An Introduction to Digital Assets

How blockchain technology is transforming our economy and society in the 21st century

August 2021

FÜRSTLICH CASTELL'SCHE BANK

Foreword

From a niche concept to a potential financial disruptor. More and more people are starting to take an interest in cryptocurrencies, blockchain and decentralised finance.

At the same time cryptocurrencies, and the blockchain concept that underpins them, are so often misunderstood. Is Bitcoin a currency? Will blockchain – a technology that stands for decentralisation – democratise financial power? Is this technology simply a game for enthusiasts, or do its applications stretch far beyond the technical aspects? These, and many more questions are often left unanswered or inadequately addressed.

I was personally first introduced to the subject a few years ago, at a junior football match. I had a discussion with another player's father, who happens to work at Deutsche Börse, the German stock exchange. At the time, I thought that decentralised finance was something that existed in the distant future, but I quickly realised how advanced it already was, and how it would only be a matter of time before this would disrupt not only finance, but many other areas.

We know that people have a tendency to overestimate the impact of technology in the short-term and underestimate it in the medium to long-term, a phenomena known as Amara's law. A few years have passed since that conversation, and an amazing €200bn has been invested by global corporates into building blockchain and decentralised finance (DeFi) technology and platforms.

This topic is so rich and complex, and changes so rapidly, that investors are seeking guidance and education. We have done thorough research, spoken to a number of outspoken experts and compiled this report to help you to understand and recognise how this new technology is transforming our economy, and potentially our entire society, in the 21st Century.

Christian Hille – CIO Fürstlich Castell'sche Bank

Blockchain Fundamentals

Towards a decentralised economy

to chapter

Blockchain Applications

The emerging token economy for payments, services and securities

to chapter

The Digital Asset Market

Blockchain's place in the financial system

to chapter

Environmental & Social Impact

Thinking "outside the blocks"

to chapter

Learn more

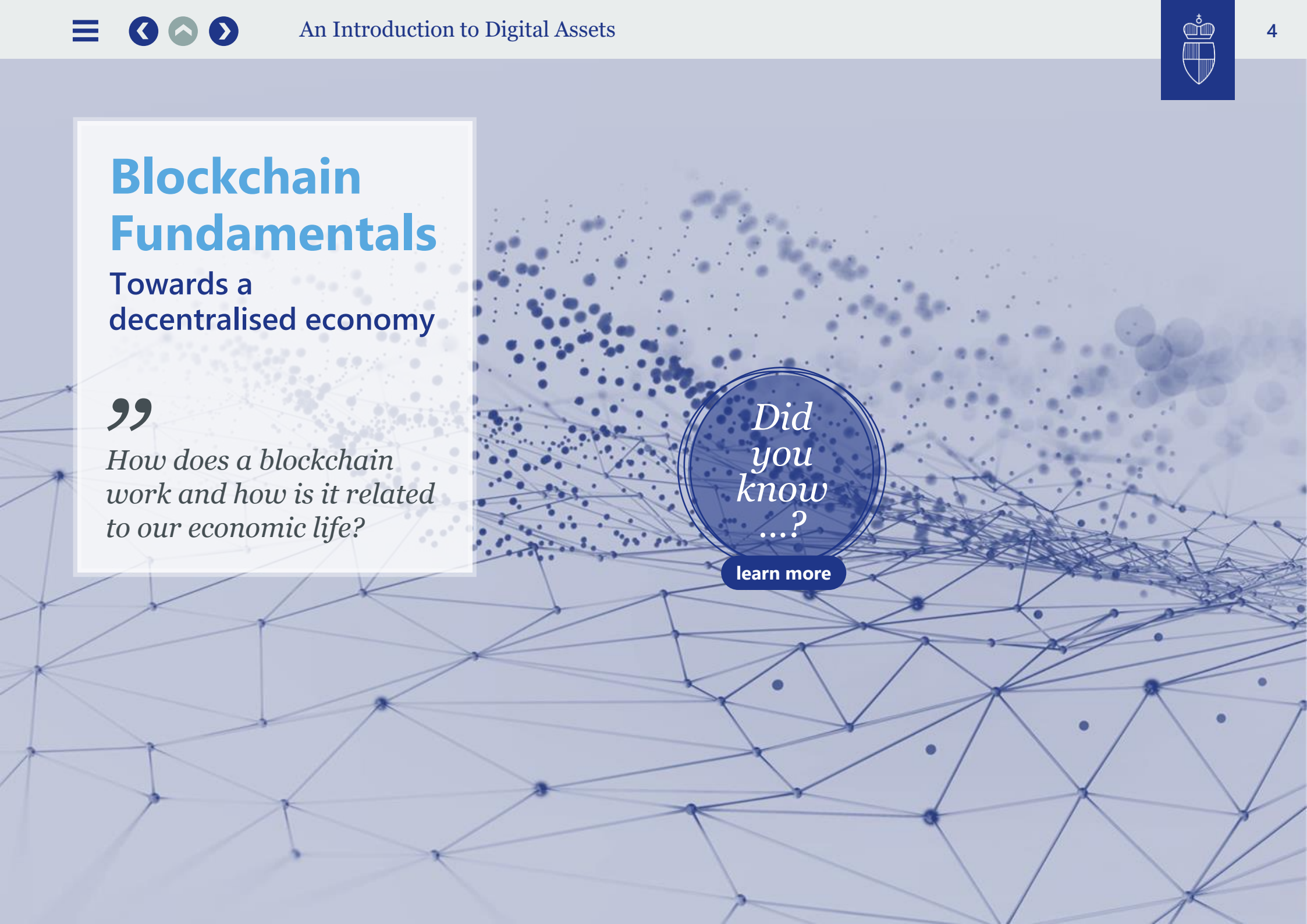
Authors, references & technical glossary

to appendix

Blockchain Fundamentals

Towards a decentralised economy

How does a blockchain work and how is it related to our economic life?



Did you know…?

Companies globally are expected to spend approx.

$20bn/year

on blockchain technical services by 2024[1]

Bitcoin's entire blockchain size is

338 Gigabytes

comparable to streaming 85 HD movies on Netflix[2]

The market value of Coinbase at initial public offering was

$100bn

more than Deutsche Bank, Commerzbank and Deutsche Börse combined[3]

1) Mitic (2021)
2) Statista (2021) & Reinhardt (2021)
3) Hinchliffe (2021) & Bloomberg L.P.

The origins: A quest for decentralisation (1/3)

On the 31st October 2008, less than two months after Lehman Brothers had filed for bankruptcy, a paper was sent out to a small mailing list of computer science enthusiasts that would change the course of economic history.

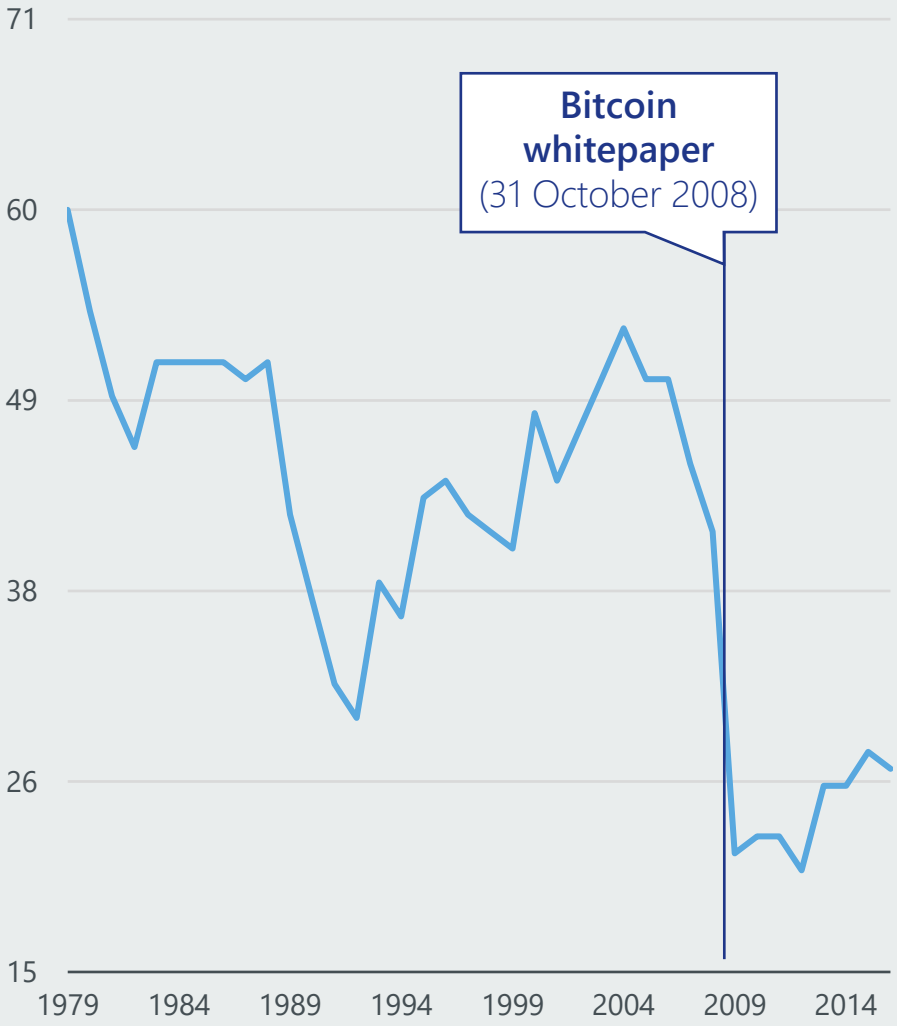
Written by an unknown author under the pseudonym of Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" outlined a concept that disrupted the world of banking and gave birth to a new capital market.

At a time when trust in the financial system was at the lowest it had been in decades, the document outlined a fully decentralised digital payment system — one that would no longer rely on financial institutions at all.

At the core of the system proposed by Nakamoto was a technology called blockchain.

The GFC – a turning point for trust and finance

Public confidence in US banking systems, % (Gallup, 2016)



The origins: A quest for decentralisation (2/3)

Bitcoin's central proposition was a fully decentralised system that allows users to make exchanges via a peer-to-peer network on the internet. Using the blockchain individuals can transact without the oversight of a central authority.

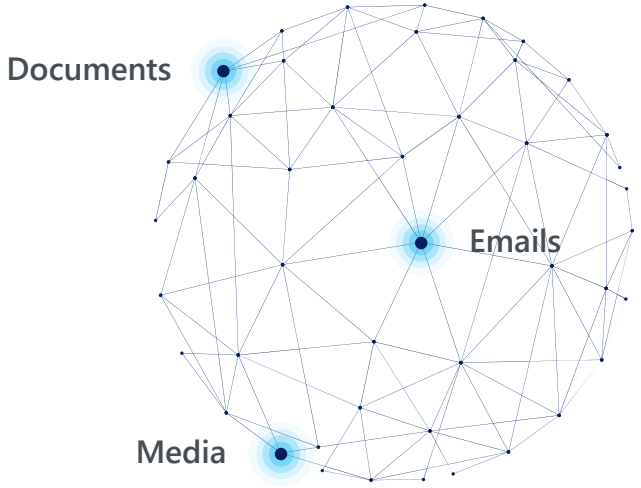
To fully grasp how revolutionary this idea is, first we need to understand how fundamentally the internet has evolved up to this point.

"Across the world today there are over 20 billion[1] interconnected devices."

The internet allows information to be passed directly between devices in the form of data such as emails, photos or video streams. These digital objects can be replicated and distributed infinitely without losing their informational value.

Today's online universe

An internet of information



1) IOT Analytics (2020)

The origins: A quest for decentralisation (3/3)

When it comes to economic interactions like banking, the entire system relies on scarcity. A value sum of money – represented in the form of data – can't simply be replicated and keep the same value. In digital economies this is known as the double-spending problem.

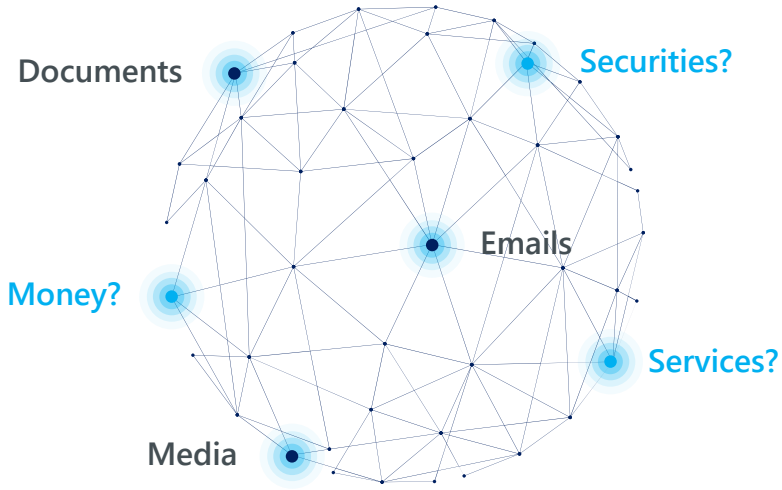
To avoid double-spending, banks maintain central databases, acting as an intermediary to ensure online transactions are legitimate. Crises such as the financial crash of 2008 highlighted the vulnerabilities of this centralised banking system, including single points of failure, corruption, data inconsistencies and settlement delays.

A blockchain is a **decentralised database** that records transactions transparently, anonymously and securely. This structure fundamentally replaces trust in authority with security through encryption, allowing for the direct exchange of assets in the same way that information is shared on the internet – without any intermediaries.

The real implications of this concept could be massive.

The next evolutionary step

An internet of assets?



The journey of a Bitcoin transaction

1

Alice wants to send Bob 1 bitcoin from her digital wallet.

2

A transaction file is created containing all relevant details.

3

Alice authorises and announces the payment using her secret "private key" password

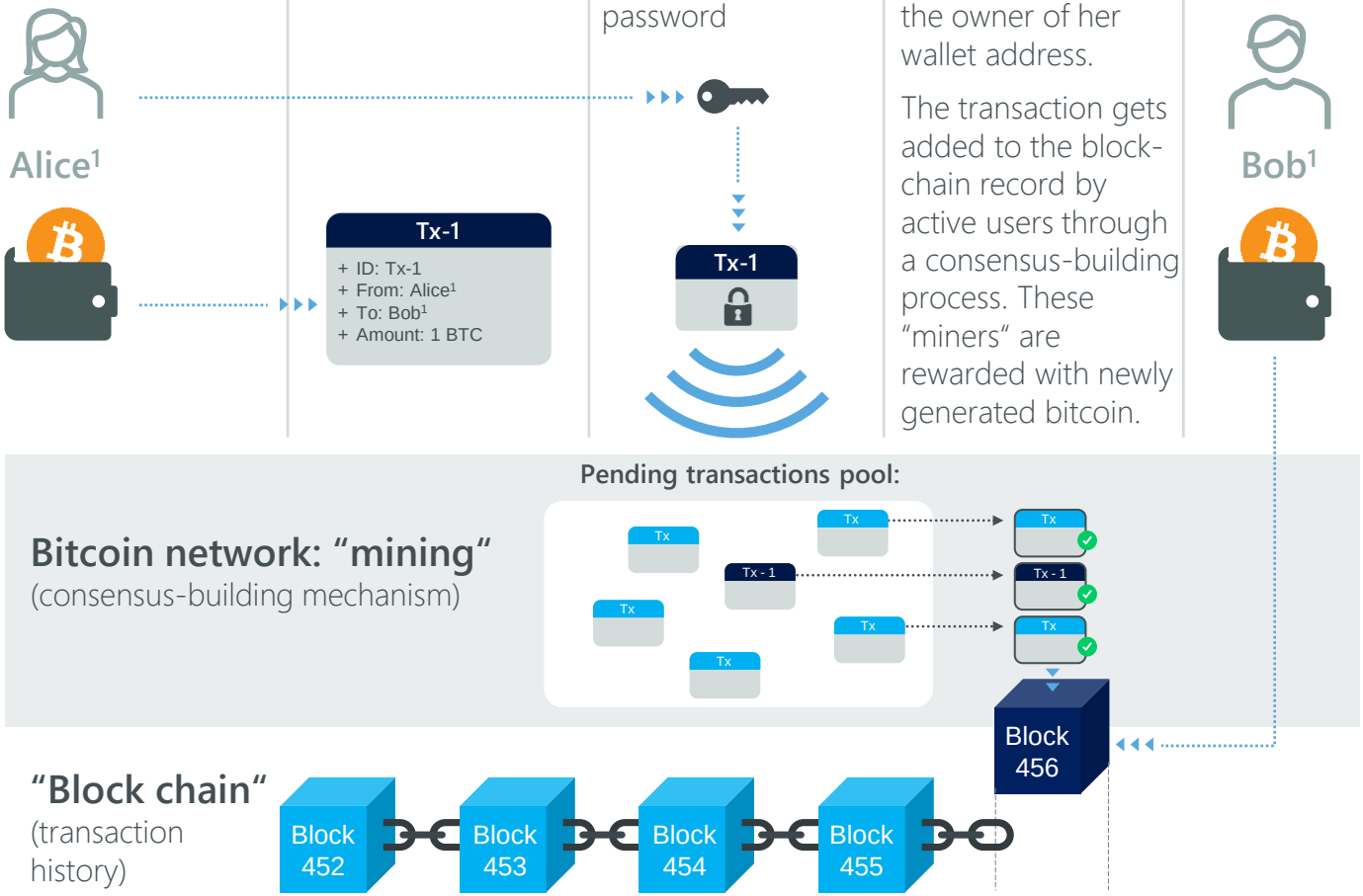
4

The network uses Alice's openly known "public key" to verify that she is indeed the owner of her wallet address.

The transaction gets added to the block-chain record by active users through a consensus-building process. These "miners" are rewarded with newly generated bitcoin.

5

Bob's wallet is now allowed to spend the transferred coins.



1) Note: user names shown for illustration purposes only – transactions only involve pseudonymous user addresses (see explanation on the right)

Some vocabulary

"A peer-to-peer ...

- Bitcoin facilitates transactions in a fully decentralised way
- Users interact directly with one another in an online network
- Users keep a copy of the entire transaction history (blockchain)

... immutable ...

- Blocks of transactions on the blockchain are linked in a securely encrypted sequence
- No user can manipulate the chain history as it would be rejected upon comparison with everyone else's chain

... auditable ledger."

- All transactions by all users are publicly visible, since everyone has a local blockchain copy
- However, only encrypted user addresses are stored – it is difficult to impossible to identify the person behind an address

Further details in appendix:

Learn more

Building consensus: Miners and validators

In a decentralised network without central oversight, a consensus-building mechanism is required to avoid double-spending. This prevents manipulations of the blockchain with false or duplicate transactions, and is essential for its overall security.

There are currently two major approaches to determine how blockchain network participants can come to a consensus about the state of the blockchain, and to verify and record new transactions:

A Proof-of-Work (PoW)

- PoW schemes like Bitcoin require users ("miners") to validate new entries to the blockchain. The miners commit computational resources to solve a complex mathematical puzzle.
- As a reward, the miners get paid in the cryptocurrency they are "mining" (e.g., Bitcoin). Similarly to the extraction of resources through real mining, this method is extremely energy-intensive.
- As with gold or fossil fuels, Bitcoin is a limited resource. There will only ever be a maximum of 21m coins in circulation.
- Proof-of-Work is the original and most widely used consensus mechanism. Bitcoin, Ether and most other applications currently operate using this mechanism.

B Proof-of-Stake (PoS)

- The PoS consensus mechanism does not require the users to solve a computational puzzle or have specialist hardware in order to validate transactions.
- In this mechanism, users are called "validators", because they validate transactions by depositing ("staking") some amount of cryptocurrency from their own wallet.
- As an incentive, validators are rewarded in the same currency. This has been compared to earning interest on a bank deposit.
- Proof-of-Stake is a lot less energy intensive than PoW but has so far only been tested on a relatively small scale. Ethereum has announced to switch to PoS in the foreseeable future.

Blockchain Applications

The emerging token economy for payments, services and securities

How could blockchain technology transform economies and where will it make the most impact?

Did you know ...?

learn more

Did you know…?

There are now more than

11,000

cryptocurrencies other than Bitcoin[1]

There are blockchain-powered

Social Networks

such as Steemit, GNU Social, and Sapien

"Digital art" sold in the first half of 2021 was worth

$2.5bn

comparable to half a year of Sotheby's auction revenues[2]

1) CoinMarketCap (2021)
2) Howcroft (2021) & Reimers (2021)

Blockchain in practice: A taxonomy of tokens

Bitcoin was proposed as an alternative world currency, but the underlying blockchain technology is what could potentially shape the future of money, government and business.

Two types of virtual objects that have emerged are standalone digital "coins" and "tokens" that are built on top of existing blockchain platforms like Ethereum. They can be used in fundamentally different ways:

bitcoin ...

Payment tokens are the purest form of cryptocurrencies, enabling the decentral transfer of digital money e.g. to purchase goods and services.

Bitcoin dominates this space but has inspired many alternative "Altcoins" over time.

Jump to section

ethereum Filecoin ...

Utility tokens provide access to specific services or goods (e.g. as an event ticket or for car sharing access), similar to vouchers.

They are bound to a single use case – for instance, Uber tokens may be redeemed for a ride but nothing else.

Jump to section

BLOCKCHAIN CAPITAL SCIENCE BLOCKCHAIN ...

Security tokens are very similar to utility tokens, but they represent an investment in an asset that already has value, e.g. company shares, bonds, or certificates.

Their key advantage is that issuers don't have to securitise these tokens through traditional clearing houses, registries etc.

Jump to section

"Pay"

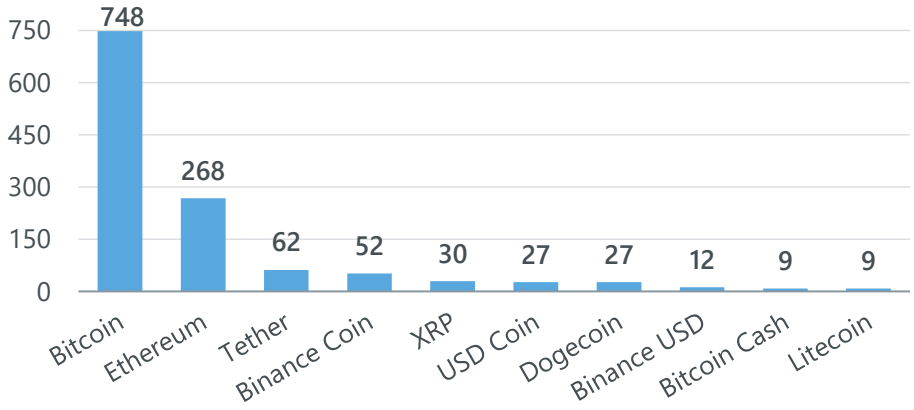
Decentralised currencies

Inspired by Bitcoin, today there are numerous cryptocurrencies available for payment transactions.

These "Altcoins" run on their own blockchain and differ in their technical implementations. For example, while new Bitcoin blocks are "mined" every 10 minutes, Litecoin produces blocks every 2.5 minutes.

Major payment-oriented cryptocurrencies[1]

By market capitalisation in USD bn (CoinMarketCap, July 2021)



Comparison of technical cryptocurrency features[1]

	Bitcoin	Ethereum	Bitcoin Cash	Litecoin	Monero
Key value proposition	Original blockchain and highly secure private payments	Native currency to power the Ethereum blockchain platform	Bitcoin protocol spin-off with larger blocks for higher scalability	Fast and secure payments with short block creation time	Privacy coin focused on enhanced user anonymity
Transactions/sec[2]	7	30	116	56	∞
Ø transaction fees	2.67 USD	5.92 USD	<0.01 USD	0.02 USD	0.03 USD
Consensus-building	Proof-of-Work mining	Proof-of-Work (switch to PoS planned)	Proof-of-Work mining	Proof-of-Work mining	Proof-of-work mining
Money creation	Capped at 21m (technically deflationary)	Unlimited supply at a fixed issuance schedule (disinflationary)	Capped at 21m (technically deflationary)	Total supply 84m (~75% mined)	Unlimited supply at a decreasing issuance rate

1) Snapshot data as of July 28, 2021 (Coinbase, 2021)
2) Numbers reflect theoretical or reported maximum transaction processing efficiency. In practice, processing speed fluctuates and usually remains significantly below efficiency limits

"Pay"

Stablecoins

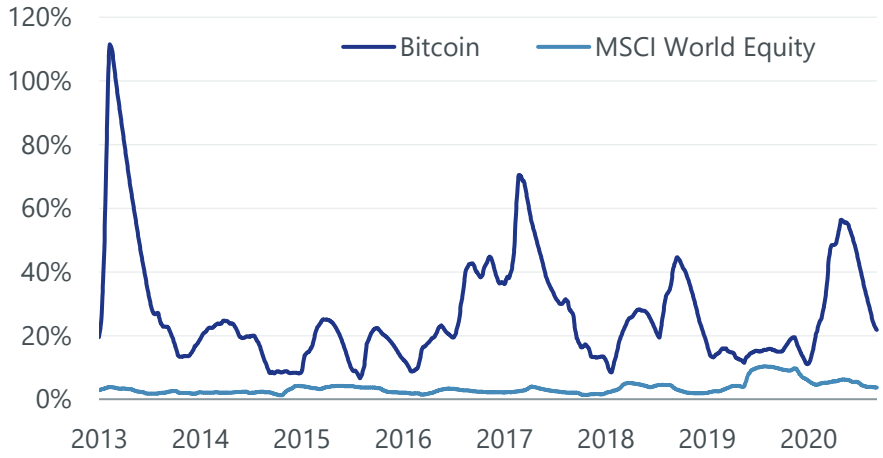
Cryptocurrencies are infamous for their volatility. Many investors have become millionaires overnight, only to see their wealth disappear weeks later.

Stablecoins share many benefits of cryptocurrencies (transparency, security, privacy) without their extreme price instability.

This is because, similar to the Gold Standard in the 20th century, the value of stablecoins is pegged to other assets such as the US dollar, gold or cryptocurrency baskets. One drawback of this is that this backing is usually managed by a central institution.

Crypto is significantly more volatile than stocks, even during market crashes like Covid-19[1]

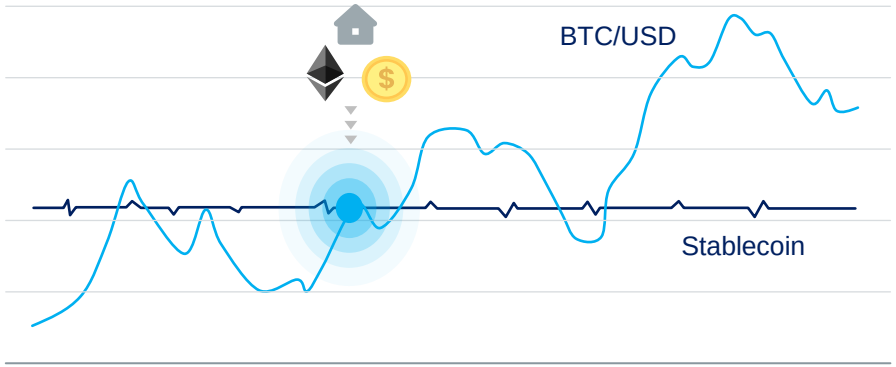
Rolling 6-month volatility in % of price mean



Examples of stablecoins

Name	Organisation	Asset backing
Tether	Centralised	USD currency
USD Coin	Centralised	USD currency
Binance USD	Centralised	USD currency
DAI	Decentralised	Cryptocurrency basket

Concept: stablecoins vs. pure cryptocurrency value

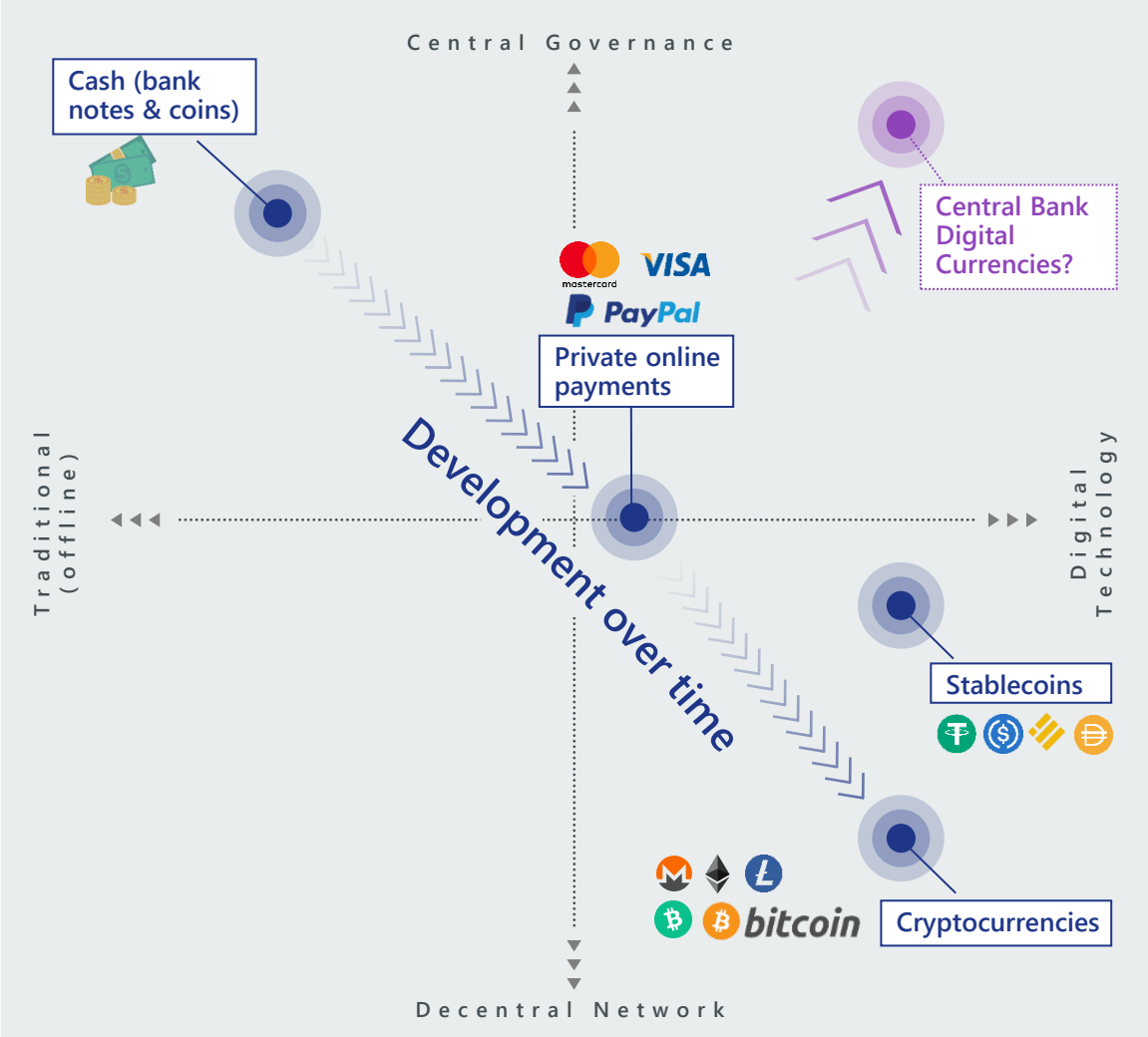


1) Bloomberg L.P.

"Pay"

Central Bank Digital Currencies

As we experience a global shift towards digital and mobile payment forms, central banks are exploring options to issue digital currency directly to end consumers. These central bank digital currencies (CBDCs), which may or may not operate on blockchain technology, would represent a huge change in the global monetary system.



The rationale for CBDCs

- Increases financial inclusion: bringing the "unbanked" into the payment system
- Effective monetary policy transmission with less interferences
- Potential efficiency gains by eliminating costly cash management processes
- Undercuts other digital currencies not managed through the central banking system

Variants of CBDCs

Wholesale: For financial institutions' central bank reserves
Retail: Digital cash issued to the public by the central bank

Outlook

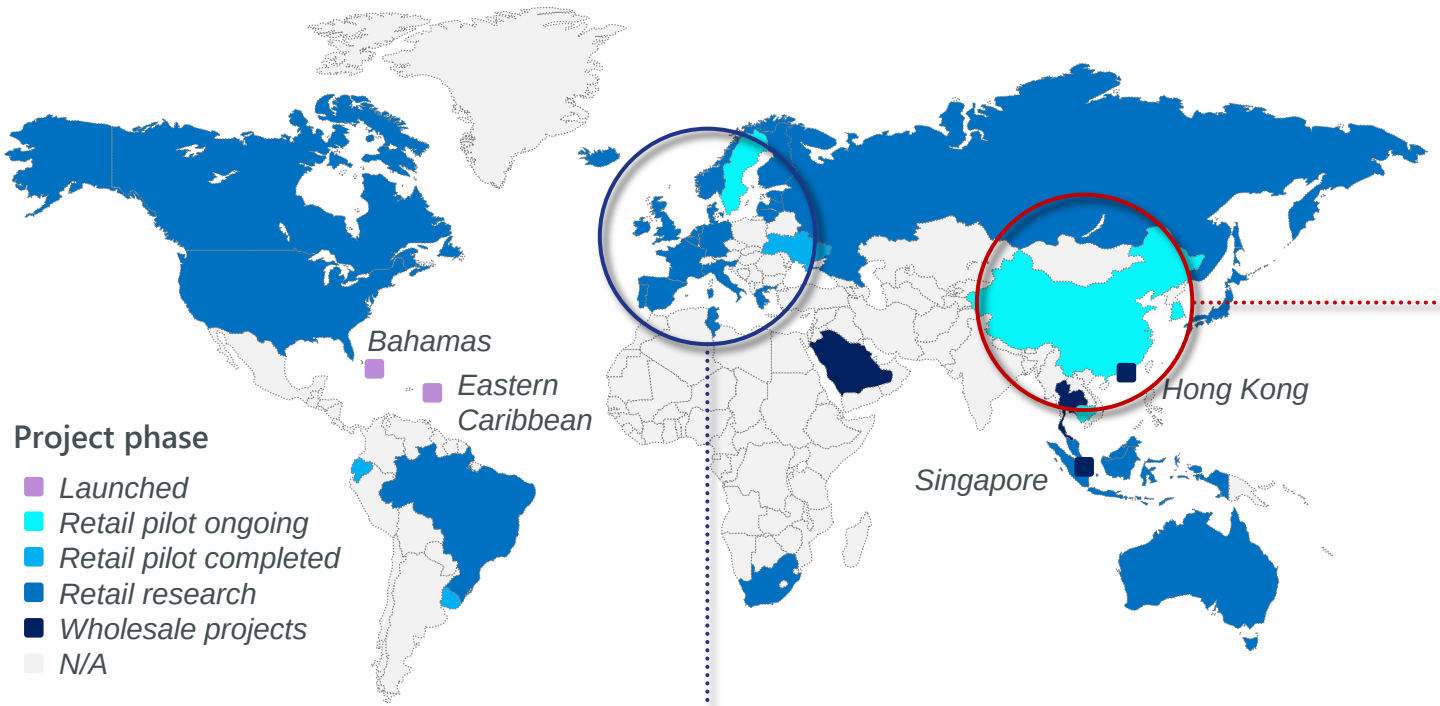
CBDCs may push stablecoins out of the market, since they provide a new low-volatility digital payment solution that is already embedded in the existing financial system.

On the other hand, CBDCs are by definition highly centralised. This represents a drastic departure from the original vision for cryptocurrency, and is a development that will undoubtedly face backlash from users.

"Pay"

Central Bank Digital Currencies

Currently, 86% of Central Banks worldwide are working on their own digital currencies.



Case | Digital Euro

+ In July 2021 the European Central Bank announced the launch of a CBDC project
+ The goal is to provide a marketable product after a two year exploration phase, with a decision on issuing a Digital Euro expected approx. in 2023 (launch would be expected in 2025-2026)
+ No decision yet regarding IT architecture, esp. the use of blockchain technology

Case | Digital Yuan

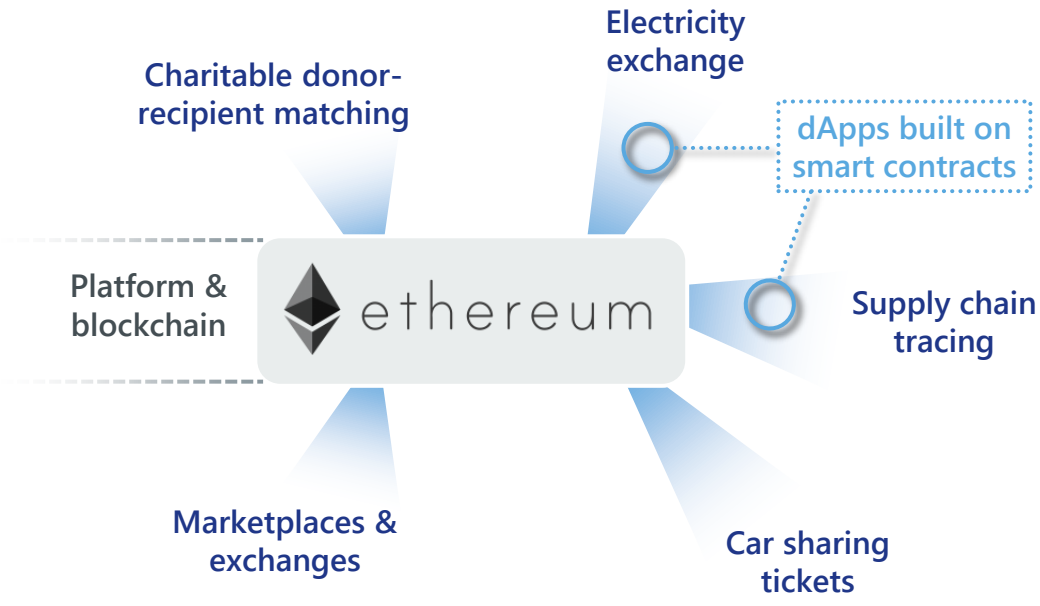
+ Research by the People's Bank of China (PBoC) began in 2014 followed by several large trials
+ The digital Yuan is one of the most advanced CBDC projects and likely to launch before the Winter Olympics in 2022
+ Hybrid Architecture with distribution through the financial sector (banks and other institutions)
+ Based on both traditional systems and blockchain (token) technology for enabling offline payments (further details have not been disclosed by the PBoC)

"Use"

From digital currencies to services

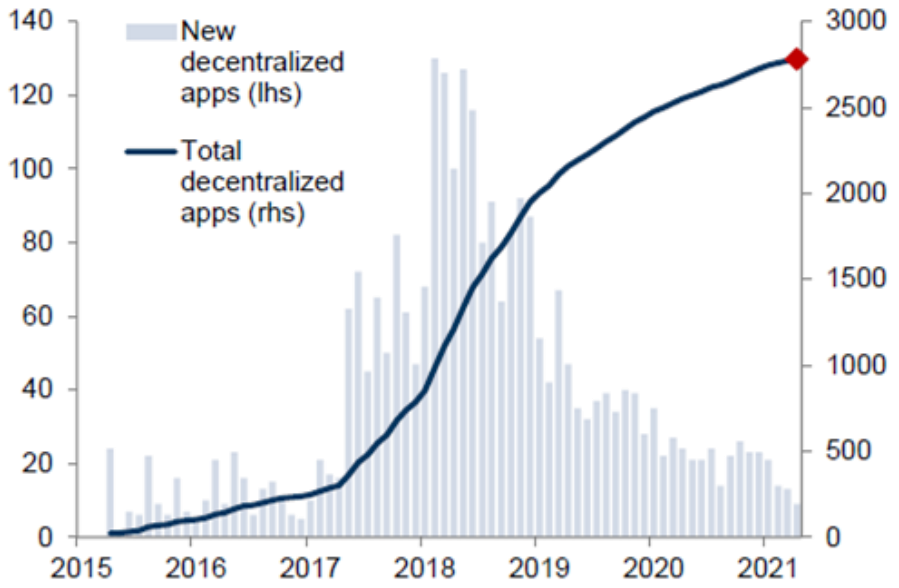
Ethereum was launched in 2015. The inventor, a Russian-Canadian programmer called Vitalik Buterin, saw the need for a cryptocurrency that had other applications besides payments. Instead, the blockchain concept is used to exchange goods and services between users.

Ethereum has its own cryptocurrency (Ether), but it's also an open platform for various decentralised applications (dApps) that enable access to real goods and services through so-called "smart contracts". Anyone can create these token applications on top of the Ethereum blockchain.



More than 2.5k dApps built on Ethereum

Monthly new and cumulative count of decentralised apps



Source: stateofthedapps.com, Goldman Sachs GIR

"Use"

Smart contracts

Signing contracts online

The Ethereum smart contract platform can facilitate a quick and secure transfer of access to assets – such as real estate, cars or electricity. Smart contracts are small computer programs that automate agreements between parties by having the contract conditions written into their code. The contract is automatically executed and enforced (e.g., payments released) once and only if all conditions have been met.

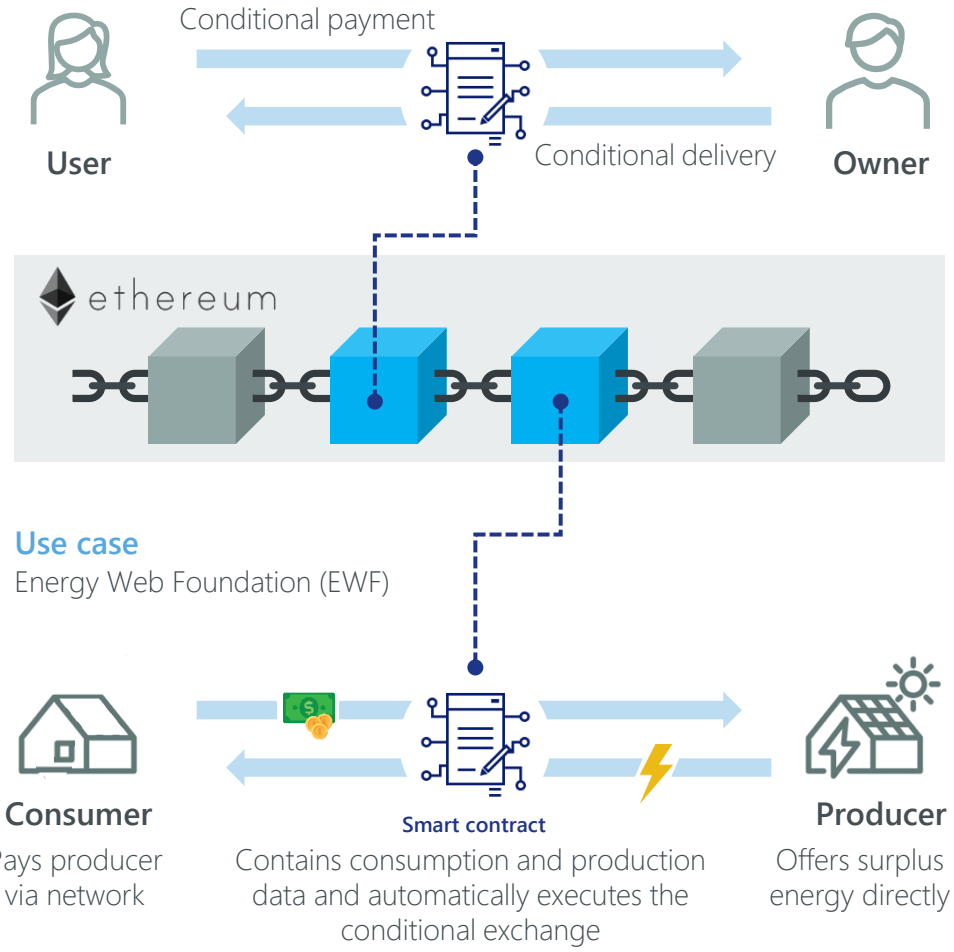
Smart contracts are stored on a blockchain – similar to cryptocurrency transactions – making it impossible for either party to violate a contract. This provides a new level of security for business relationships in a decentralised economy as conceptually, there is no need for lawyers or judicial systems to enforce contracts and resolve disputes.

Key Advantages:

- Saves time, money and reduces the margin of error.
- Ethereum provides a known framework with a core developer team
- The Canadian Energy Web Foundation (EWF) already utilises smart contracts to connect electricity suppliers (e.g. households with solar installations) to consumers in a peer-to-peer trading network. The efficiency of decentralised energy grids promises to accelerate a low-carbon, consumer-centric electricity system.

How smart contracts work

Illustrative concept on the Ethereum platform



"Own"

Security and Non-fungible tokens

Security tokens – the future of investing?

A key area where blockchain has the potential to disrupt is financial markets. A security token is issued on a blockchain and represents a stake in an external asset – like a business.

Security tokens are managed by smart contracts, and allow for many traditionally time consuming and fallible processes to be automated. The blockchain provides a source of truth that all parties can depend on.

Non-fungible tokens – the future of owning?

Unique assets such as artwork or exclusive collectibles could become easily investible through securitisation as "non-fungible tokens".

Unlike fungible assets (e.g., a $5 note), non-fungible tokens are not interchangeable – they represent ownership of unique or rare items and allow for people to own shares of a market that is traditionally hard to access.

"The most famous artist you've never heard of:"

In March 2021 an artist known as "Beeple" sold an NFT of his digital artwork for $69 million at Christie's, making him "among the top three most valuable living artists," according to the auction house.

Advantages

- Simplifies trading of company shares
- Transfer of ownership can take place without a stockbroker or notary public
- Small companies can raise capital without being listed on the stock exchange
- Private investors get an easy option to participate in "start-ups" and to sell these participations at any time

Potential use cases

- Securitising unique digital artwork
- Collectibles such as "NBA Top Shots":
  A blockchain-based platform that allows fans to buy, sell and trade officially-licensed video highlights.
- In the future we might see the tokenised ownership of physical items, such as fashion items or cars

The Digital Asset Market

Blockchain's place in the financial system

Are crypto assets an entirely new asset class, and does this present an investment opportunity?

Did you know ...?

learn more

Did you know...?

$100 invested in Bitcoin in 2011 are now worth[1]

$6.1 mn

Price volatility of Bitcoin is

4.7x

of Global Equity markets[2]

Of all Ethereum transactions

90%

go into decentralised Finance (DeFi) applications[3]

1) Own calculations, Bloomberg L.P.
2) Based on weekly returns (Bloomberg L.P., Deutsche Bank AG, as of April 2021)
3) BeInCrypto (2020)

Between hype and paradigm shift

After over a decade of investment bubbles, fear-of-missing-out, bull-runs and crashes, we are starting to see the increasing adoption and institutionalisation of digital assets.

A history of enthusiasm and fear

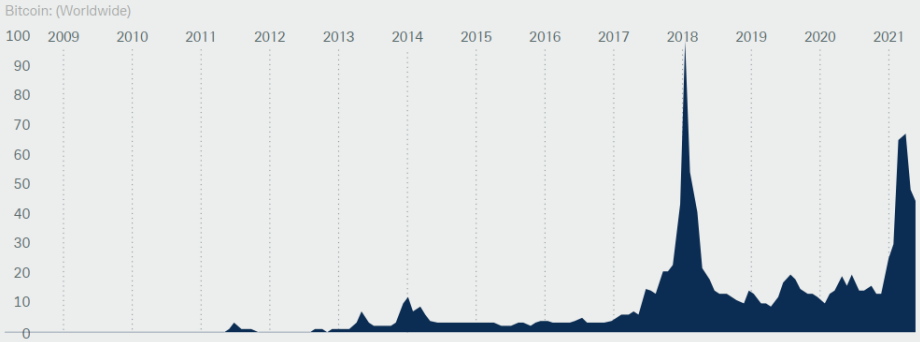
- Emergence of digital assets with the publication of the Bitcoin whitepaper at the end of 2008
- Early market players mostly technology enthusiasts and Fintechs
- Extreme phases of hype cycles and crashes, e.g. the ICO bubble of 2017
- Bitcoin gains a reputation for illegitimate transactions on the dark web while seeing more and more adoption for legitimate use cases

Where we stand & where we are headed

- Bitcoin still dominates the digital asset niche market although large-scale adoption is continuously increasing
- Growing number of established institutional investors in the market
- Economists expect the "token economy" of blockchain to boost global GDP by 1.76trn USD, or +1.4% until the year 2030[1]
- Boston Consulting Group believes digital assets "could become the biggest financial asset by the end of the decade"

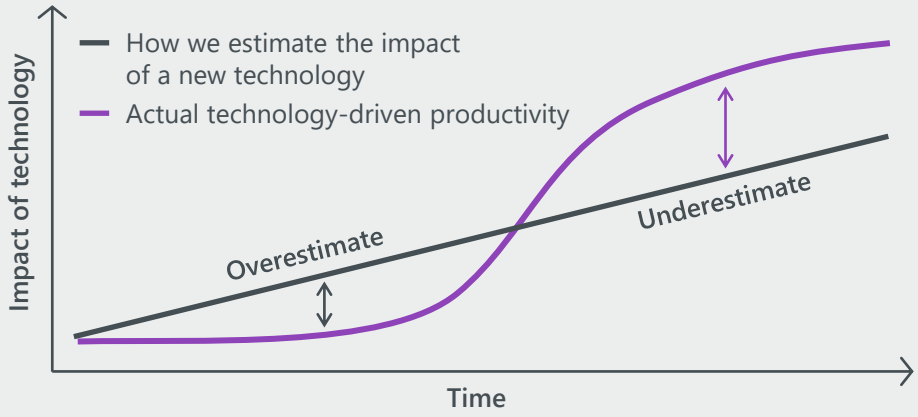
Public interest in Bitcoin over time

Google searches of bitcoin-related topics relative to peak in 2018



Source: Google Trends data, Deutsche Bank, data as of April 2021

Amara's law



1) PricewaterhouseCoopers (2020)

Measuring up the digital asset market

Since 2018, the value of one Bitcoin has increased 17 fold. In part because of the media attention and hype around cryptocurrencies and blockchain, this technology has become a major topic in financial markets and the public.

However, this picture should not distract from the reality that Bitcoin and other cryptocurrencies currently make up only a tiny fraction of global markets.

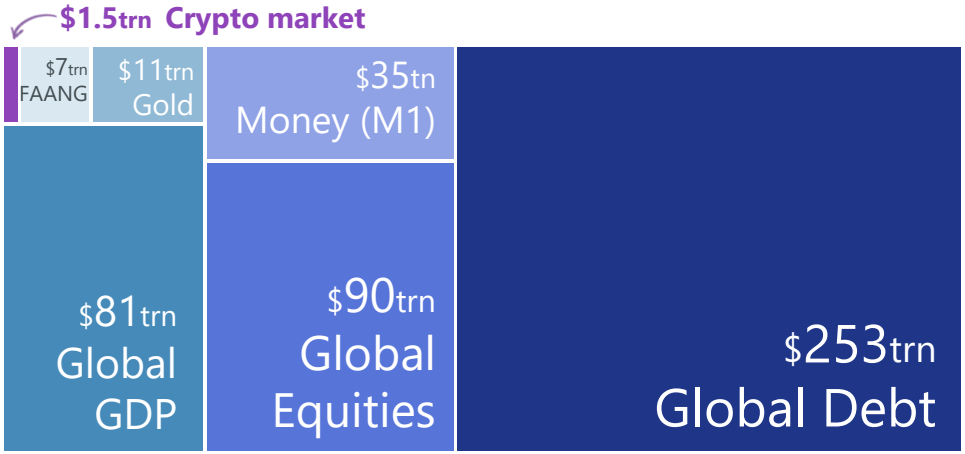
The key questions for investors, regulators and users remain:

"Are crypto assets a separate new asset class?"

"Can they reasonably be considered for diversified portfolios?"

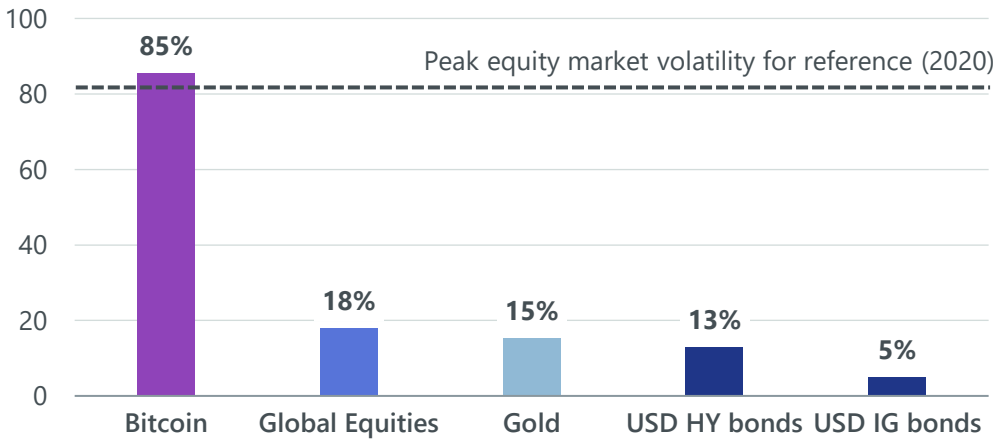
Putting the market in perspective

Market capitalisation of major global asset classes



Bitcoin is signifcantly more volatile than other traditional assets

Based on rolling weekly returns, % calculated over the last 5 years



Source: Bloomberg L.P., Deutsche Bank, data as of April 2021

Is Bitcoin an asset class or a currency?

Assigning cryptocurrencies to an existing or new asset class requires a look under the hood to examine their features. Intuitively, one might view these "coins" and "payment tokens" simply as currencies. Yet they struggle to meet the economic criteria of what constitutes money (a medium of exchange, unit of account and store of value). Meanwhile, evidence on the diversification potential vs. other asset classes is mixed.

Functional characteristics

1 Medium of exchange

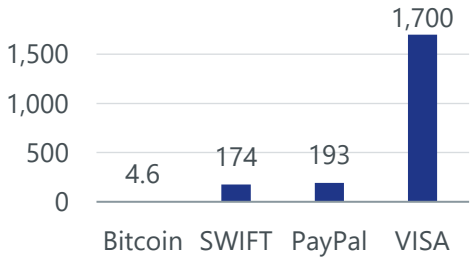
2 Unit of account

3 Store of value

4 Safe haven/anti-cyclical

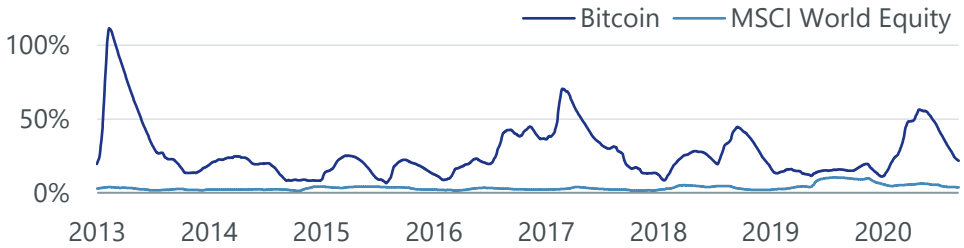
Assessment

Transactions per second (approx.)



Bitcoin is already used to make exchanges between users; however, its widespread adoption has caused severe delays in transaction processing. Solutions have been developed within the Bitcoin protocol and in the form of Altcoins, but scalability remains a critical challenge.

Rolling 6-month volatility in % of mean price



Because Bitcoin so far is rather disconnected from the real economy, there is no market consensus (equilibrium) of what certain goods and services should cost in cryptocurrency terms. This lack of reference creates price volatility, rendering their practical application difficult (imagine shops having to adjust their price tags every few minutes!)

Volatility is also a key obstacle for using cryptocurrencies as savings – there is no guarantee of what your wealth will be worth in the future. On the other hand, Bitcoin has been used by many as a buy-and-hold investment, and so far has kept appreciating in value over long time spans. Cryptocurrencies are used by many to evade capital restrictions and dispossession.

	BTC	ETH	Brent	Gold	DAX	MSCI	AMZN	GOOG
BTC	1.00							
ETH	0.59	1.00						
Brent	0.21	0.08	1.00					
Gold	0.01	0.03	-0.29	1.00				
DAX	0.25	0.26	0.62	-0.16	1.00			
MSCI	0.25	0.25	0.63	-0.15	0.99	1.00		
AMZN	0.03	0.11	0.06	0.11	0.34	0.37	1.00	
GOOG	0.16	0.18	0.28	-0.05	0.46	0.48	0.45	1.00

The disconnect between digital assets and the real economy may prove useful. Many point to low correlations with traditional asset classes, suggesting that crypto investments may be used to diversify investment portfolios. Cryptocurrencies have been used as a gold-like safe haven in times of market crises.

Investing in digital assets

Investors in cryptocurrencies have enjoyed massive returns. However, all major tokens have experienced extended period of large-scale losses, making blockchain-related investments challenging.

On a fundamental level, investors can enter the market by directly buying and holding Bitcoin, Ethereum or any other combination of altcoins and tokens.

More recently, derivatives and passive investment vehicles have started to emerge in line with increasing institutional interest and adoption.

There are also a strategies of actively managed investments in the crypto space, which require a comprehensive review and analysis of their own.[1]

Further, investors can make use of staking as a strategy that effectively earns interest in crypto currency and can be a lucrative complementary investment strategy.

Comparing staking returns to traditional interest deposits

0.40 % p.a.
Bank deposit rate (United Kingdom)

13.29 % p.a.
Staking reward (delegated) (Polkadot)

Performance since 2013: Bitcoin and Ethereum

in USD

Historical drawdown: Bitcoin and Ethereum

Relative price difference to last peak

1) Castell's experienced PM team has screened the available universe and has selected a few sustainable strategies as appropriate for investments in long-term portfolios

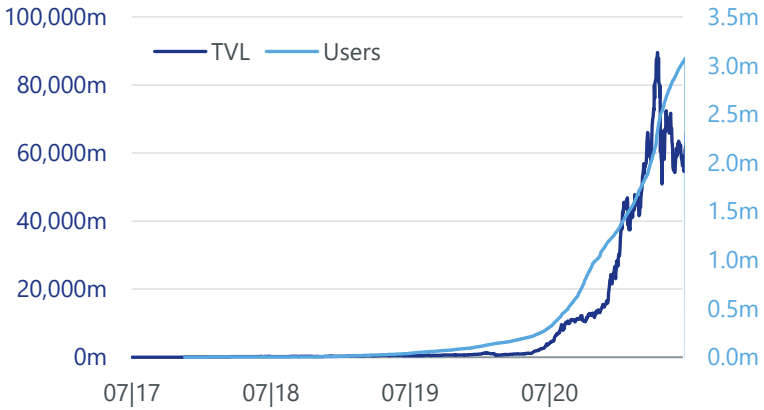
The market for Decentralised Finance

Recent years brought the emergence of blockchain-based instruments in what is known as "decentralised finance" (DeFi). Removing intermediaries from financial transactions allows not just the transfer of money, but also lending activities or entirely new financial activities, such as liquidity mining and yield farming.

Nearly all DeFi applications are built on the Ethereum blockchain using smart contracts without any centralised company or governance body. Instead of the decentralisation of money, DeFi aims for the broader decentralisation of the traditional financial industry and giving access to the population of 1.7bn "unbanked" people. DeFi is also emerging as a tool for smaller businesses in developing markets, especially for remittances and small loans.

Development of the DeFi market

Left scale "total value locked (TLV)" in USD, right scale "user"



Digital replications of existing financial activities

Exchanges & barter trading

UNISWAP SushiSwap PancakeSwap

Borrowing & lending

AAVE Compound MAKER

Derivatives & options

SYNTHETIX augur

Asset management

Set Protocol

Non-fungible tokens

Digital art, in-game items, virtual land sales etc.

Novel financial activities

Atomic swaps

Simultaneous execution of transaction parts (delivery versus payment)

Flash loans

Extremely short-termed loans used for arbitrage and portfolio reallocations

Staking

Participating in proof-of-stake validation processes and earning interest-like rewards in the form of newly created coins

Yield farming / liquidity mining

Active optimisation of investment returns through constantly shifting assets and earning rewards from e.g. providing liquidity in exchange pools or lending out cryptocurrency to other users

Environmental & Social Impact

Thinking "outside the blocks"

Did you know ...?

learn more

What are the environmental and social implications of blockchain technology?

Did you know...?

The entire bitcoin network could be powered for

1.9 years

with the annual electricity consumption of always-on but inactive home devices in the US alone[1]

Of all invested assets in the US today

33%

are managed in accordance with environmental, social and governance (ESG) considerations[2]

Of all cryptocurrency transactions

0.34%

are estimated to be connected to illicit activities[3]

1) CBECI (2021)
2) Nason (2020)
3) Chainalysis (2021)

The environmental costs of decentralisation

Bitcoin currently consumes huge amounts of energy and has a significant carbon footprint. At a time when increasing emphasis is being placed on mitigating climate change, the sustainability profile of blockchain technology is a major concern.

The high energy consumption is a "flaw" that was intentionally designed into the Bitcoin system, since Proof-of-Work consensus mechanisms rely on the block mining process to be computationally difficult and resource-intensive. However, several solutions have been put forward already to mitigate these issues.

Identified issues

Electricity consumption (TWh/year)

Footprint of a single Bitcoin transaction[1]

Carbon emissions

811 kg CO_2

equivalent to 1.8 million VISA transactions

Electricity

1,708 kWh

equivalent to 59 days of power consumption in an average US household

Electronic waste

83.1 g

equivalent to 1.3 batteries

Approaches / solutions

1 Energy mix

Volcanoes and natural springs in Iceland have provided a cheap source of natural energy. 8% of all Bitcoins have been mined there using this renewable energy[1] – yet the vast majority of Bitcoin mining takes place in China, the US and Russia, countries that are still heavily reliant on fossil fuels.

2 Consensus protocol

In recent years, the Ethereum project has made steps to move to a Proof-of-Stake consensus mechanism that would replace compu-tational effort with a staking system, reducing energy consumption.

3 Using the work of Proof-of-Work

Other ideas include sticking to Proof-of-Work schemes but utilising the invested computational power to solve complex scientific problems, e.g. in medicine or physics research. One small pilot is currently run in the US as "fold@home".

1) Digiconomist (2021)

Social implications of blockchain technology

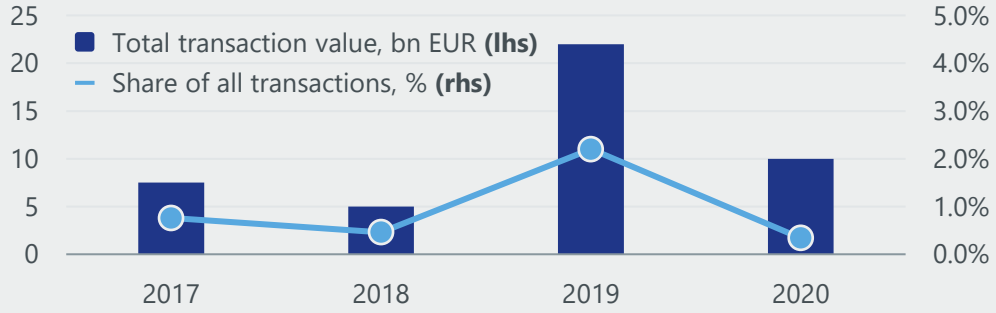
Blockchain technology addresses concepts at the very core of our social and economic life – the formation of trust and authority. Similar to the environmental debate, there are societal implications that would arise from wide-spread adoption of cryptocurrencies and tokens.

Risks & threats

- Many blockchain projects in practice are developed and operated by centralised organisations with commercial motives, counteracting the original ideas of blockchain
- CBDCs entail risks for data privacy and potential threats regarding surveillance of consumer spending
- The pseudonymous nature of some cryptocurrencies could make identifying things like political donations and fraud more difficult
- Cryptocurrencies play a central role to various criminal activities. Bitcoin remains the primary payment currency in the dark web

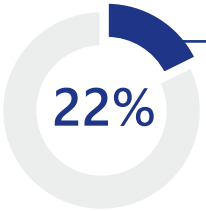
Illegal activities connected to cryptocurrencies

Value and share of transactions linked to illicit uses



Benefits & opportunities

- Decentralised governance eliminates risks of centralisation, such as corruption and technical or administrative failure
- Security: Money laundering or identity fraud become more difficult in a public system where transactions can be systematically tracked to its origins
- Ability to make supply chains more transparent in the future, for instance through better records of where supplies are sourced from, kept and ultimately used
- Decentralisation of economic power comparable to the invention of open source knowledge databases (Wikipedia)
- Inclusion: Possibility for the "unbanked" to access financial services using only a mobile phone and the internet



1.7bn people "unbanked"
without access to the banking system)

1) Chainalysis (2021)

Closing thoughts

”

Blockchain is about decentralisation and democratising power.

It will change the way we do business in the 21st century.

We are in an exciting era of knowledge democratisation. 30 years ago, who would have predicted that a decentralised encyclopaedia written by readers themselves would beat Brockhaus in terms of accuracy and quality? In the age of the internet, knowledge is in the hands of anyone with access to Wikipedia.

As the old adage goes: “knowledge is power.” Whilst the internet had democratised knowledge, blockchain is democratising power. As we have seen, blockchain offers the opportunity to completely remove the middleman for the first time, allowing all sorts of financial processes to be transparently and securely managed on a peer-to-peer network. This technology offers more people access to financial services and creates a new ecosystem of digital assets. This is the real potential of blockchain.

It’s still early days for this emerging market. Coins and tokens are highly volatile, and the competition between the official central bank digital currencies and private decentralised systems has only just begun.

From accelerating the transition to renewable energy to creating a market for carbon offsetting, the stage is set for this technology to unleash great innovation and ingenuity over the next decades. Perhaps, at the same time, creating more equal and open markets and societies, and transforming the fundamental structures of our economic life.

— Christian Hille

Appendix

Authors, references & technical glossary

Authors

Christian Hille
CIO Fürstlich Castell'sche Bank,
Head of Portfolio Management

Nils Mallock
Portfolio Management

Lukas Kreß
Product Management

Acknowledgments

We would like to thank everyone involved, internally and externally, for bringing this comprehensive publication together. Special acknowledgement goes to **Katharina Gehra** and **Walther Doernte** for their valuable insights and very constructive, critical discussions around blockchain and its applications, as well as journalist **Tarn Rodgers Johns** for her professional writing services.

References

Auer, R., Cornell, G., Frost, J. (2021). Rise of Central Bank Digital currencies: Dirvers, approaches and technologies. BIS working paper, No. 880.

BeInCrypto (2020). DeFi Accounts for Almost 90% of Ethereum Transactions.

Blockchaincenter.net (2021). Various Articles.

Cambridge Bitcoin Electricity Consumption Index CBECI (2021). Comparisons.

Chainalysis (2021). Crypto Crime Summarized: Scams and Darknet Markets Dominated 2020 by Revenue, But Ransomware Is the Bigger Story.

Chainalysis (2021). Cryptocurrency Ecosystem Comparison: Bitcoin vs. Ethereum vs. Stablecoins.

CoinMarketCap (2021). Various data.

DappRadar (2021). Various Reports and Articles.

Digiconomist (2021). Bitcoin Energy Consumption Index.

Defi Pulse (2021). Total Value Locked (USD).

Ethereum Foundation (2021). Stablecoins.

Ethereum Foundation (2021). Dezentrale Anwendungen (DAPPS).

Ethereum Foundation (2021). Decentralized finance (DeFi).

Ethereum Foundation (2021). Non-fungible tokens (NFT).

Gallup (2016). Americans' Confidence in Banks Still Languishing Below 30%.

Goldman Sachs (2021). Crypto: A New Asset Class?

Gulley, A. (2021). Understanding Ethereum.

Harris, M. (2017). A Few Bitcoin Statistics and Similarities to Equities.

Hinchliffe, R. (2021). Coinbase IPO values hits $99.6bn valuation with shares up 52% on debut.

Howcroft, E. (2021). NFT sales volume surges to $2.5 bln in 2021 first half.

IOT Analytics (2020). State of the IoT 2020.

Mitic, I. (2021). 45 Blockchain Statistics & Facts That Will Make You Think: The Dawn of Hypercapitalism.

Morgan Stanley (2021). Update: Bitcoin, Crypto and Digital Currencies.

Nason, D. (2020). 'Sustainable investing' is surging, accounting for 33% of total U.S. assets under management.

PricewaterhouseCoopers (2020). Time for trust.

Reimers, A. (2021). Das Credo heisst online Bilanz der internationalen Auktionshäuser.

Reinhardt, A. (2021). Ratgeber: So viel Speicherplatz sollte Ihr Smartphone haben.

Sandner, P. (2019). Decentralized Finance (DeFi): What Do You Need To Know?

Schär, F. (2021). Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets.

Statista (2021). Size of the Bitcoin blockchain from January 2009 to July 12, 2021.

The Block (2021). Various data.

Further technical information

Crypto wallet

A software that enables you to send and receive cryptocurrencies, such as Bitcoin and Ether. Wallets can be web-based, similar to an online banking account (**"hot wallet"**) or offline in the form of encrypted USB memory sticks or even written down on paper (**"cold wallet"**). Setting up a wallet is a prerequisite to send and receive cryptocurrencies.

Wallets contain **user addresses** which uniquely identifies them in the network. In public blockchains like Bitcoin, network participants can look up each and every past transaction an address has been involved in: see for yourself!

Private & public key

To use cryptocurrencies in their wallets, users generate a random pair of keys that are essential elements of blockchain security. The **public key** is the basis for the openly known user address that is used as the sender or receiver ID in the network. The **private key** can be understood as a secret passcode that is used to authorise transactions made with the public key (address).

The two keys are mathematically linked in a way that allows for the user to generate a **digital signature** with them. Signatures are included with every transaction to prove that the sender knows the private key belonging to the public key (address) – in other words, that they are the rightful owner of the coins to be spent. Importantly, deriving the private key from the public key is impossible. It is critical that users do not lose or disclose their private keys – otherwise, the coins and tokens linked to their address will be lost forever. In practice, key pairs are usually stored within a user's wallet and secured by encryption.

Proof-of-Work mining & block generation

In order to be rewarded with newly created cryptocurrency and transaction fees, active network users compete in a **race to add new blocks of transaction data to the blockchain** in a process called "mining". Under a Proof-of-Work regime, **miners continuously generate large random numbers** until they find a value in a target range. This range is automatically adjusted to keep the PoW puzzle difficult and account for changes in the number of miners and computational resources invested.

Disclaimer

This document is marketing information of Fürstlich Castell'schen Bank and does not constitute an offer, recommendation or solicitation to buy or sell any financial instrument, but is provided for information purposes only. The products and services listed herein are not suitable for every investor. By providing this information, Fürstlich Castell'sche Bank does not assume any advisory or fiduciary duties towards any investor. This document is neither a substitute for individual investment advice nor for individual, qualified tax advice and does not claim to contain a complete presentation of risks and product features. We strongly recommend that you consult your personal advisor before entering into any transaction. Any offer or transaction based on information contained in this document is made on the basis of a separate and independent agreement.

The indicative investment opportunities and portfolio structures presented in this document, as well as model calculations contained therein, are only intended to inform you about the general possibilities of an investment and do not claim to be fully suitable. The data contained in this document has been obtained from sources we believe to be reliable. The Bank accepts no liability for the timeliness, accuracy or completeness of this data. All presentations, opinions and assessments, including forward-looking forecasts, are based on data and assessments made by the Bank at the time this document was prepared, which may change at any time without prior notice, also in view of the current legal and tax situation. The investment opportunities and portfolio structures presented in this information may become irrelevant at short notice due to market developments and are therefore only of a momentary nature. The Bank is not obliged to notify any future changes. The bank is under no obligation to update or adjust this document. Past performance is not a reliable indicator of future performance.

This document may not be reproduced or distributed without the express consent of Fürstlich Castell'sche Bank. Fürstlich Castell'sche Bank accepts no liability for any damage or loss arising directly or indirectly from the distribution or use of this document or its contents.