments, for projects like Ripple, a currency exchange and remittance network that focuses on the transfer of funds; and privacy, for projects that are providing anonymous, untraceable cryptocurrencies.[27]

— *Developer Tools*

Blockchain was introduced on the back of Bitcoin, but, since then, a diverse category of Developer Tools has emerged, populated by companies and consortiums who are building and refining the tools required to actually deliver game-changing Blockchain applications. As Nassbaum puts it, “In order for many of the Blockchain use cases we’ve been promised to come to fruition, such as fully decentralised autonomous organisations or a Facebook alternative where users have control of their own data, foundational, scalable infrastructure needs to grow and mature. Many of these projects aim at doing just that.”[26]

Part 5: The Age of Blockchain

Ethereum and Hyperledger lead the Smart Contract sub-group, yet are just the tip of the iceberg for a deep and entwined category, with each sub-group enhancing or supporting the other. Other Developer Tool sub-groups that Nassbaum identifies include: scaling, oracles, security, legal, interoperability, privacy, and DAGs (a variation on the technology that uses a 'tangle' or 'block-braid' rather than a Blockchain).[26]

— *Fintech*

Fintech on Blockchain is the natural outgrowth of number systems, each with their own currencies, that are required to work together. The projects under this category serve to facilitate the exchange, lending, and investment of different cryptocurrencies. Sub-groups under the Fintech category include: trading and decentralised exchange, insurance, lending, and funds or investment management.[26]

The insurance and lending sub-groups are particularly interesting, as Nassbaum points out, for their scalability. Blockchain networks enable greater differentiation of individual risk potentials, leading to cost savings that should in theory pass on to the customer. And since Blockchain ledgers are unalterable, users can be confident their individual histories haven't been tampered with.[26]

— *Sovereignty*

Projects in the Sovereignty category are turning to Blockchain to address privacy concerns for highly sensitive data on the cloud. Centralised servers that store user data are prime targets for hackers. Blockchain's distributed database provides a more secure alternative for some data sets. The Blockchain is not mature enough to handle such projects at scale yet, but is very effective at securing data on a smaller scale. Sovereignty projects can be clustered into seven sub-groups, each addressing a specific data type: user-controlled, governance, VPN, communication, identity, security, and stablecoins.[25]

— *Value Exchange*

While the Currency and Fintech categories profile Blockchain applications for currency exchanges, the technology is able to support a wide range of transactions between people or parties, without the need for a relationship or trust between those parties. Blockchain facilitates the exchange of both fungible and non-fungible goods, and this category identifies projects in both spaces.[26]

Blockchain is being deployed for the exchange of non-fungible value with projects in the content monetisation, data, marketplaces, and social sub-groups. Blockchain projects for the exchange of fungible goods can be classified under five sub-groups: file storage, computation, mesh networking, energy, and video.[26]

— *Shared Data*

In traditional shared data exchanges, the aggregator of the data is the one who benefits the most and rarely passes that value on to the individuals and companies who own the data. Shared data is also difficult to aggregate and verify between multiple parties, creating a significant barrier to entry where only the biggest players can capitalise on the benefits.[26]

Blockchain lowers the barrier to entry by giving autonomy to data owners that allows them to 'take their data with them,' as they engage with other parties for whom their data may be useful. For example, a seller who has built up a reputation for quality over many years in a single market can open business in a new market and carry his reputation with him on an immutable Blockchain. Blockchain also allows for the democratisation of data-collection, enabling a wide network of participants to add, annotate, and build insights from data. Contributors whose data has proven the most useful can be incentivised through tokens, which increase in value as the organisation grows.[26]

Projects currently underway to leverage Blockchain technology for shared data are divisible into five sub-groups: Internet of Things, supply chain and logistics, attribution, reputation, and content curation.[26]

Part 5: The Age of Blockchain

— Authenticity

Blockchain's verification protocol and indelible ledger are a cryptographic means of ensuring that a datum or product — like a movie ticket — is what it says it is and will remain that way infinitely. Products that are susceptible to fraud can benefit from the Blockchain to guarantee their integrity. Recent projects in the Authenticity category have focused on two sub-groups: data and ticketing.[26]

From the speed with which the Blockchain ecosystem has grown and the scope that it already spans, it is clear that this is a technology that, in some form, will soon have a tangible impact on how we interact with and transact data on the internet.[26]

The value exchange use cases alone are an invitation to imagine just what is possible when we view every transaction as an opportunity to introduce the Blockchain into our daily lives. Specific use cases from banks, governments, and cutting-edge start-ups show what changes are already taking shape.[26]

"66% of banks will have commercial-scale Blockchain operations by 2020"

- IBM

THE BANKS

Since Nasdaq OSX's first overtures on Bitcoin's Blockchain in 2015, dozens of financial institutions have begun experimenting with the emerging technology.

In 2016, IBM issued a report predicting that 15% of global banks would implement Blockchain by the end of 2017, and that 66% of banks would have Blockchain operations in commercial production and at scale by 2020.[27]

— Bond Transactions (R3, 2016)

In September 2016, US-based fintech start-up R3 announced it had successfully completed a pilot for bond transactions on Blockchain. The platform deployed Smart Contracts to enable the trading, matching, and settlement of US Treasury bonds, as well as automated coupon payments and redemption.

The project utilised Intel's Blockchain technology and was carried out in partnership with eight banks, including HSBC and State Street, with support from the US Treasury.[28]

— Utility Settlement Coin (UBS, 2017)

Led by UBS and supported by the UK-based Blockchain company Clearmatics, a growing network of European banks have teamed up to roll out a Utility Settlement Coin (USC), a type of cryptocoin that is convertible at parity with the currency denomination of any bank deposit. The system, which aims to be operational by 2018, would facilitate the near-instant digital exchange of fiat currencies, with the USC functioning as a digital equaliser. Spending a USC would be the same as spending the real currency it is paired with.[29]

— Cheque Chain (Emirates NBD, 2017)

Emirates National Bank of Dubai (Emirates NBD), a leading banking group in the Middle East, announced a unique Blockchain pilot in spring 2017. As a developing region, many of the bank's customers still prefer to transact via cheque. Rather than enforce a new consumer behaviour, Emirates NBD is piloting an integration for Blockchain that allows customers to continue to write cheques but enables the bank to instantly store the cheque data on the Blockchain as soon as the cheque is deposited. Once a digital copy of the cheque is made — usually after it is deposited into a cheque deposit machine — the bank reads the details of the cheque and stores it on the 'Cheque Chain', creating an indelible record of the transaction.[30]

BOUNDARY-CROSSING START-UPS

The iconoclastic nature of Bitcoin drew start-ups in droves. Much of the infrastructure around Bitcoin today — including dedicated trading websites, international event organisations, and print publications, not to mention the volume of programmers rolling our new applications — did not exist before 2013.

Between 2012 and 2013, venture funding of Bitcoin and Blockchain start-ups surged from $2.13 million to $95.05 million. Over the next two years, funding grew an eye-popping 726% — hitting $690.18 million by the end of 2016.[31] Investment in the blockchain ecosystem nearly doubled again in 2016, reaching $1.1. billion by the end of that year.[32]

As the technology matures, start-ups are tackling more than just financial applications, as Nassbaum's Blockchain Ecosystem demonstrates. Shipping and logistics, art, and even HR are among the industries about to encounter Blockchain solutions.

— Provenance (Shipping, Retail, Art)

One feature of Blockchain, its ability to maintain indelible records, has proven particularly useful to merchants concerned with validating the origin of the products they buy and sell. The fight against counterfeits consumes the entire value chain, from brands and buyers to port authorities and customs officials. Provenance, a start-up based in Southeast Asia, has built a Blockchain application to leverage the indelible ledger to validate product 'proof of existence', and track the history and origin of goods.

The start-up is a boon to luxury brands who are turning to Provenance to help remove counterfeit goods from the market. Provenance is proving the applicability of Blockchain technology for wide-ranging, non-financial implementations.

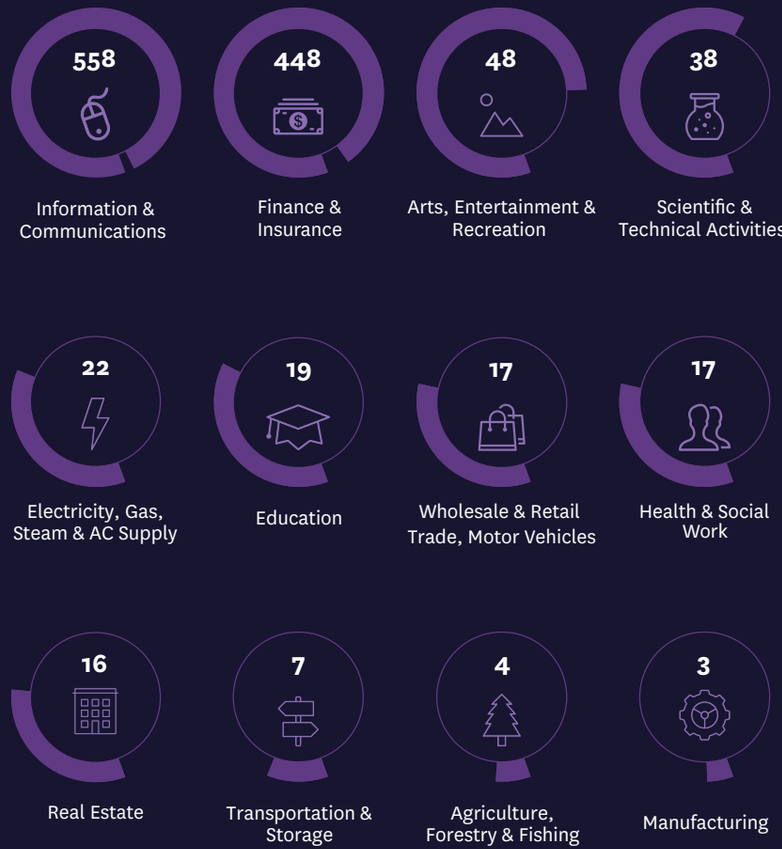
Industry watchers are keen to see Provenance take on the art world as well, where advancements in technology have led to a surge of counterfeits, creating a pressing need to tell truth from fiction.[33]

— Educhain (Education)

In the education space, degree and certification issuance and attestation is a surprisingly time consuming process requiring multi-step approvals and signatures. Smart Contracts on the Blockchain create an opportunity to automate the issuance of certificates and attest achievements in real time through a distributed ledger.

Educhain, a Canadian start-up that recently won second place in the Dubai Blockchain Challenge, is providing a solution for educators, students, and governments to remove current roadblocks surrounding the issuance of certificates, including diplomas. By utilising the Blockchain, Educhain is improving student experiences while reliably verifying the authenticity of certificates for academic institutions and governments.[35]

ACTIVE BLOCKCHAIN START-UPS PER SECTOR



Source: Outlier Ventures, 2017

EVERY ORGANISATION WILL BE ON BLOCKCHAIN

Early adopters in the Information & Communication industry and the Finance & Insurance industry, which stand to harness up to USD 10 billion in productivity savings from Blockchain, will lead adoption — but soon, every sector will benefit. Start-ups are already accruing success in industry ranging from Arts & Entertainment to Agriculture & Forestry.

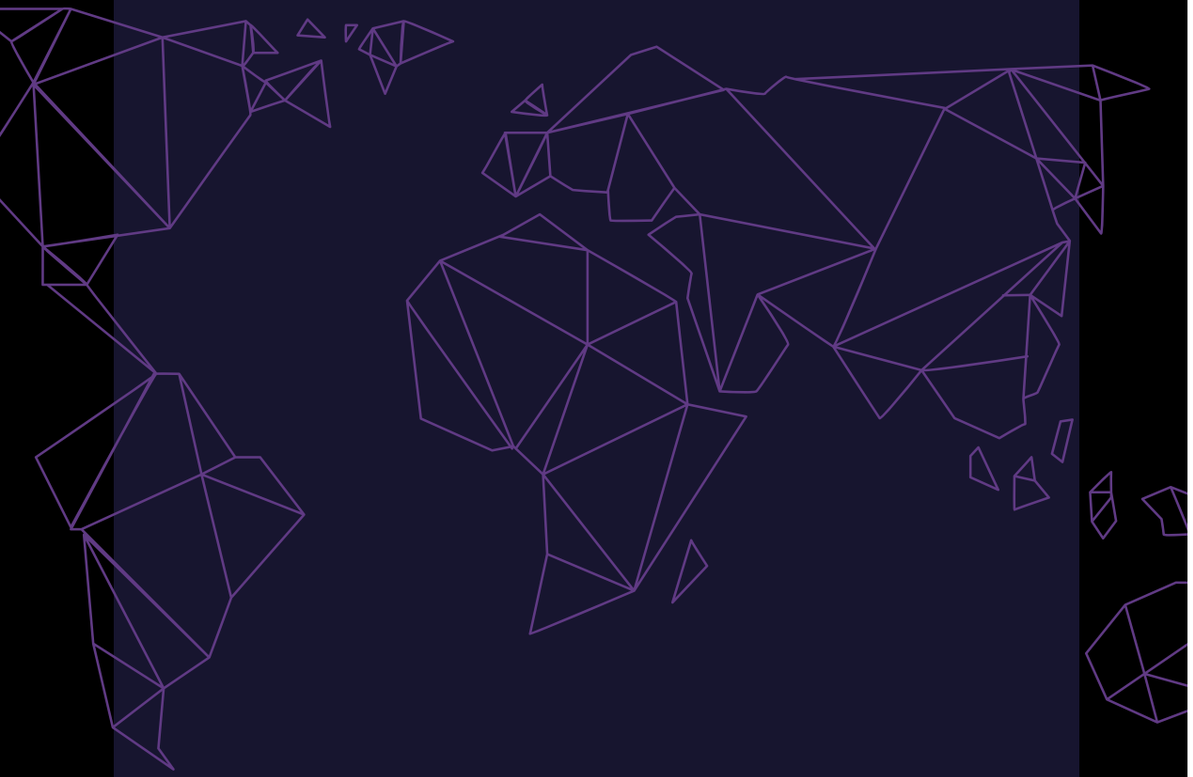
— Colony (Organisation Management)

Perhaps the most profound applications of Blockchain, however, will come not from any one sector or industry but from a radical disruption to the nature of work. To explore what work will look like when the potential of Blockchain is realised, concept artist Jack du Rose designed a thought experiment that utilises both Blockchain and artificial intelligence to manage a decentralised, autonomous organisation of real human beings.

The concept, called Colony, examines what happens when humans are removed from organisation management, and are instead allowed to focus purely on creative endeavours. By deploying Artificial Intelligence to manage tasks and initiate Smart Contracts, Colony creates a space for people to come together to work and create — on time and on budget — without pesky humans messing up the process.

Colony is a perfect storm of emerging technology and a thought-provoking look at what Blockchain might accomplish for society when we realise the potential of the Internet of Transactions.[34]

SPARKING A GLOBAL TECHNOLOGY REVOLUTION



1,200+ Start-ups
50+ Countries
30+ Governments
6 Continents

TRULY GLOBAL INNOVATION WAVE

The decentralised, stateless nature of Blockchain has sparked a global wave of innovation. Within a handful of years, thousands of blockchain projects by start-ups, institutions, and governments have taken root in every corner of the earth.

Source: Outlier Venture and Deloitte University Press, 2017

In March 2017, there were over 100 Blockchain pilots in progress, planned, or announced by more than 30 government agencies on six continents.

BOLD GOVERNMENTS

Governments' interest in Blockchain, which could be surprising given the technology's anti-establishment origins, seems to fulfil a prediction by Brad Peterson, who led the Blockchain project at Nasdaq OSX. While developed markets with centuries of financial inertia may be slow to adopt the Blockchain, he said, countries in the developing world, unhindered by institutional legacies, could "jump straight to the Blockchain".

By moving certain government functions to the Blockchain, where all transactions are publicly recorded and validated, governments have been able to weed out the corrosive influence of corruption and increase public trust. For large bureaucracies, Blockchain is also proving efficient at streamlining processes and removing the paperwork burden that frustrates citizens and drains government resources.

From effectively zero in 2013 to over two dozen today, government agencies across the globe are actively pursuing Blockchain implementations to introduce greater security, efficiency, and speed into all manner of government transactions. According to a recent report from Deloitte, there are as many as 64 government Blockchain pilots in progress across the globe, and another 50 pilots planned.[33]

"In 2020, the Dubai government will celebrate its last paper transaction."

- HIS HIGHNESS SHEIKH HAMDAN BIN MOHAMMED AL MAKTOUM, CROWN PRINCE OF DUBAI

— Dubai, UAE

Blockchain has proven particularly attractive to younger countries without a backlog of bureaucratic precedents to overcome. No where else is this trend more apparent than in the UAE, where the federal government and the local government of Dubai have embraced the technology wholeheartedly.

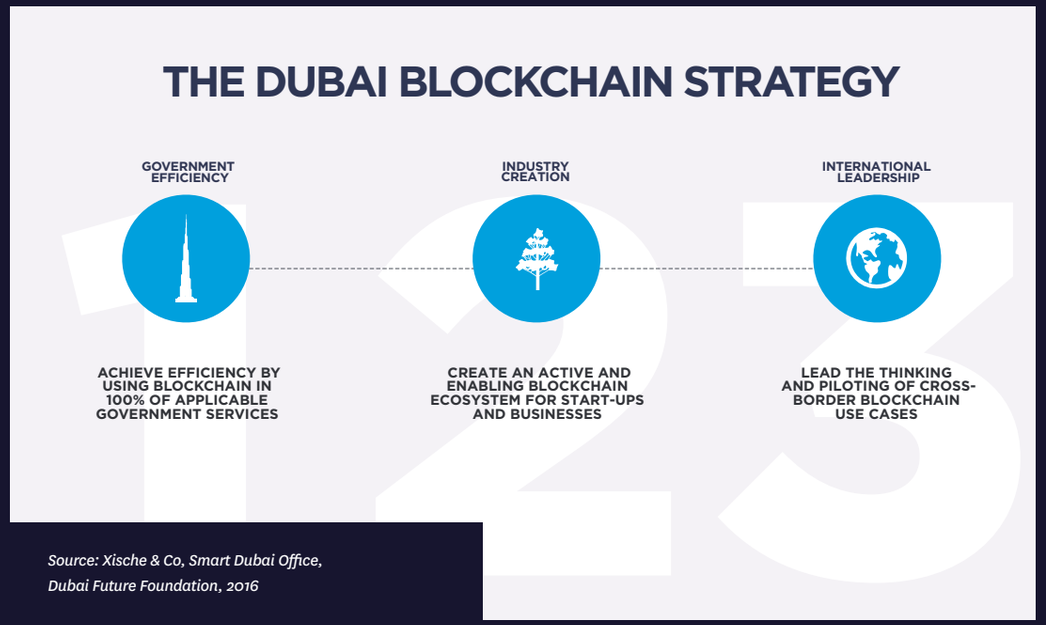
The Dubai Future Foundation, a government think tank charged with imagining and creating the future of the city ten to 50 years ahead of schedule, was instrumental in the establishment of the Global Blockchain Council in early 2016. The Council is made up of heavy-hitters from the technology sector, banks, and major industry players from a wide swath of backgrounds, including Emirates Airlines and Nasdaq Dubai. It was established to facilitate the exchange of knowledge on Blockchain pilot trends and policy development, and serve as a catalyst to Blockchain development in the region.

Within nine months, Dubai announced its own Blockchain strategy, led by the Dubai Future Foundation and the Smart Dubai Office, with a vision to bring 100% of all applicable government transactions onto the Blockchain by 2020. Dubai is bullish on Blockchain. In the words of the Crown Prince of Dubai, "In 2020, the Dubai government will celebrate its last paper transaction."[36]

According to some back-of-the-envelope calculations, Dubai stands to save up to $1.5 million every year by moving document processing to the Blockchain by 2020. That is the equivalent of delivering the cost of one Burj Khalifa — the world's tallest building, located in downtown Dubai — in savings to the economy, year on year.

To transform its vision into reality, Dubai is pursuing Blockchain implementation across all sectors. The government operates three accelerator programmes — Dubai Future Accelerators, the Dubai Blockchain Challenge, and the Dubai Smart City Accelerator — that bring international start-ups to Dubai to test and run Blockchain pilots from and for the city.[38]

As of March 2017, the UAE had announced seven Blockchain projects, the most in the developing world.[37] In Dubai, as many as 21 Blockchain projects have been identified by the end of the year.



Source: Xische & Co, Smart Dubai Office, Dubai Future Foundation, 2016

Part 5: The Age of Blockchain

By October 2017, one year after the launch of its strategy, Dubai showcased its first Blockchain pilot, an application to streamline land title transfers, at the annual GITEX exhibition. The system, developed in partnership with Smart Dubai, which seeks advisory support from IBM and Consensys to implement their Blockchain projects, uses Blockchain to provide a secure database that records all real estate contracts, including lease registrations, and links these with the local utility authority, the telecommunications system, and various property-related bills. The platform, which is also linked to residents' Emirates ID and residency visas, enables tenants to complete transactions electronically and from anywhere in the world.[39]

Image reused with permission under the Creative Commons Attribution-ShareAlike licence

— Ghana

The benefits of Blockchain extend beyond countries with established technology infrastructure and a robust knowledge economy.

As much as 90% of agricultural lands in Ghana are undocumented and unregistered. The Land Commission of Ghana, which is responsible for regulating land ownership and titles, is widely viewed as ineffective. Land disputes are commonplace among all participants in Ghana's real estate market, from mining operations and real estate developers to local subsistence farmers.

Bitland, a non-profit NGO headquartered in Ghana, has turned to Blockchain to build a trusted and indelible record of title statuses for unprotected land owners. Bitland is creating a redundant record of land ownership, providing citizens and farmers, as well as larger corporations, with a trusted certificate validating their possession should it be required in the event of a dispute.

Bitland is helping Ghana leapfrog decades of technology infrastructure development and entrenched bureaucratic processes to deliver value, security, and speed to its citizens with the Blockchain.

Inspired by the early success of the programme in Ghana, Bitland is now building its own cryptotoken wallet and Land Registry Blockchain to extend Blockchain technology at scale to all African nations.[40]

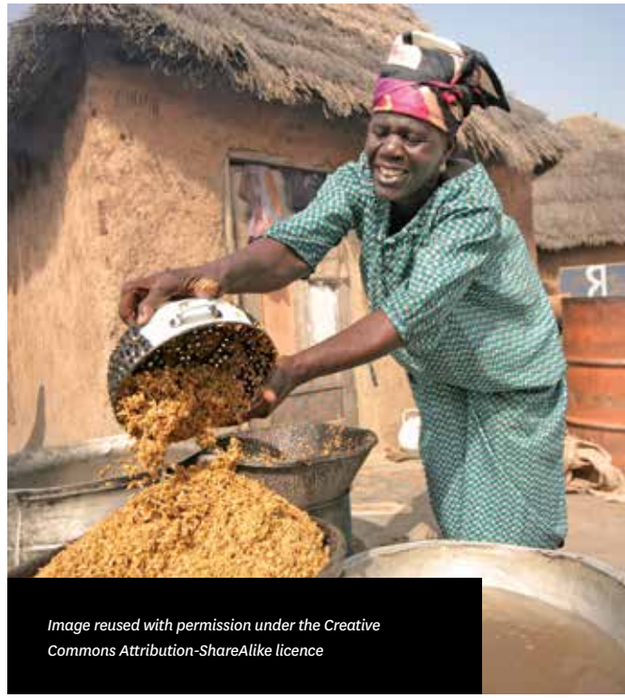


Image reused with permission under the Creative Commons Attribution-ShareAlike licence

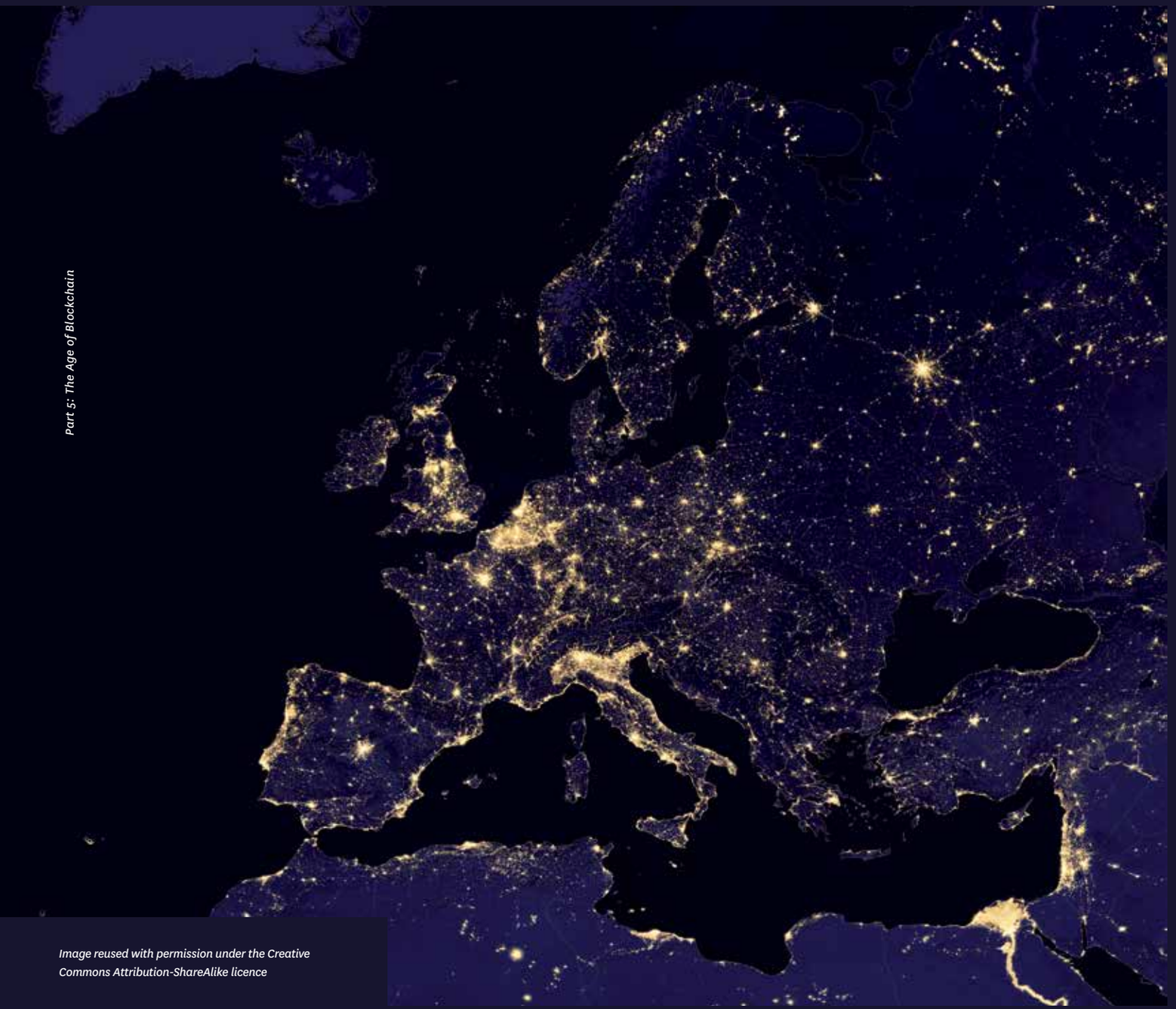


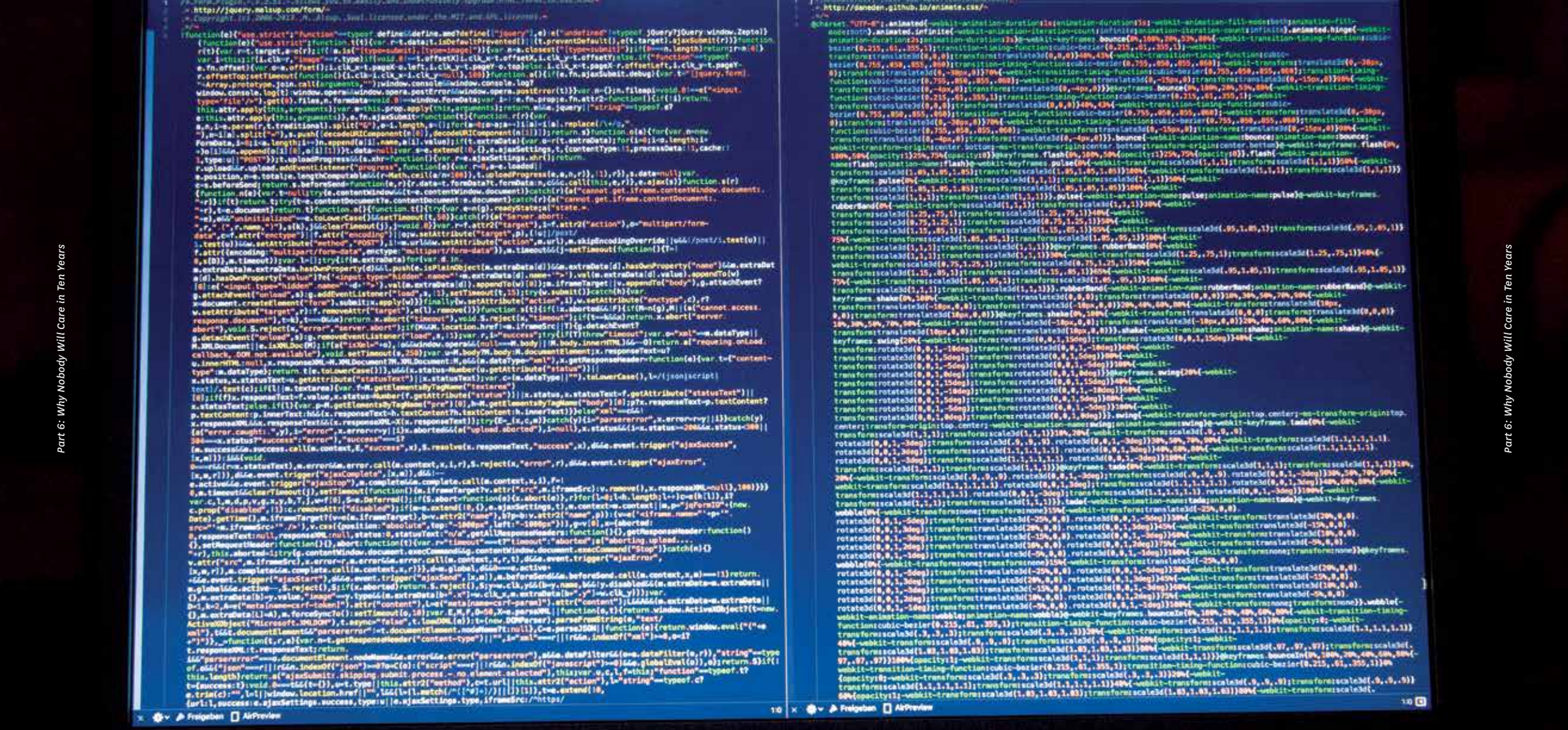
Image reused with permission under the Creative Commons Attribution-ShareAlike licence

— Estonia

Estonia made waves a few years ago by rolling out an e-Citizenship programme for all Estonian citizens — and anyone else in the world who was interested in joining the former Soviet-bloc country's digital experiment.[41] Estonia's e-citizen IDs were secured with public key infrastructure, a system for double-blinding user identities that is integral to the blockchain: Public key infrastructure enables anonymous participation in a network.

As Blockchain technology emerged, Estonia moved quickly to integrate its existing infrastructure with the Blockchain, becoming the first nation to implement Blockchain at a country level. Estonia designed the Keyless Signature Infrastructure (KSI) Blockchain to ensure the government's critical networks, systems, and data are free of compromise while retaining 100% data privacy.

Estonia's KSI Blockchain is now available in 180 countries.[42]



6. WHY NOBODY WILL CARE IN TEN YEARS

Part 6: Why Nobody Will Care in Ten Years

Interest in the Blockchain has continued to accelerate dramatically into late 2017. Major technology trade shows, including the Consumer Electronics Show in Las Vegas and the Smart City Expo and World Congress in Barcelona, featured panels on Blockchain for the first time in 2017.

Blockchain venture capital investment reached $107 million by Q1 2017. The aggregate cryptocurrency market cap reached an all-time high of $25 billion in Q1 2017.[43]

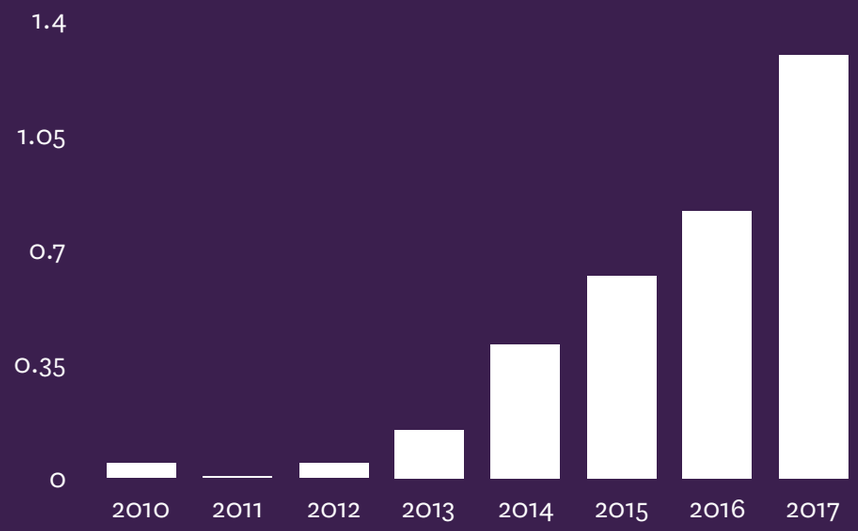
In 2017, industry heavyweights completed a significant pivot towards Blockchain. PwC (Vulcan Blockchain), Microsoft (Project Bletchley), JP Morgan (Juno and Quarom), IBM (Hyperledger and IBM Blockchain), Accenture, and Deloitte entered into the Blockchain market with meaningful stand-alone projects.[44]

Multiple reports point to adoption rates of 66 to 75% among banks and other financial institutions by 2020. In spite of a seeming peak of interest in Blockchain in 2017, adoption will only gain momentum in the coming years.

A report published by Grand View Research, a San Francisco-based market research and forecasting company, has predicted that the global Blockchain market will reach $7.74 billion by 2024.[45] Financial institutions will lead the charge, but the public sector will dominate the market in the coming decade, the report predicts. Public institutions and governments will increasingly turn to Blockchain to facilitate open and efficient transactions for the range of services that undergird civic life — from municipal fees to vehicle inspections to voting.

INVESTMENT IN BLOCKCHAIN IS ACCELERATING

TOTAL FUNDING RAISED BY BLOCKCHAIN START-UPS IN BILLION USD



Part 6: Why Nobody Will Care in Ten Years

$7.74 BN

BLOCKCHAIN MARKET VALUE WORLDWIDE 2024

Following the surging growth and investment in Blockchain over the past four years, the worldwide blockchain technology market is forecast to reach $7.74 billion by 2024, according to recently released reports. Other sources predict an even greater impact, with blockchain achieving up to $20 billion expected value by 2024.

Source: Grand View Research, 2016

With interest in Blockchain at an all-time high, and the prospect of a billion-dollar market on the horizon, the technology has a long road ahead before the public can reap the benefits of widespread adoption envisioned by Blockchain evangelists.

THE DAO, PARITY AND THE RISKS OF BEING HUMAN

A favourite line of Blockchain enthusiasts is that the platform is 'tamper-proof'. Early adopters of Blockchain have praised the platform as the most secure solution for managing vast amounts of data. Others have pointed to the use of public and private key infrastructure as a meaningful solution to secure an individual's data privacy.

But tamper-proof does not mean threat-proof, and while Blockchain is capable of doing all these things, it is not a foolproof system. As the technology gains more attention, the rate of hacking attempts will also increase.

Image reused with permission under the Creative Commons Attribution-ShareAlike licence

Two landmark attacks against the Ethereum network serve as an apt reminder that the Blockchain, in spite of its massive decentralised databases and indelible ledger, is ultimately a human endeavour and not infallible.

The Decentralised Autonomous Organisation (DAO) on Ethereum utilised Smart Contracts on the Blockchain to facilitate venture funding for pre-approved companies. These companies could submit proposals for funding to the DAO, and investors would vote on whether or not to approve the request. Once 20% of investors approved the request, funds would be transferred automatically to the company's wallet. In case an investor wanted, for whatever reason, to leave the organisation, the programme's developers built in a 'splitting function' to allow investors to withdraw from the DAO and regain the capital they had leveraged when signing up: the DAO raised an equivalent to $150 million in its first month.[47]

Despite initial success, The DAO was hacked less than two months after it was formed. Hackers exploited a bug in the 'splitting function' to drain over $70 million in funds from the DAO in a matter of hours. The Ethereum community was able to stop the attack by re-writing the rules of the platform to permit a transaction to be reversed. Part of 'indelible' is 'irreversible'.

The action saved millions of dollars for DAO investors but led to a contentious 'hard fork' in the Ethereum Blockchain. Today there are actually two Ethereum cryptocurrencies: Ethereum (users who accept the fork) and Ethereum Classic (users who did not agree with the fork). Hard forks are destabilising for the network.[47]

In a separate attack, hackers were able to withdraw $30 million from Ethereum users by exploiting an error in the code for a digital wallet in the Parity Smart Contract, which allowed hackers to reprogramme wallets in their name, then simply withdraw all of the funds within that wallet. The attack was stopped, but the money could not be returned.[47]

Neither attack was caused by a flaw in Ethereum or in the Blockchain. Mistakes were made in the coding for a particular programme and maliciously exploited. Security is hard. Attackers only have to be successful once, but defenders have to be successful every time. And on a distributed network like Blockchain, the risk is even higher: an attack on one ledger is an attack on every ledger.[24]

So, what can we do?

Being indelible means once a piece of Blockchain code is out there, it is in the world to stay, along with any mistakes, bugs, or vulnerabilities built into it. Just as Blockchain Smart Contracts have introduced cutting-edge cryptography, Blockchain programmers will need to introduce cutting-edge programming languages as resistant as humanly possible to error and attack.[24]

Blockchain programmers are among the smartest and most dedicated in the world, but there is still a lot to do if this technology will truly transform how we transact on the internet in the future.

BLOCKCHAIN FOR EVERY ORGANISATION

If all goes according to plan — and there's no reason to expect it won't — Blockchain will be embedded within nearly every organisation on the planet in the next decade.[47]

Business, by definition, is the exchange of goods or services in fulfilment of a contract. Blockchain can regulate every step of that equation. Every stage of a business life-cycle in any sector can be enhanced by Smart Contracts on Blockchain.

Smart Contracts in the music industry can be deployed by artists to ensure their intellectual property is protected, and to make sure they receive payment for their work whenever an album or song is downloaded. The British recording artist Imogen Heap has emerged as a Blockchain pioneer and evangelist, working to introduce the benefits of an indelible ledger and self-executing smart contracts to the music industry.[48]

Through smart contracts, musicians can automatically receive payments for a song and, as Imogen Heap has done, automatically share royalties with everyone who contributed to the making of the song.

Blockchain is also being explored as a legal and mutually remunerative reincarnation of Napster. Through its distributed network and ledger technology, Blockchain can support an open, peer-to-peer music library that simultaneously allows fans access to all of their favourite music while ensuring artists get paid for their work.

In the art world, Blockchain can be deployed to open a digital market for investors and artists, simultaneously assessing and validating the worth of an artwork, and recording the exchange of possession between artist and buyer. As forgery techniques become even more advanced, Blockchain networks can also be deployed to verify an artwork's origins, helping would-be investors differentiate between an original Monet and an Artificial Intelligence copy.

Experts are also exploring use cases for Blockchain in the more routine field of human resources, where the Blockchain ledger could present a welcome alternative to the often time-consuming process of verifying references for new hires. With an employee's work record and referrals stored on a Blockchain ledger, hiring managers can quickly asses a candidate's fit for a role.[47]

Self-executing contracts on the Blockchain can also dramatically reduce payment turn-around times for client work. Companies in service, design, and consulting fields who have entered into a Smart Contract with a client can receive payment for services within moments of the client signing a delivery note, reducing the payment processing period from weeks to seconds. And because the contract terms and transaction history are permanently stored on the Blockchain, the audit trail is tamper-proof.

Businesses of all sizes should investigate the potential role of Blockchain in their organisation and be ready to embrace the technology as it matures. Mass adoption will come sooner than you think.

A CLOSING DOSE OF REALITY

The internet existed for nearly a decade and a half before the World Wide Web was invented in 1989.

Like Blockchain, the early web remained staunchly in the domain of academics, technology firms, computer geeks, and open-minded governments. Then, in 1992, the first multimedia graphic browser, Mosaic, opened the internet to the masses.[49]

Within a year, the World Wide Web grew from 24 websites to over 1 million. Netscape launched in 1993. AOL rolled out its iconic CD-ROM campaign one year later. By 1995, 16 million people were using the Internet. By 2000, that number had soared to 361 million. Today, 3.8 billion people are online.[50]

The World Wide Web has become so ubiquitous that most people confuse the platform with the internet itself.[25]

Mosaic transformed the World Wide Web by making it visually appealing and easy to use, and in so doing rewrote how we live and interact with the world. Will Blockchain ever achieve the same degree of influence on our daily lives?

Today, the Blockchain interface is still largely code-based. While governments, start-ups, and banks have gotten involved, it is still largely in the domain of computer science experts, much like the early 1990s, before the World Wide Web took off.

Unless a new, user-friendly experience for Blockchain emerges, it is unlikely that the technology will ever reach such global prominence as the Web. Although the team behind Ethereum is trying, the platform's interface is still a terminal-based interaction. While Smart Contracts might eventually achieve a user interface more akin to a webpage or mobile app, the Blockchain will never attain the same level of visibility to the average user as the World Wide Web.

For all its acclaim, Blockchain is a closer kin to html, the standard markup language for creating web pages and web applications. Most people recognise it, some use it, and a few know what it is truly capable of. And that is probably fine.

Whereas the value of the web is understood through the opportunities it has created, the value of Blockchain will most strongly be felt through what it reduces in time, effort, and resources.

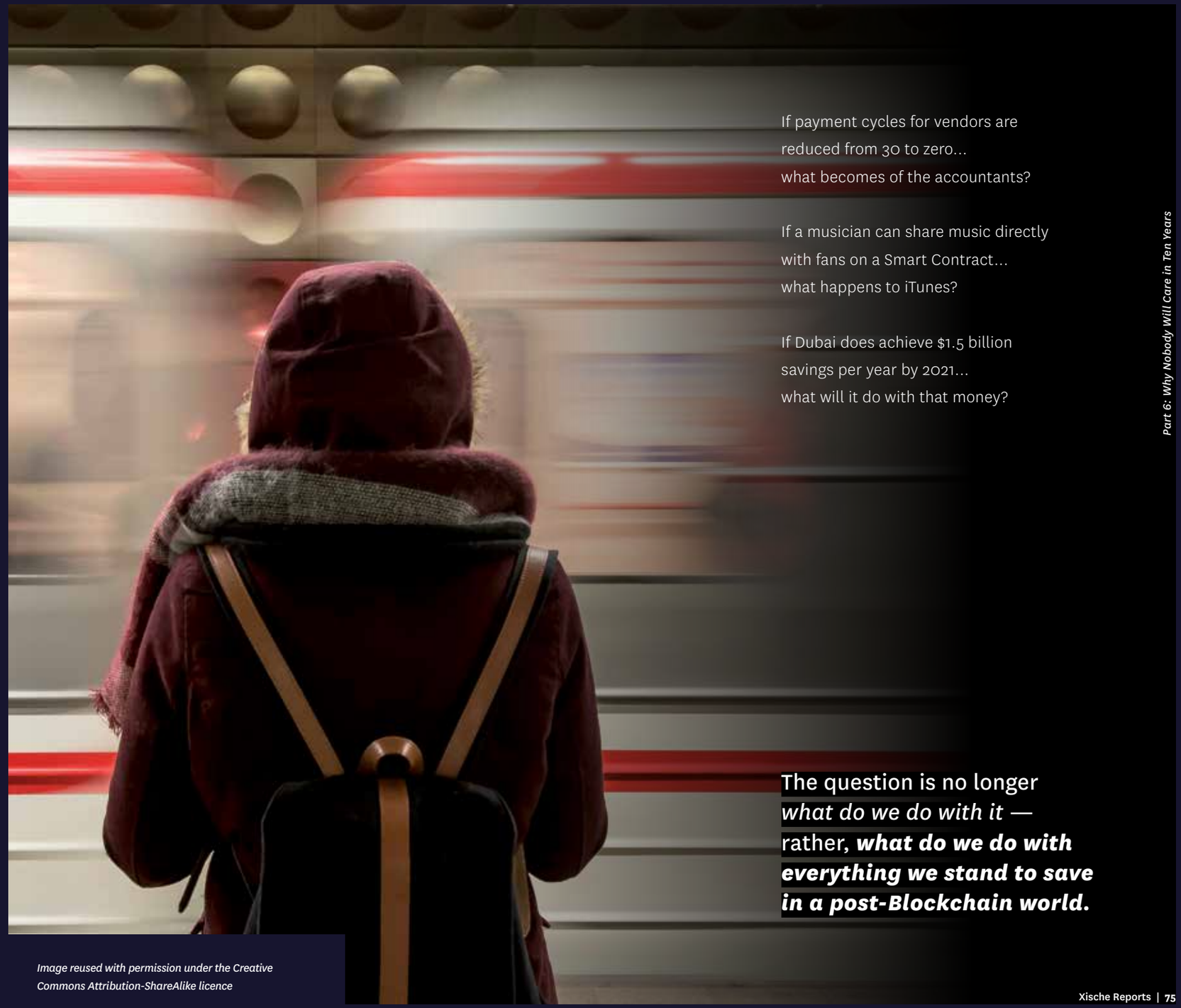


Image reused with permission under the Creative Commons Attribution-ShareAlike licence

If payment cycles for vendors are reduced from 30 to zero…
what becomes of the accountants?

If a musician can share music directly with fans on a Smart Contract…
what happens to iTunes?

If Dubai does achieve $1.5 billion savings per year by 2021…
what will it do with that money?

The question is no longer *what do we do with it* — rather, ***what do we do with everything we stand to save in a post-Blockchain world.***

Part 6: Why Nobody Will Care in Ten Years

REFERENCES

1. 10 Key Marketing Trends for 2017 and Ideas for Exceeding Customer Expectations. (2017). IBM. https://public.dhe.ibm.com/common/ssi/ecm/wr/en/wrl12345usen/watson-customer-engagement-watson-marketing-wr-other-papers-and-reports-wrl12345usen-20170719.pdf

2. Hern, A. (2017, Sept. 19). Equifax: credit firm was breached before massive May hack. Retrieved Nov. 15, 2017 from https://www.theguardian.com/technology/2017/sep/19/equifax-credit-firm-march-breach-massive-may-hack-customers

3. "New Threats in Healthcare Cybersecurity: 2017." IT Strategy, www.itstrategyinc.com/blog/healthcare-threats-2017.

4. Thompson, D. "Bitcoin is a Delusion That Could Conquer the World." (Nov. 30, 2017) The Atlantic. https://www.theatlantic.com/business/archive/2017/11/bitcoin-delusion-conquer-world/547187/

5. Szabo, N. (1970, Jan. 01). Unenumerated. Retrieved November 12, 2017 from http://unenumerated.blogspot.ae/2005/12/bit-gold.html

6. E. (n.d.). Ethereum/wiki. Retrieved Nov. 12, 2017 from https://github.com/ethereum/wiki/wiki/White-Paper#history

7. DigiCash loses U.S. toehold. (1998, September 02). Retrieved Nov. 12, 2017 from https://www.cnet.com/news/digicash-loses-u-s-toehold/

8. Dai, W. (1998). Retrieved Nov. 15, 2017 from http://www.weidai.com/bmoney.txt

9. Popper, N. (2015, May 15). Decoding the Enigma of Satoshi Nakamoto and the Birth of Bitcoin. Retrieved Nov. 12, 2017 from https://www.nytimes.com/2015/05/17/business/decoding-the-enigma-of-satoshi-nakamoto-and-the-birth-of-bitcoin.html

10. Nakamoto, S. (2008, Oct. 31). Bitcoin P2P e-cash paper. Retrieved Nov. 12, 2017 from http://article.gmane.org/gmane.comp.encryption.general/12588/

11. Nakamoto, S. (2008, Oct. 31). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf

12. Méndez, S. (2015, Mar. 31). The Global Economic & Financial Crisis: A Timeline. Retrieved Nov. 12, 2017 from https://www.slideshare.net/sandermendez/the-global-economic-financial-crisis-a-timeline

13. Dai, W, Nakamoto, S. (2017, September 17). Dai/Nakamoto emails. Retrieved Nov. 12, 2017 from https://www.gwern.net/docs/bitcoin/2008-nakamoto

14. Madeira, A. (2017, Sept. 28). What is the Bitcoin Genesis Block? Retrieved Nov. 15, 2017 from https://www.cryptocompare.com/coins/guides/what-is-the-bitcoin-genesis-block/

15. Francis Elliott, Deputy Political Editor, and Gary Duncan, Economics Editor. (2009, Jan. 03). Chancellor Alistair Darling on brink of second bailout for banks. Retrieved Nov. 12, 2017, from https://www.thetimes.co.uk/article/chancellor-alistair-darling-on-brink-of-second-bailout-for-banks-n9l382mn62h

16. Zetter, Kim. "Bullion and Bandits: The Improbable Rise and Fall of E-Gold." Wired, Conde Nast, 9 Jun. 2009, www.wired.com/2009/06/e-gold/

17. Bitcoin Price Hits $500, a 50x Increase in Just 12 Months. (2013, Nov. 19). Retrieved Nov. 12, 2017 from https://www.coindesk.com/bitcoin-price-hits-500-50x-increase-12-months/

18. Dzieza, J. (2014, Sept. 19). Regulators and Law Enforcement Boost Bitcoin's Prospects. Retrieved Nov. 12, 2017 from https://www.technologyreview.com/s/521636/regulators-see-value-in-bitcoin-and-other-digital-currencies/

19. Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies. (n.d.). Retrieved Nov. 12, 2017 from https://dig.watch/resources/application-fincens-regulations-persons-administering-exchanging-or-using-virtual

20. Metz, C. (2017, Jun. 06). Bitcoin May Never Make It to Wall Street, But Its Tech Will. Retrieved November 12, 2017 from https://www.wired.com/2015/05/nasdaq-bringing-bitcoin-closer-stock-market/

21. Metz, C. (2015, Dec. 17). Tech and Banking Giants Ditch Bitcoin for Their Own Blockchain. Retrieved November 12, 2017 from https://www.wired.com/2015/12/big-tech-joins-big-banks-to-create-alternative-to-bitcoins-blockchain/

22. Ethereum Project. (n.d.). Retrieved Nov. 12, 2017 from https://www.ethereum.org/

23. What is Ethereum? - CoinDesk Guides. (2017, March 31). Retrieved November 12, 2017 from https://www.coindesk.com/information/what-is-ethereum/

24. Qureshi, Haseeb. "A hacker stole $31M of Ether - how it happened, and what it means for Ethereum." FreeCodeCamp, FreeCodeCamp, 20 Jul. 2017, medium.freecodecamp.org/a-hacker-stole-31m-of-ether-how-it-happened-and-what-it-means-for-ethereum-9e5dc29e33ce

25. History of the Web. (n.d.). Retrieved Nov. 15, 2017 from https://webfoundation.org/about/vision/history-of-the-web/

26. Nussbaum, Josh. "Blockchain Project Ecosystem – Josh Nussbaum – Medium." Medium, Medium, 13 Oct. 2017, www.medium.com/@josh_nussbaum/blockchain-project-ecosystem-8940ababaf27

27. Blockchain Could Start Making Some Real Waves the Banking Industry Next Year. (2016, Sept. 28). Retrieved Nov. 12, 2017 from http://fortune.com/2016/09/28/blockchain-banks-2017/

28. These Banks Are Testing an Intel-Powered Blockchain Platform for Bond Transactions. (2016, Sept. 26). Retrieved Nov. 12, 2017 from http://fortune.com/2016/09/26/intel-blockchain-bonds/

29. Neghaiwi, B. H. (2017, August 31). Six big banks join blockchain digital cash settlement project. Retrieved November 12, 2017 from https://www.reuters.com/article/us-blockchain-banks/six-big-banks-join-blockchain-digital-cash-settlement-project-idUSKCN1BB0UA

30. Emirates NBD launches 'Cheque Chain' to integrate blockchain technology into cheques. (2017, May 1). Retrieved Nov. 12, 2017 from https://www.emiratesnbd.com/en/media-centre/media-centre-info/?mcid_en=445

31. Allidina, Sarah. "The future of blockchain in 8 charts." Raconteur, Raconteur Media Ltd., 28 Jun. 2016, www.raconteur.net/business/the-future-of-blockchain-in-8-charts

32. Ramada, M. For insurers #blockchain is the new black. (2016, December 28). Retrieved December 17, 2017 from https://blog.willis.com/2016/12/for-insurers-blockchain-is-the-new-black/

33. Madeira, Antonio. "The DAO, The Hack, The Soft Fork and The Hard Fork." CryptoCompare, 28 Sept. 2017, www.cryptocompare.com/coins/guides/the-dao-the-hack-the-soft-fork-and-the-hard-fork/

34. Thompson, C. (2016, Jan. 08). The Top 10 Blockchain Startups to Watch in 2016 – The Blockchain Review – Medium. Retrieved November 12, 2017, from https://medium.com/blockchain-review/the-top-10-blockchain-startups-to-watch-in-2016-the-leaders-who-are-changing-the-game-6195606b0d70

35. Educhain. (n.d.). Retrieved Nov. 15, 2017 from https://educhain.io/

36. Al Ramahi, Nawal. (2017, Apr. 16). "All Dubai Goverment Departments to be Paperless in Four Years, Says Sheikh Hamdan." The National. https://www.thenational.ae/uae/all-dubai-government-departments-to-be-paperless-in-four-years-says-sheikh-hamdan-1.77291

REFERENCES

37. Killmeyer, Jason, et al. Will blockchain transform the public sector? Deloitte University Press, 2017.

38. Smart Dubai. Dubai Blockchain Strategy. Retrieved from http://smartdubai.ae/dubai_blockchain.php

39. Report, S. (2017, October 07). Dubai Land Department becomes world's first government entity to conduct all transactions through Blockchain network. Retrieved Nov. 12, 2017 from http://gulfnews.com/business/sectors/technology/dubai-land-department-becomes-world-s-first-government-entity-to-conduct-all-transactions-through-blockchain-network-1.2102060

40. Bitland | Real Estate Land Title Registration Ghana | Blockchain Land Security Africa 2016. (n.d.). Retrieved Nov. 12, 2017 from http://bitlandglobal.com/

41. Korjus, K. (2017, July 07). Welcome to the blockchain nation – E-Residency Blog – Medium. Retrieved Nov. 12, 2017 from https://medium.com/e-residency-blog/welcome-to-the-blockchain-nation-5d9b46c06fd4

42. KSI Blockchain. (n.d.). Retrieved Nov. 12, 2017 from https://e-estonia.com/solutions/security-and-safety/ksi-blockchain/

43. "State of Blockchain: Q1 2017." CoinDesk, 22 Jun. 2017, www.coindesk.com/research/state-blockchain-q1-2017/

44. "6 Trends From CoinDesk's New 2017 State of Blockchain Out Today." CoinDesk, 19 May 2017, www.coindesk.com/6-top-trends-coindesks-2017-state-blockchain-report/

45. "Blockchain Technology Market Size Worth USD 7.74 Billion By 2024." Grand View Research, Dec. 2016, https://www.grandviewresearch.com/press-release/global-blockchain-technology-market

46. Madeira, Antonio. "The DAO, The Hack, The Soft Fork and The Hard Fork." CryptoCompare, 28 Sept. 2017, www.cryptocompare.com/coins/guides/the-dao-the-hack-the-soft-fork-and-the-hard-fork/

47. Mamoria, Mohit. "Every company will use blockchain by 2027 – Hacker Noon." Hacker Noon, Hacker Noon, 21 Oct. 2017, hackernoon.com/your-company-will-use-blockchain-in-less-than-10-years-heres-how-6d9da452fa8d.

48. Heap, I. (2017, July 06). Blockchain Could Help Musicians Make Money Again. Retrieved November 15, 2017 from https://hbr.org/2017/06/blockchain-could-help-musicians-make-money-again

49. History of the Web. (n.d.). Retrieved November 15, 2017 from https://webfoundation.org/about/vision/history-of-the-web/

50. Internet Users 1995 - 2008. Global Policy Forum. Retrieved November 15, 2017 from https://www.globalpolicy.org/tables-and-charts-ql/27519-internet-users.html

INFOGRAPHIC REFERENCES

Sam Wouters, Blockchain Speaker and Consultant @ Duval Union Consulting Follow. (2016, Oct. 13). The future of Bitcoin & 9 ways to improve it. Retrieved Dec. 17, 2017 from https://www.slideshare.net/SamWouters/the-future-of-bitcoin-9-ways-to-improve-it

Nassbaum, J. (2017, Oct. 13). Blockchain Project Ecosystem – Josh Nussbaum – Medium. Retrieved Dec. 16, 2017 from https://medium.com/@josh_nussbaum/blockchain-project-ecosystem-8940ababaf27

Startup Tracker curated by Outlier Ventures. (Live). Retrieved Dec. 17, 2017 from https://outlierventures.io/startups/charts/

Killmeyer, Jason, et al. Will blockchain transform the public sector? Deloitte University Press, 2017.

Blockchain Technology Market Analysis By Type (Public, Private, And Hybrid), By Application (Financial Services, Consumer/Industrial Products, Technology, Media & Telecom, Healthcare, Transportation, and Public Sector), By Region, & Segment Forecasts, 2015 - 2024. (Dec. 2016). Grand View Research. Retrieved Dec. 17, 2017 from https://www.grandviewresearch.com/industry-analysis/blockchain-technology-market

NOTES

XISCHÉ
REPORTS

Xische & Co.
POBox 500601
A-202, Building 4
Dubai Design District
T +9714 367 8184

www.xische.com