METACO

DIGITAL ASSET GLOSSARY

# The A-Z of Digital Assets

www.metaco.com | info@metaco.com

# Content

# A is for **APPLICATION-SPECIFIC INTEGRATED CIRCUIT (ASIC)**

Most devices we use, such as PCs, tablets, and smartphones are built to run multiple applications. We use them for everything from a work Zoom call to playing games (possibly at the same time!).

To perform these different functions and computations, these devices are fitted with multi-purpose integrated circuits called CPUs (central processing units) which can handle the instructions from different programs. These CPUs are built for a variety of functions, but not for efficiency.

In contrast, an Application Specific Integrated Circuit (ASIC) is designed to perform a single function very fast. ASICs are used across various areas of computing, such as machine learning and IoT devices. Since 2013, they have also been used for bitcoin mining. Bitcoin mining was first done with basic CPUs, then high-end GPUs (Graphic Processing Units), then field-programmable gate arrays (FPGAs), and finally with ASICs.

## WHY ARE ASICS SUITABLE FOR BITCOIN MINING?

For a new block of transactions to be written to the blockchain (the public database), computers (bitcoin miners) work on finding a proof-of-work code for this block by performing a complex calculation known as a hash.

The miner that gets the proof-of-work code is rewarded with bitcoin, which is how new bitcoins enter into circulation. That's why bitcoin mining is a competitive process: the more hashes you perform, the higher the chances of you getting bitcoin, which incentivizes people to invest in machines and chips that can perform these calculations faster.

In addition, the difficulty of these calculations is constantly increasing so mining power is added to the network to keep up, which also creates an incentive to invest in faster throughput.
This is why bitcoin mining is now done by ASICs and why these ASICs get faster all of the time.
For more detail on mining, see M is Mining.

## SOME FACTS

The Avalon chip, produced by Canaan Creative, was the first application-specific integrated circuit (ASIC) designed for bitcoin mining and it entered the market in 2013.

Like all chips, the R&D expenditure is extremely high which means the chips must be produced at high scale for the chip maker to be profitable. This results in a highly concentrated industry.
Today, the three largest producers of ASICs for bitcoin mining, Microbt, Cannan, and Bitmain - all Chinese - collectively have over 90% market share.

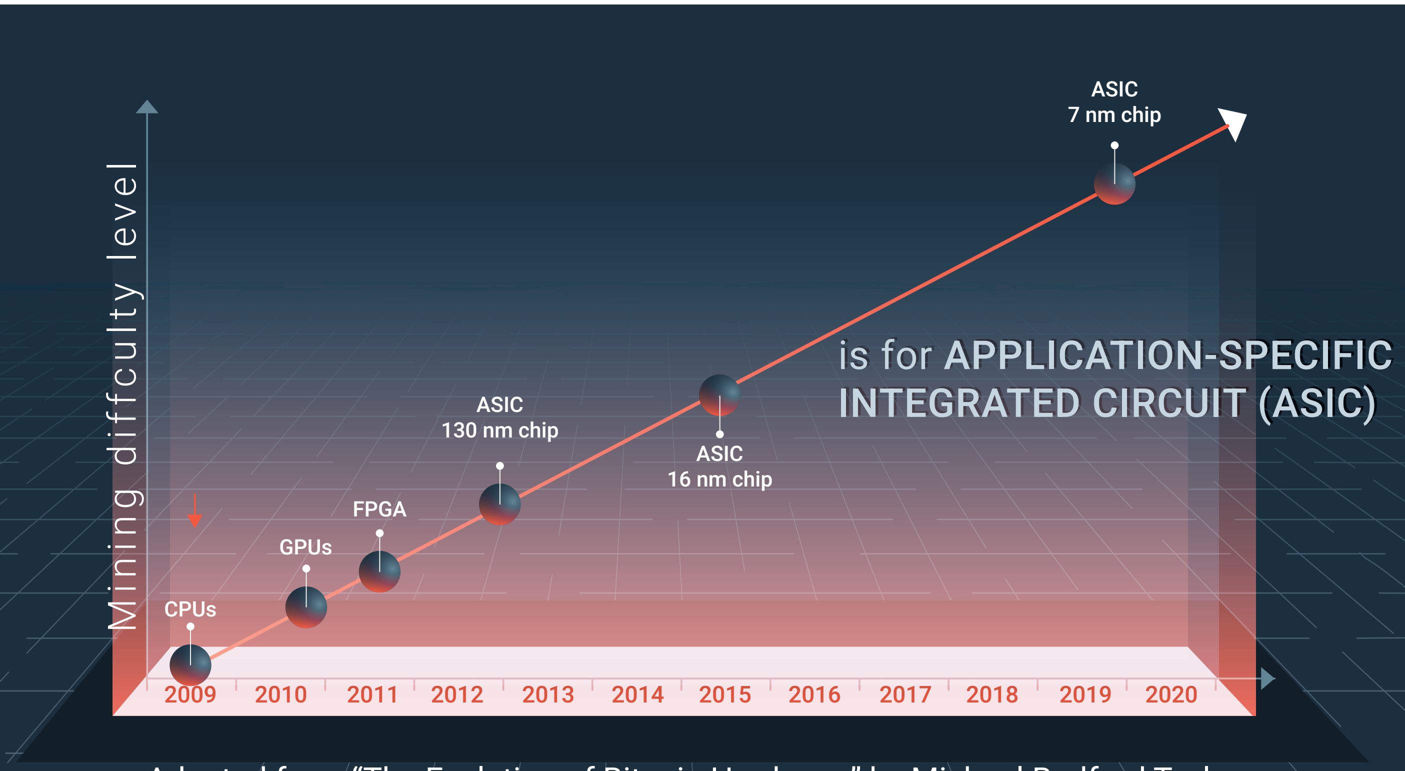
Most bitcoin miners are formed into pools to spread the risk/reward: to split the cost of the equipment and to increase the chances of getting bitcoin. While some of the pools are located in places like Iceland, where electricity is cheap, the majority of these pools are in China.

## WHAT TO KNOW MORE?

For a deeper dive into how hardware for cryptocurrency mining has evolved, as well as the economic impact and much more, we recommend this excellent report from ARK Invest.

## THE METACO VIEW

> *“Bitcoin mining is a competitive process that incentivizes the industry to invest in producing ever more efficient ASICs. Inevitably, this weaponization of the mining industry leads to concentration in large specialized firms and pools, which some people argue increases the risk of 51% or other attacks.*
>
> *However, we see this as just another sign of the professionalization of the crypto ecosystem. The more specialized firms invest in ASICs and other technology, the more skin in the game they have and the less likely are to want to disrupt it.”*



Adapted from “The Evolution of Bitcoin Hardware” by Michael Bedford Taylor

# B is for BITCOIN

Bitcoin is the first cryptocurrency to ever hit the market. It's also the best-known, most widely traded cryptocurrency, and the one with the highest market cap.

Bitcoin first came to prominence in October 2008, when Satoshi Nakamoto published a white paper in which he explained how the trust underpinning our financial system could be replaced with mathematical proof. Shortly thereafter, in January 2009, the first Bitcoins entered circulation. Unlike fiat currencies, Bitcoin isn't issued by a central authority. It's mined. Mining is a process in which computers solve complex mathematical problems in exchange for Bitcoin. This is called proof of work.

In theory, anyone can mine Bitcoin. But the process is expensive and resource-heavy. It's estimated that mining consumes more electricity in one year than the entire Republic of Ireland, and five times more than is produced by the largest wind farm in Europe.

Proof of work is also difficult to produce (though easy to verify). So, someone's mining efforts may result in very few Bitcoins or none at all. This is intentional. The aim is to prevent a single individual or group from being in a position where they can exercise undue influence on the system or corner the market.

Bitcoin transactions are made using public and private keys. The **public key** is an address made up of random letters and numbers which you share with the person you want to transact with. The **private key** is like a password which authorises the transaction.

Transactions are recorded on the blockchain, which acts as a shared public ledger. Every transaction, or block in the chain, is time-stamped and has to be verified by the entire network.

Crucially, once a transaction is recorded, it can't be modified. Any modifications would invalidate all subsequent blocks.

## SOME FACTS

- One of the first purchases ever paid for in Bitcoin were two take-away pizzas. Developer Laszlo Hanyecz paid 10,000 Bitcoins for them. Today, those Bitcoins would be worth $100 million
- Bitcoin may be the first cryptocurrency, but it's not the first attempt at creating one. The credit for that belongs to David Chaum, whose staunch views on privacy led him to invent 'blinded cash' — a system that anonymised transactions using cryptographic protocols. Chaum's company DigiCash made waves when it was founded in 1989. Sadly, the internet was still in its infancy, so DigiCash didn't catch on. The company declared bankruptcy in 1998.
- It's been more than a decade since the Bitcoin white paper was published, but Satoshi Nakamoto's true identity remains a mystery.

Some of the people touted as being Bitcoin's elusive inventor include:

- Physicist Dorian Nakamoto
- Scientist Craig Wright
- Computer engineer Nick Szabo
- Interestingly, Szabo worked for DigiCash.

## WHAT TO KNOW MORE?

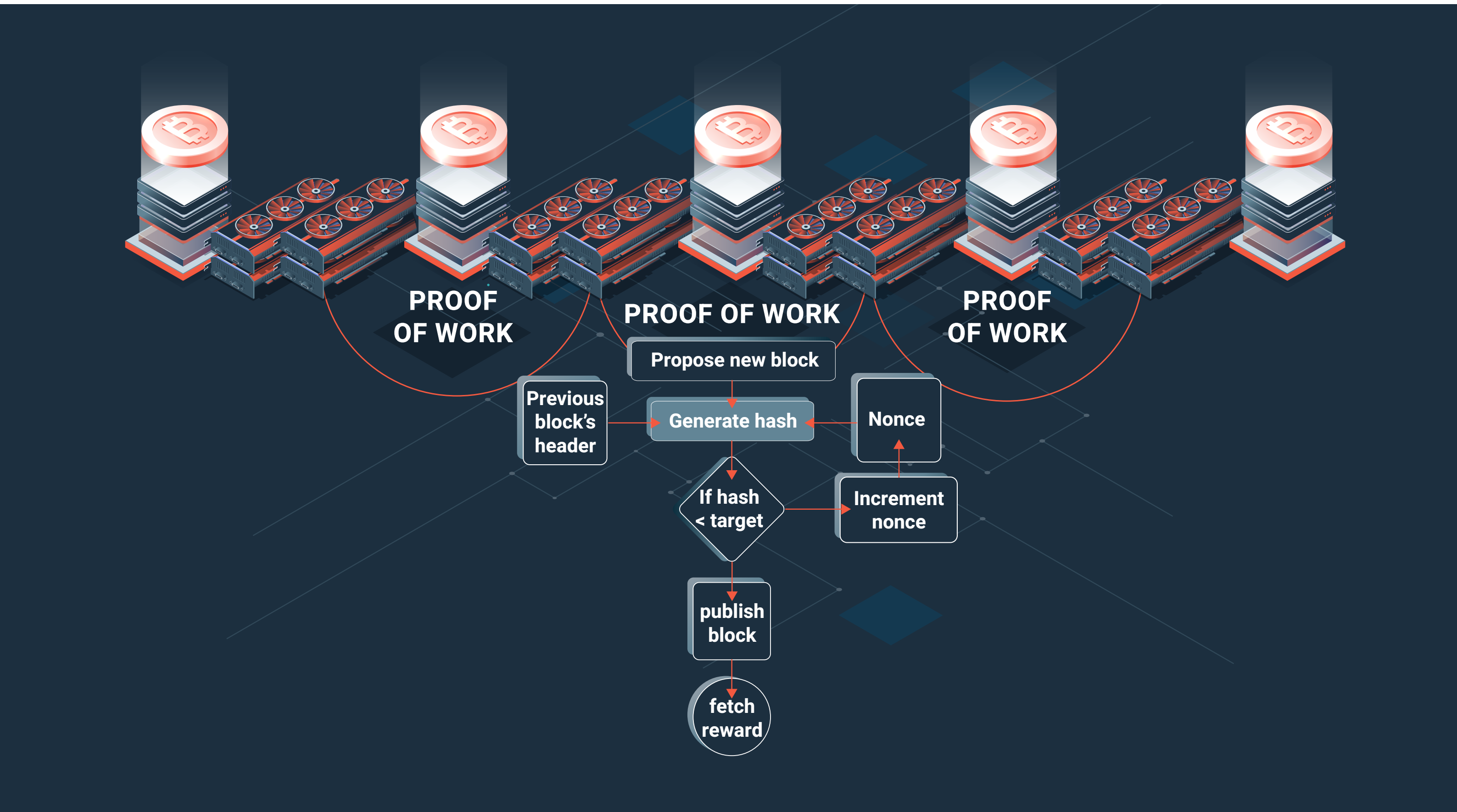
Nakamoto's white paper — Bitcoin: a peer-to-peer electronic cash system — explains in great detail the philosophy and mathematical formulas that underpin Bitcoin and the blockchain.

If you're looking for a less technical introduction, this course on Khan Academy is endorsed by bitcoin.org, Bitcoin's official site and the place where Nakamoto's white paper was originally published.

## THE METACO VIEW

> *"Bitcoin and the blockchain are the most transformative innovations of our time, because they can unlock financial sovereignty for everyone.*
>
> *As someone who's personally struggled to find financial backing for entrepreneurial projects, I feel very strongly about its potential. That's why, at Metaco, we work hard to further the vision of a financial system in which there are no gatekeepers."*
>
> **Nicolas Dorier**, Founder and VP of Digital Currencies.

## PROOF OF WORK IN BITCOIN MINING



# C is for **CENTRAL BANK DIGITAL CURRENCY**

Central Bank Digital Currencies — CBDCs for short — are digital fiat currencies, or digital cash. CBDCs are inspired by cryptocurrencies, in that they allow users to transact anonymously. This is because they use a system of encrypted signatures — known as 'blind signatures' — to keep the payer and payee's identities hidden.

That said, CBDCs differ from cryptocurrencies in two key ways. Firstly, where cryptocurrencies are decentralized, a CBDC is, by definition, centralised. It's established by law, backed by the state, and has official status as legal tender in the country or countries where it's issued.

Secondly, while some proposed CBDCs are blockchain-based, distributed ledger technology isn't necessary for them to work.

The blockchain's purpose is to provide a replacement for trust. Put simply, complex mathematical calculations fulfil the role that would usually belong to counterparties and other actors that ensure the integrity of a fiat currency transaction.

That's important in decentralized systems. But in the case of a CBDC, the central authority that controls and manages it provides that trust.

The concept of CBDCs has started gaining momentum because we're living in increasingly cashless societies. This has made it harder for the unbanked, those who are predominantly paid in cash, and other vulnerable sectors of the population to participate in economic life.

Going cashless has also had other unintended negative consequences. In particular:

- Digital payments have concentrated power in private actors' hands
- Credit risk and liquidity risk are increasing, because ever more transactions involve private deposits settled through other banks, rather than through the central bank
- Some central banks have seen drops in seigniorage revenue — the profit they make from the difference between cash's face value and the cost of manufacturing and recycling it

It's thought that CBDCs will address these problems and ensure everyone continues to have access to cash, even if physical notes and coins are eventually phased out.

## SOME FACTS

- Ecuador was the first country to roll out a CBDC. Sistema de Dinero Electrónico was launched in 2014 to support dollarisation (the country replaced the failing Sucre with the US Dollar in 2000). Ironically for a CBDC trailblazer, Bitcoin and other cryptocurrencies are illegal in Ecuador. This doesn't seem to be deterring Ecuadorians — Bitcoin's popularity keeps growing

- Ben Broadbent is credited with coining the term 'Central Bank Digital Currency' while serving as the Bank of England's deputy governor. He used the term in a March 2016 speech at the London School of Economics in which he also acknowledged that Bitcoin inspired the idea.

## WHAT TO KNOW MORE?

This 2019 paper from the Institute and Faculty of Actuaries explains the origin, rationale, and issues surrounding CBDCs in detail, but it's highly readable and easy to follow.

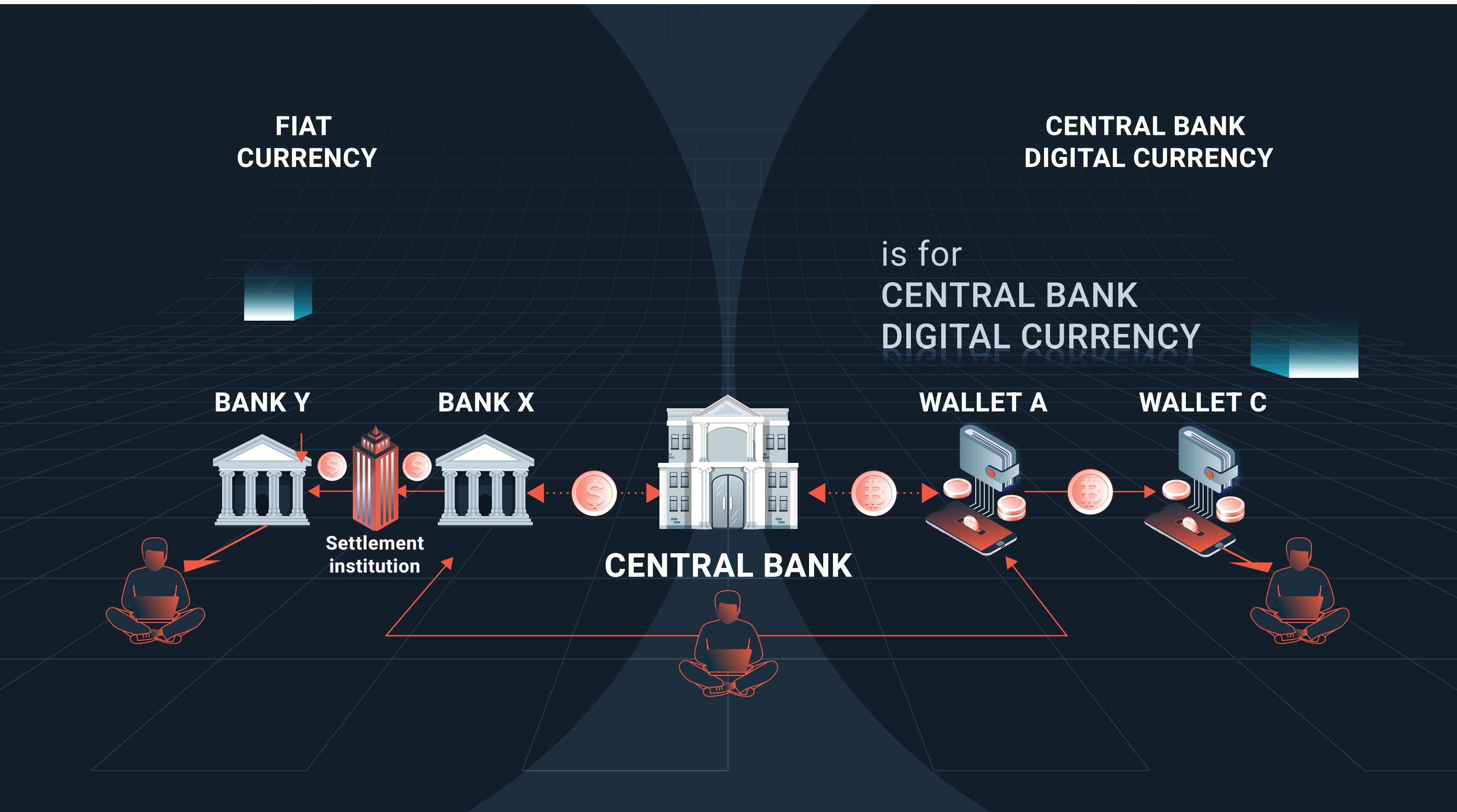
Of particular interest is page 20, a table summarising different countries' attitudes to cryptocurrencies. A number of countries classified as having a 'generally negative view' of cryptocurrencies and crypto assets — most notably Australia, Japan, and the UK — are now regulating them.

See also this great article in Forbes about how our partner Giesecke & Devrient is moving from printing physical banknotes to providing the infrastructure for CBDCs

## THE METACO VIEW

> *"As the enthusiasm for going cashless increases, it's crucial that we take steps to keep our financial system resilient... and make sure nobody is left behind.*
>
> *We believe CBDCs represent a natural progression in the evolution of money, one that allows for easier and cheaper transmission of payments and monetary policy, which benefits everyone."*
>
> **Adrien Treccani**, CEO METACO

## HOW CBDCS ARE DIFFERENT FROM FIAT CURRENCY



# D is for DECENTRALIZED

Decentralization is a fundamental feature of crypto assets. Cryptocurrencies, tokenized assets, and the networks they run on — blockchains — are decentralized by design.

There's no single body with ultimate decision-making authority to act as gatekeeper. Instead, the system runs by distributed consensus. Put simply, a transaction is approved when a mathematical calculation is completed successfully and it's accuracy is verified by the entire network.

The rationale for decentralization is that it makes the financial system more resilient, efficient, and democratic. By contrast, systems that rely on a central authority have a single point of failure. Should things go wrong at that point, the negative effects would inevitably spread to the whole system.

Over the years, the concept of decentralization has been extended beyond cryptocurrencies and crypto assets to other blockchain-based applications.

Here are four key terms worth getting familiar with:

- **Dapps, or decentralized applications**
  Unlike traditional apps, which typically run on a few dedicated servers, Dapps run on the excess power of thousands of servers. They're also fully autonomous. Their operation is governed by mathematical calculations, so they don't need to be overseen by humans
- **DeFi, or decentralized finance**
  This is a catch-all term for blockchain-based apps that cut intermediaries out of financial transactions, whether direct — that is, purchases of goods or services — or contract-based transactions like loans, mortgages, and insurance
- **DEX, or decentralized exchange**
  DEXs are a type of DeFi. They're exchanges that exist on the blockchain and aim to make trading more transparent. When you trade on a DEX, orders are completed using smart contracts — digital agreements written in code that are enforced automatically when predetermined rules are met. Crucially, unlike traditional exchanges, you don't give up custody of your funds until a trade is complete
- **DAO, or decentralized autonomous organization**
  This is an organization that uses the blockchain as a replacement for human management. For example, a shop could store its inventory on the blockchain and smart contracts could manage stock based on historical demand, including triggering purchase orders, specifying delivery dates, and settling supplier invoices.

## SOME FACTS

- Bitcoin is often regarded as the first fully-functional DAO. But it was the Ethereum blockchain that brought wider attention to DAOs by perfecting the environment in which smart contracts could be developed, tested, and deployed

- While the Ethereum blockchain was crucial in popularizing smart contracts, the concept dates back to the mid-90s. Computer scientist Nick Szabo first described smart contracts in 1996 and spent several years developing the idea, publishing a number of papers in the process
- Interestingly, Szabo has been mooted as the true identity of Bitcoin's inventor Satoshi Nakamoto. Szabo has categorically denied this.

## WANT TO KNOW MORE?

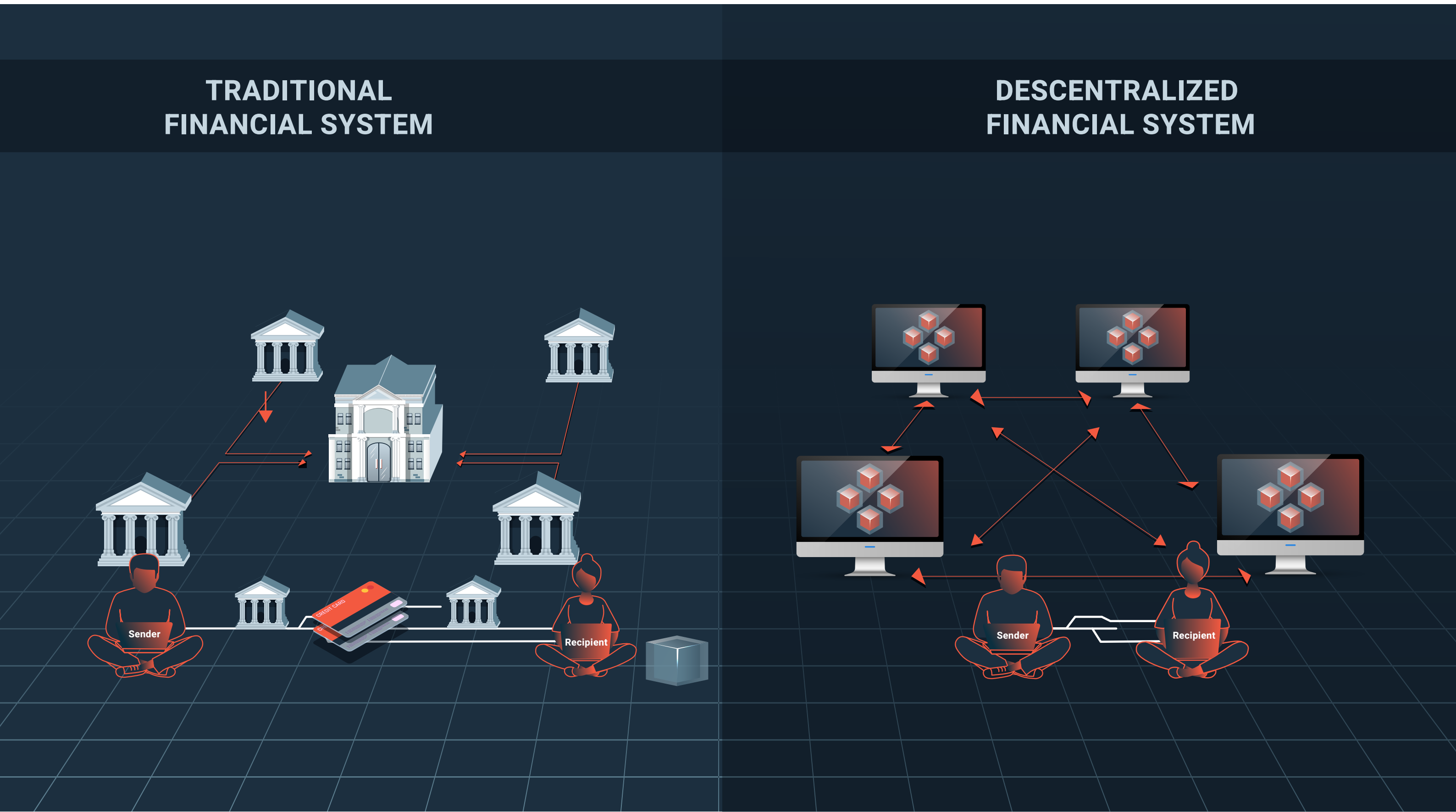
This article on CoinTelegraph is an excellent primer on DAOs and Dapps.

You can also learn more about decentralized exchanges on Binance Academy. What's particularly noteworthy about this article is that it acknowledges that, despite their many advantages, decentralized exchanges aren't always the cheapest or most practical option.

## THE METACO VIEW

> *"Decentralisation creates complete transparency, and that means a fairer, more inclusive financial system for all. But the concept has the potential to be revolutionary well beyond finance.*
>
> *DAOs, for example, can negate the need for any admin, freeing up businesses so they can focus on more important tasks…like maximizing customer success."*
>
> **Seamus Donoghue**, VP of Sales & Business Development at METACO.

## DECENTRALIZING DIGITAL ASSETS



# E is for ETHEREUM

Ethereum is often compared to Bitcoin and thought of as an alternative to it. But while Ethereum uses blockchain technology and has its own cryptocurrency — Ether — that's where the similarities with Bitcoin end.

Bitcoin's ultimate aim is to provide a medium of exchange that's better than traditional money. By contrast, Ether is only one small part of the Ethereum project. First and foremost, Ethereum is a multipurpose, public, and open source software platform: a decentralized internet, if you will.

Ethereum's blockchain is a transaction-based state machine. Put simply, this means that when a transaction — or block — is verified, Ethereum's blockchain transitions from one state to another. Verification happens through mining, a process in which computers either solve complex mathematical problems or confirm that those problems have been solved correctly.

Ethereum's biggest upside is that it can store not just information about financial transactions, but also computer code. This means that the Ethereum blockchain has practical applications that go well beyond currency or financial services.

Developers can use the Ethereum blockchain to build and deploy Dapps — decentralized, autonomous apps — with a wide range of possible applications. They can also create decentralized autonomous organizations (DAOs) for any industry imaginable.

Dapps and DAOs built on the Ethereum blockchain are powered by smart contracts. These are agreements written using computer code that is designed to enforce what's been agreed automatically when a set of predetermined criteria are met. As a result, Dapps and DAOs can operate continuously and autonomously, without the need for human monitoring or intervention.

## SOME FACTS

- Ethereum's inventor, Vitalik Buterin, first put forward his ideas in a 2013 white paper he sent to a few close friends for feedback. The white paper was so well-received that his friends forwarded it to several other people until, eventually, around 30 interested parties got in touch to discuss how they could make the project happen. Buterin was just 19 years old at the time
- Ether is a cryptocurrency, but it's also the 'fuel' of the Ethereum blockchain. You need to pay a fee in Ether to change an app, execute a smart contract, or do some other action on the Ethereum blockchain. The fee is worked out based on how long the action will take and how much computing power is needed to perform it
- Ethereum has four times more developers than any other blockchain. The Ethereum Alliance, or EEA, is an association of developers and block startups and includes the likes of Deloitte, Intel, JP Morgan, Microsoft, and Samsung SDS.

- While the Ethereum blockchain was crucial in popularising smart contracts, the concept dates back to the mid-90s. Computer scientist Nick Szabo first described smart contracts in 1996 and spent several years developing the idea, publishing a number of papers in the process
- Interestingly, Szabo has been mooted as the true identity of Bitcoin's inventor Satoshi Nakamoto. Szabo has categorically denied this.

## WANT TO KNOW MORE?

The Ethereum white paper — A Next Generation Smart Contract & Decentralized Application Platform — is a fascinating insight into Buterin's thought process. Buterin's initial intention was to improve on Bitcoin by introducing features such as blockchain-based escrow and withdrawal limits. But he quickly realised that blockchain technology could be applied to any type of transaction imaginable.

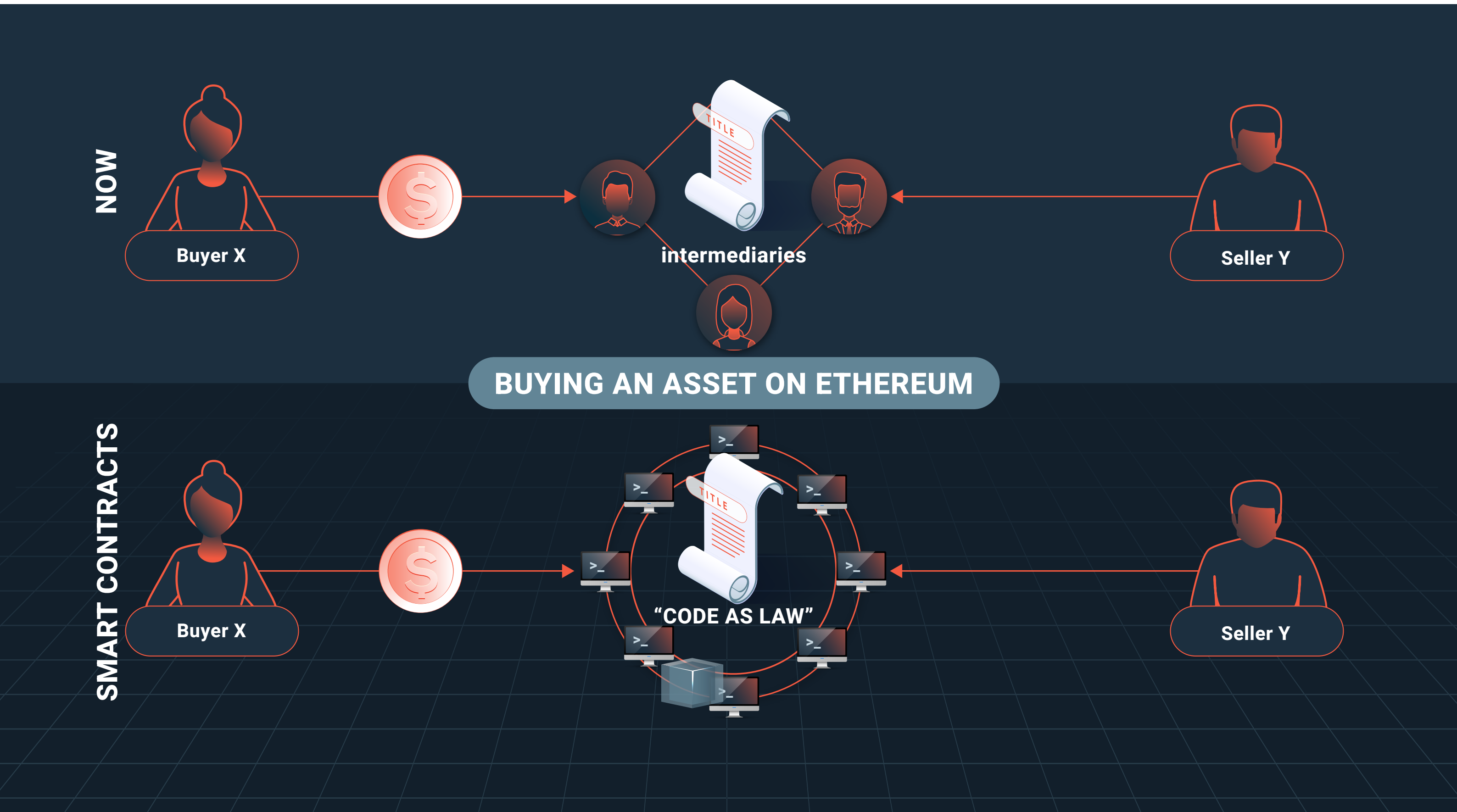
If you'd prefer a lighter read, this article on CoinTelegraph is a good overview of what Ethereum is, how it works, and its pros and cons.

And if you want to go deeper and find out more about Ethereum 2.0, also known as Eth2 or "Serenity", which is the planned upgrade to the Ethereum network that aims to make the blockchain more scalable, secure, and sustainable, read our dedicated article.

## THE METACO VIEW

> *"Ethereum has been pivotal in opening up mainstream consciousness to the blockchain's potential. With Ethereum, the conversation is no longer about theoretical potential. There's an infinite number of real world use cases that can materially improve our everyday lives and revolutionise industries that are ripe for change."*

## HOW ETHEREUM WORKS - THE ABRIDGED VERSION



# F is for FORK

A fork is a split in a blockchain network. It can be accidental or intentional. An **accidental fork** happens when two or more miners find a block at the same time.

When subsequent blocks are added, one chain becomes longer than the other. The system will ignore blocks on the shorter chain, and this resolves the fork. The abandoned blocks are known as ‘orphaned blocks’.

**Intentional forks** happen when someone purposefully modifies the blockchain’s rules. Blockchain software is open source. So anyone can access it and make changes.

Intentional forks can be soft or hard.

**Soft forks** happen when some network nodes are upgraded while others aren’t, but the upgrade is compatible with the old rules. In this case, the upgraded and non-upgraded nodes can still communicate with each other.

By contrast, **in a hard fork**, the upgrade isn’t compatible with the old rules, so upgraded and non-upgraded nodes can no longer communicate. As a result, the blockchain splits into two separate networks: one that follows the old rules and one that follows the new rules.

When a blockchain splits, the two chains will share the same history up to the time of the split. But, from the moment the split happens, each blockchain will take on a life of its own, creating its own history.

Needless to say, hard forks have wide-ranging — indeed, divisive — implications, whereas soft forks tend to have mainly cosmetic effects. That said, the only way to reverse the effects of a soft fork is a hard fork.

## SOME FACTS

- Most forks are short-lived. Typically, they’re used to add new features or fix bugs. P2SH (pay-to-script-hash), for example, was added to Bitcoin in 2012 to enable users to send Bitcoins without having to worry about how the recipient would gain access to them
- Bitcoin XT is one of the first known hard forks. Its aim was to increase the number of allowable transactions from seven per second to 24 per second. Sadly, interest waned quickly. And while Bitcoin XT is technically still available, it’s fallen into disuse
- Bitcoin Cash, a 2017 hard fork also on the Bitcoin network, was far more successful. It currently has a market cap of $4.6 billion. This fork was a result of disagreements in the Bitcoin community on the best way to scale.

## WANT TO KNOW MORE?

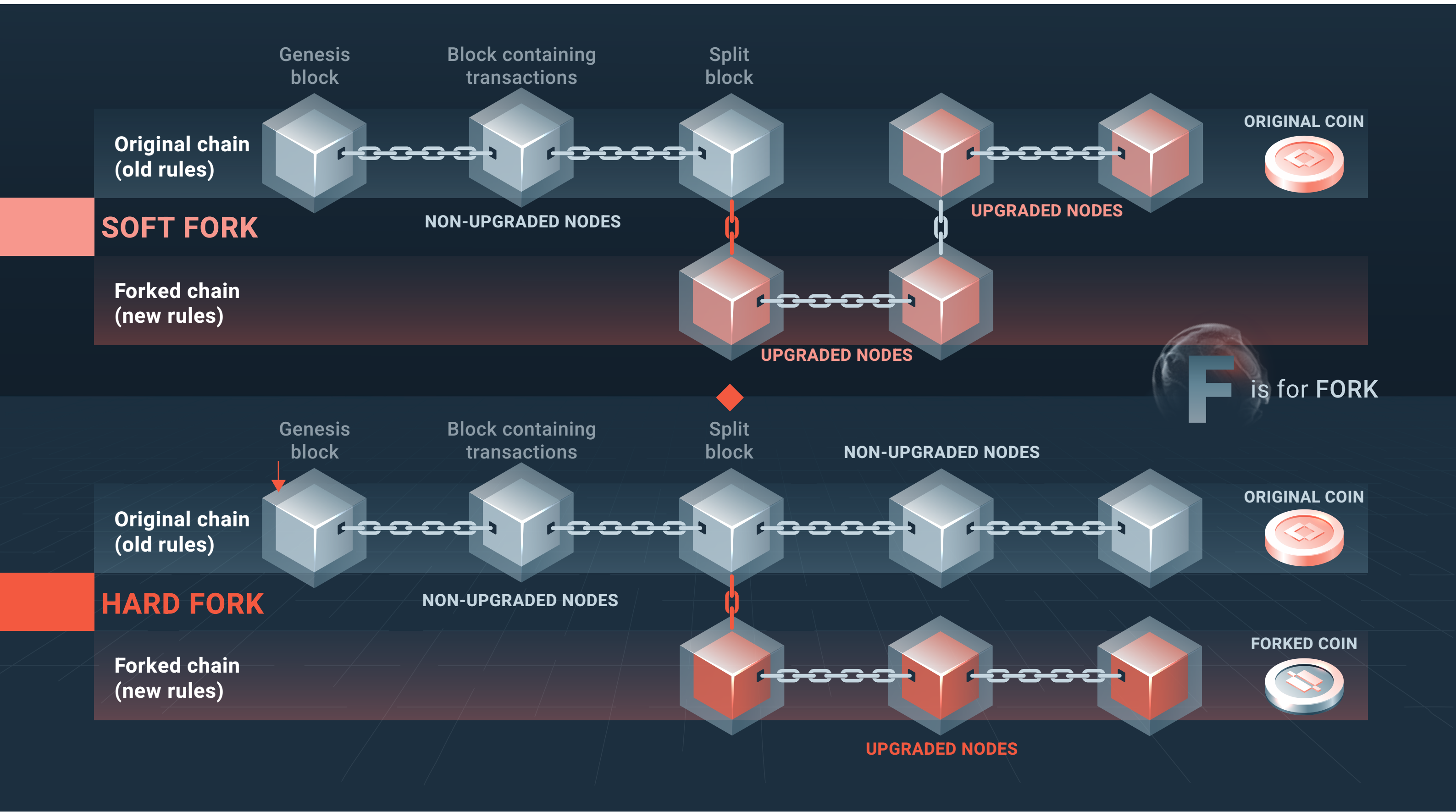
This article and accompanying video on Binance Academy walks you through the different types of forks and the rationale behind them. It also offers a fascinating insight into the politics of cryptocurrency decision-making.

If you want a better grasp of how common disagreements are in the crypto community, this post lists every hard fork there's been on every cryptocurrency network.

## THE METACO VIEW

> *"As much as disagreements are healthy and change can be for the better, forks, whether hard or soft, can have significant implications on crypto asset holdings. It's critical to have strong frameworks and governance in place, as this will help ensure any divergence is handled smoothly."*

## THE TWO TYPES OF FORKS IN A BLOCKCHAIN NETWORK



# G is for **GAS**

In crypto, gas can mean one of two things:

- Gas coin, a cryptocurrency
- A unit that measures how much computer power is required to perform an action on the Ethereum network.

**Gas coin**
Gas coins are tokens generated on NEO, a decentralized app platform based in China and originally called Antshares. NEO's aim is to create a smart economy by using blockchain technology and smart contracts to issue and manage digital assets.

Gas coins are one of two types of tokens created on NEO, the other one being NEO tokens. Gas coins are utility tokens, not assets. This means that, rather than having value as a medium of exchange, they grant the holder access to specific services.

Users need Gas coins to execute smart contracts and pay for the cost of transaction fees on the NEO network.

**Gas (Ethereum)**
On the Ethereum network, gas is a unit of measurement. It's the fee required to execute a smart contract or perform a transaction.

Gas compensates miners — the network users that carry out the complex mathematical calculations necessary for processing and verifying transactions on the Ethereum network — for the computing power required to perform the action. It's worked out as a fraction of Ethereum's cryptocurrency Ether and typically referred to as gwei.

The minimum amount of gas, or gwei, required in a given situation is determined by the miners themselves. A transaction may fail or be declined if the amount of gas the user offers doesn't meet the threshold the miners set.

## SOME FACTS

- It's no coincidence that Gas coins share the same name and purpose as gas on the Ethereum network. NEO is a direct competitor of Ethereum, to the point where it's been dubbed the "Chinese Ethereum"
- According to the Ethereum yellow paper — a more technical version of the white paper Ethereum's inventor Vitaliki Buterin wrote in 2013 — every transaction on the Ethereum network requires at least 21,000 gwei. This is equal to 0.000021 Ether

- The rising popularity of decentralized finance apps — apps aimed at cutting out intermediaries from financial transactions — is increasing network congestion. In turn, this is increasing gas fees, because more congestion means more computing power is needed to perform an action. On 1 September 2020, Ethereum miners earned a whopping $500K in gas fees in one hour.

## WANT TO KNOW MORE?

If you want to learn how gas works on Ethereum, this article stands out for its thoroughness. It starts with what prompted the idea for Ethereum in the first place and goes on to explain smart contracts, the Ethereum Virtual Machine — which developers use as a sandbox for building and testing decentralized apps — and how gas fits into the picture.

Want to learn about Gas coin? This article is an excellent introduction to it and to the NEO network.

## THE METACO VIEW

> *“Rising gas prices are exposing some scalability issues for Ethereum, which could have negative implications on the network’s usability and the viability of many of its most exciting use cases. On the upside, rising gas prices create the incentive for miners to invest in more and better technology to improve scalability as well as opening the door for competitors to swoop in and steal market share.”*

THE “GAS” THAT FUELS ETHEREUM

# H is for HASH

A hash is a hexadecimal number that represents a string of data. The process that converts the data into a hash is called hashing.

Hashes are deterministic. In other words, a specific string of data always produces the same hash. So if XYZ is hashed into ecf5b31f02c66b85, for instance, the latter will always be XYZ's hash.
That said, hashing algorithms are typically designed to be one-way. So, while hashes are deterministic, it's extremely difficult to convert them back into the original string of data. This ensures they're secure.

Hashes are also always the same length, regardless of how long — or short — the original string of data was. The hash's length depends on which hashing algorithm is used. Bitcoin, for instance, uses the SHA-256 hashing algorithm, so hashes are always 256 bits — 64 characters — long.

In the crypto space, hashes have a number of important functions:

- They're proof of work. The solutions to the mathematical puzzles that miners must solve to earn new coins and verify transactions are hashes.
- They link blocks together. Each verified block on a blockchain has a 'hash pointer' which identifies the previous block's address and the data it holds. This is how the blocks on the blockchain are 'chained' together.
- They make the blockchain immutable. Because every valid block on the chain contains a hash of the previous block, any attempts to change one block will affect every other block on the chain. Changing every single block requires so much computing power that it's not technically feasible.

## SOME FACTS

- The word "hash" comes from the French "hacher", which means to chop into small pieces. This is an apt description of what hashing does: it chops up a large string of data so it's smaller and more manageable but still identifiable.
- Whitfield Diffie and Martin Hellman identified the need for one-way hashing in public key cryptography in an academic paper published in 1976. But the first practical application came in 1993, when Cynthia Dwork and Moni Naor invented a hash-based proof of work system that could be used to prevent denial of service attacks and other online abuses, including email spam.
  Dwork and Naor didn't call their system 'proof of work', though. Credit for this goes to Markus Jakobsson and Ari Juels, who coined the term in a 1999 paper.
- Many commentators argue that, while quantum computers do present risks to the blockchain, hashing algorithms should be safe. This is because they're relatively unstructured. So, while quantum computers are far faster and more powerful than traditional machines, they'd still have to try and break a hash the same way a traditional machine would: through a brute force attack (a type of attack in which the machine keeps submitting different combinations until it guesses the right one).

- That said, Brandon Rodenburg and Stephen P. Pappas are less optimistic. In a 2017 technical report, they theorised that when a quantum computer attacks a hash, the hash would only be half as secure as it would be while under attack by a traditional device.

## WANT TO KNOW MORE?

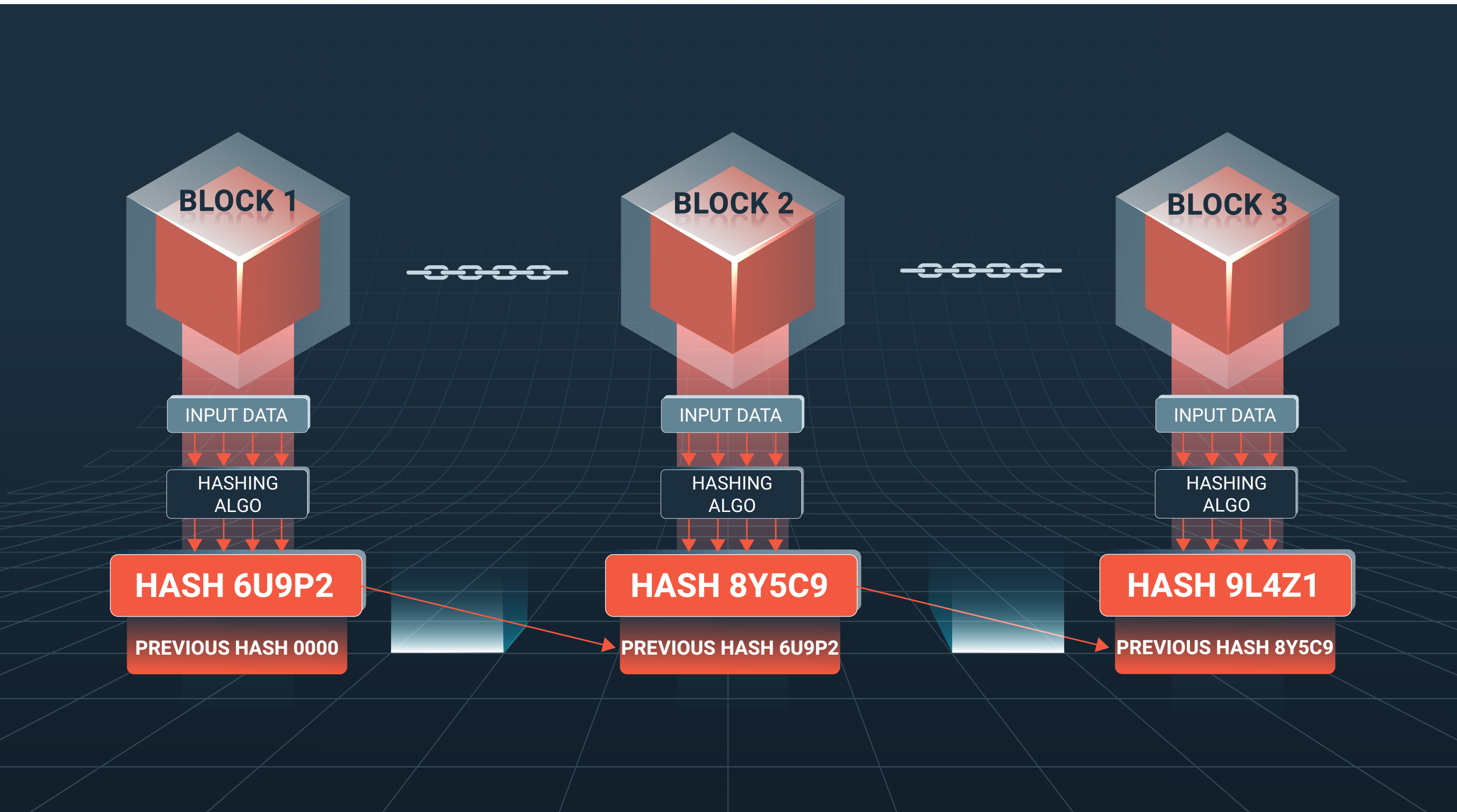
Diffie and Hellman's paper, written at a time when cryptography was still in its infancy, is remarkably forward-looking, but it also highlights quite starkly the technological limitations of the time.

Rodenburg and Pappas' report has an excellent explanation of hashing algorithms and how quantum computing could put their security at risk.

## THE METACO VIEW

> *"Hashes are at the core of crypto. They preserve data integrity and keep blockchains secure. So while it remains to be seen whether quantum computers will be able to crack hashes, more powerful hashing algorithms are a good thing, because they'll strengthen the blockchain, which ultimately benefits everyone."*

## HOW HASHING WORKS



# I is for **INITIAL OFFERING**

Initial offerings are the cryptocurrency world's version of an IPO.
There are two main types of initial offerings:

- **Initial coin offerings**, or ICOs
  As the name suggests, in an ICO investors receive an amount in a new cryptocurrency in exchange for their investment
- **Initial token offerings**, or ITOs
  In an ITO, the project seeking funding doesn't issue a new coin. Instead, investors receive tokens in exchange for their investment.

  These tokens can be:

  - Security tokens — traditional assets that have been converted into a tokenized, digital format on a blockchain-based platform
  - Utility tokens — assets that give the holder access to a product or service. For example, Gas coins grant their holders access to the NEO network.

While ICOs and ITOs are similar to IPOs in concept — all three have the purpose of raising money from the public — there are some key differences.

Firstly, most IPOs are launched by established companies seeking further growth. By contrast, ICOs and ITOs are typically launched to fund projects that are still in their initial stages. The project's details are usually set out in a white paper on the ICO or ITO's website.

Secondly, and more importantly, unlike IPOs, ICOs and ITOs do not usually grant investors an ownership stake in the project being funded. Instead, they give the holder of the coins or tokens other benefits.

For example, a token could give you preferential access to the product or service that will be sold once the project launches. Alternatively, you may be able to

## SOME FACTS

- The first initial offering was held by MasterCoin — now known as Omnilayer — in 2013. But ICOs and ITOs really took off in 2017. That year, there were approximately 50 initial offerings a month, which collectively raised $4 billion
- Brave Browser's ICO in May 2017 raised $35 million in 30 seconds. But the highest grossing initial offering to date was launched by Filecoin, which offers decentralized cloud storage. Their ITO raised $257 million in one hour

- ICOs and ITOs are largely unregulated, but they're increasingly appearing on regulators' radars. In the UK, the Financial Conduct Authority has taken the view that tokens are 'specified investments' — and, so, regulated — if they grant holders some of the rights typically enjoyed by shareholders, bondholders, and fund investors. Similarly, the SEC considers some types of initial offerings to be 'securities offerings', which means they fall under its jurisdiction.

## WANT TO KNOW MORE?

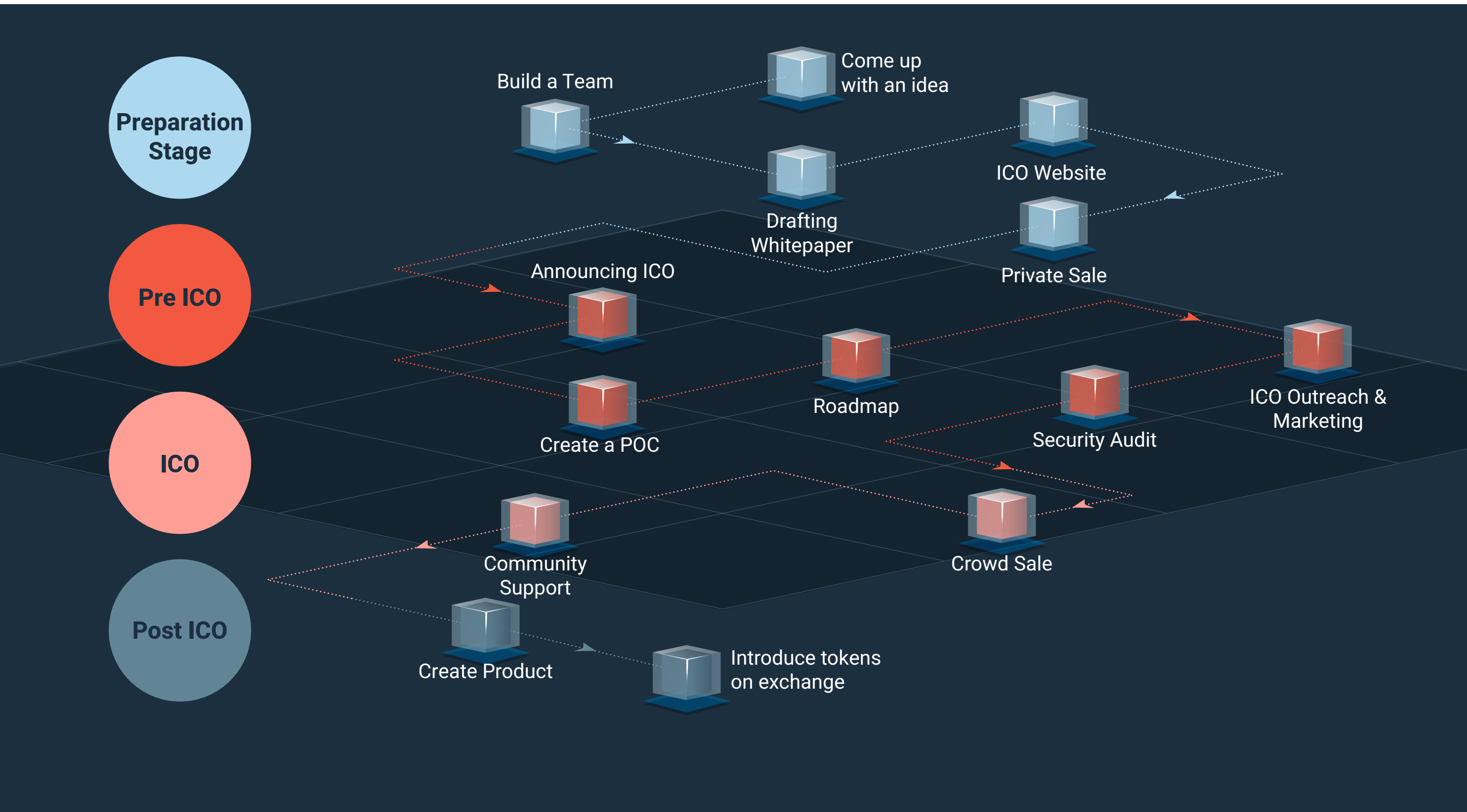
This interactive map runs you through the regulatory status of ICOs and ITOs  in 11 jurisdictions, including the US, UK, and Japan

Because the barriers to entry are low, ICOs and ITOs can be exploited by fraudsters and scammers. This excellent guide by CoinTelegraph walks you through the ins and outs of picking an initial offering to invest in, including how to spot red flags

## THE METACO VIEW

> *"ICOs and ITOs could revolutionise entrepreneurship, because they open a route to getting exciting and potentially transformative projects off the ground to founders who wouldn't be able to get funding via traditional means. The challenge moving forward is going to be finding a way to regulate the process and curb abuse without stifling cryptocurrencies' original mission — democratising finance for all."*

## HOW TO LAUNCH AN ICO OR ITO



# J is for JAMIE DIMON

Jamie Dimon has been the chairman and CEO of US banking giants JP Morgan since 2005. He made the Time 100 — Time magazine's yearly list of the 100 most influential people — in 2006, 2008, 2009, and 2011. Dimon made headlines in 2017 when he declared Bitcoin a scam that would blow up. In a blistering conference speech, he didn't hold back: *"It's worse than tulip bulbs. It won't end well. Someone is going to get killed."*

He then went on to say that wouldn't think twice about firing JP Morgan traders who bought Bitcoin: *"It's against our rules and they are stupid."*

Dimon's remarks caused a stir, not least because they came at a time when Wall Street was starting to take cryptocurrencies seriously. Indeed, JP Morgan themselves were reportedly involved in some Ethereum blockchain projects at the time.

Just a few days after Dimon's remarks, Citigroup CFO John Gerspach said, *"We think the area of cryptocurrency and digital currency is an area worthy of exploration."*

And JP Morgan's CFO Marianne Lake also struck a more measured tone, saying that *"We are open-minded for digital currencies that are properly controlled and regulated."*

Dimon blasted cryptocurrencies on subsequent occasions, too. Answering a question at an Institute of International Finance Conference shortly after he made his infamous remarks, for instance, he repeated his view that
*"If you're stupid enough to buy it, you'll pay the price for it one day."*

But in 2018, barely a year after his infamous remarks, he expressed his regret and retracted them:
*"The blockchain is real. You can have crypto dollars in yen and stuff like that. ICOs ... you got to look at every one individually. The bitcoin was always to me what the governments are going to feel about bitcoin when it gets really big. And I just have a different opinion than other people."*

## SOME FACTS

- Dimon's retraction couldn't have come at a more convenient time for JP Morgan. Shortly thereafter, the bank launched a blockchain centre of excellence with the aim of "actualize[ing] enterprise-grade blockchain tools" and "drive[ing] industry standards."
- JP Morgan came full circle in 2020, when their head of U.S. interest rate derivatives strategy hailed cryptocurrencies' resilience and recommended them as institutional investments.
- '...worse than tulip bulbs' is a reference to a 17th century economic crash brought about by runaway speculation on the price of... tulip bulbs.

- When tulips were introduced to Europe in the late 1500s, they were unlike anything grown natively, so they quickly became a sought after luxury item.
- At the height of tulipmania, rare bulbs could fetch up to six times the average person's annual salary. And this is when things went wrong. Speculators started purchasing future consignments on credit, banking on the fact that they could sell them on at a profit. But once the novelty wore off, prices nosedived and people went bankrupt.

## WANT TO KNOW MORE?

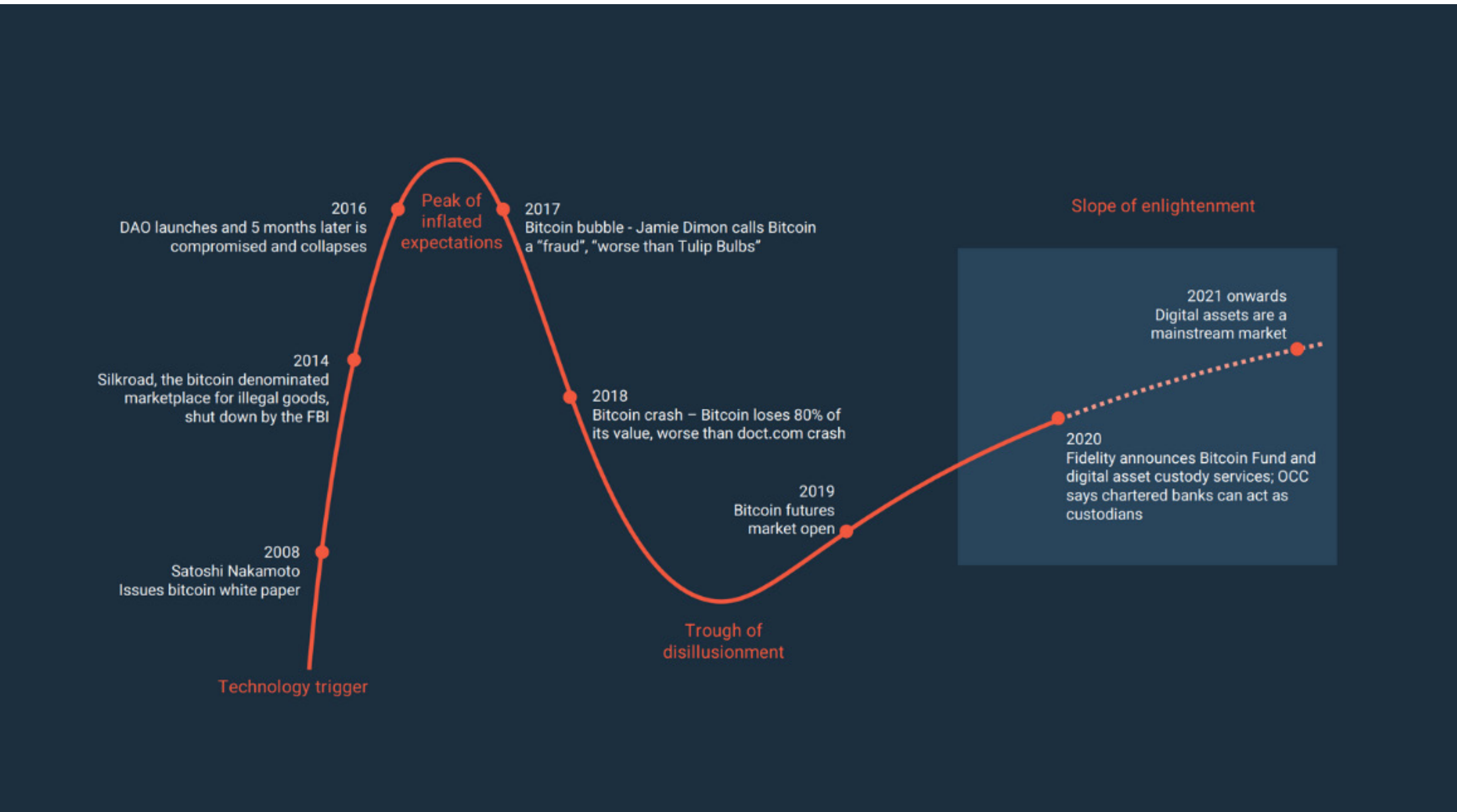
Dimon made his negative opinion of Bitcoin known again when he testified in front of congress in 2018 shortly before his much publicised retraction. He was less blunt this time though, repeating the line that "We are supportive of cryptocurrencies as long as they are properly controlled." Needless to say, Bitcoin supporters didn't take his comments well and made their opinions very clear in the comments.

While their 2020 report on Bitcoin isn't publicly available, this article highlights just how far in the other direction JP Morgan has gone since Dimon's 2017 remarks. While arguing that Bitcoin is still primarily speculative, the report says that *"there is little evidence of run dynamics, or even material quality tiering among cryptocurrencies, even during the throes of the crisis in March."* This, concludes the report, suggests Bitcoin passed its first stress test.

## THE METACO VIEW

> *"JP Morgan's change in tack from sceptics to endorsers shows we're well and truly through the hype cycle. Having institutional investors on board can only increase trust in cryptocurrencies as a legitimate asset class. This will allow these assets to start fulfilling their potential."*

## THE HYPE CYCLE


Peak of inflated expectations
2016
DAO launches and 5 months later is compromised and collapses
2017
Bitcoin bubble - Jamie Dimon calls Bitcoin a "fraud", "worse than Tulip Bulbs"
Slope of enlightenment
2021 onwards
Digital assets are a mainstream market
2014
Silkroad, the bitcoin denominated marketplace for illegal goods, shut down by the FBI
2018
Bitcoin crash – Bitcoin loses 80% of its value, worse than doct.com crash
2020
Fidelity announces Bitcoin Fund and digital asset custody services; OCC says chartered banks can act as custodians
2019
Bitcoin futures market open
2008
Satoshi Nakamoto Issues bitcoin white paper
Trough of disillusionment
Technology trigger

# K is for KEY

Keys enable two parties to complete a cryptocurrency transaction securely. They also prove that the transaction is legitimate. Or, in other words, that it was made by the true owner of the funds.

You need two keys to perform a cryptocurrency transaction: a public key and a private key.

As the name suggests, public keys are publicly known. This is because their purpose is to identify the individuals taking part in the transaction. By contrast, a private key is secret and only known to the individual who holds it. Private keys authenticate and encrypt transactions.

It's helpful to think of a public key as a username, or an email address. Others can use this information to look you up and get in touch. A private key, on the other hand, is the password you'd use to log onto your account.

In cryptocurrency, you don't own the coins themselves. What you really own are private keys. Whoever has access to the private key controls the coins that key grants access to. More importantly, if you lose your private keys, there's no way to recover your coins. This is because, unlike fiat currencies, cryptocurrencies aren't backed by a central authority. Instead, they run on a decentralized, immutable public network.

This means it's important to keep your private keys safe.

There are three main ways to store keys:

- **Hot wallets**
  Here, the keys are stored on the internet. This is the most practical form of storage, because it gives you instant access to your cryptocurrency when you need it. The flipside is that your private keys are more vulnerable to attacks by malicious hackers.

  Experienced cryptocurrency users typically store only a small portion of their cryptocurrency holdings in hot wallets, for this reason
- **Warm wallets**
  Warm wallets store keys in downloadable software instead of an online server. You need a code or PIN to gain access to the key.

  The advantage is that warm wallets are only connected to the internet when you need them. This means they're harder to hack than hot wallets. That said, when they're connected to the internet, there's a window in which malicious hackers can try their luck
- **Cold storage**
  Here, the private key is stored offline. This could be as simple as writing it down on a piece of paper placed in a locked drawer, or as sophisticated as using an air-gapped server — a standalone server that isn't connected to the internet or another unsecured network.

  Offline keys can't be hacked, because they don't come in contact with a publicly accessible server. The trade-off is that it takes longer to make a transaction

## SOME FACTS

- The system of public and private keys that cryptocurrency transactions use is called public-key cryptography, or asymmetric cryptography.
  Stanford University researchers Whitfield Diffie and Martin Hellman publicised the concept in a 1977 paper. But it was originally — and covertly — proposed several years earlier by James Ellis, who worked with British intelligence
- Asymmetric cryptography isn't exclusive to the crypto world. Transport layer security (TLS) and secure sockets layer (SSL) — the protocols that make HTTPS possible — also also use asymmetric cryptography
- Over the years, improper private key storage has led to many headline-grabbing hacks. The biggest one ever recorded happened in January 2018, when NEM coins worth $534 million disappeared from Japanese crypto exchange Coincheck. NEM's president Lon Wong called the hack "the biggest theft in the history of the world."

## WANT TO KNOW MORE?

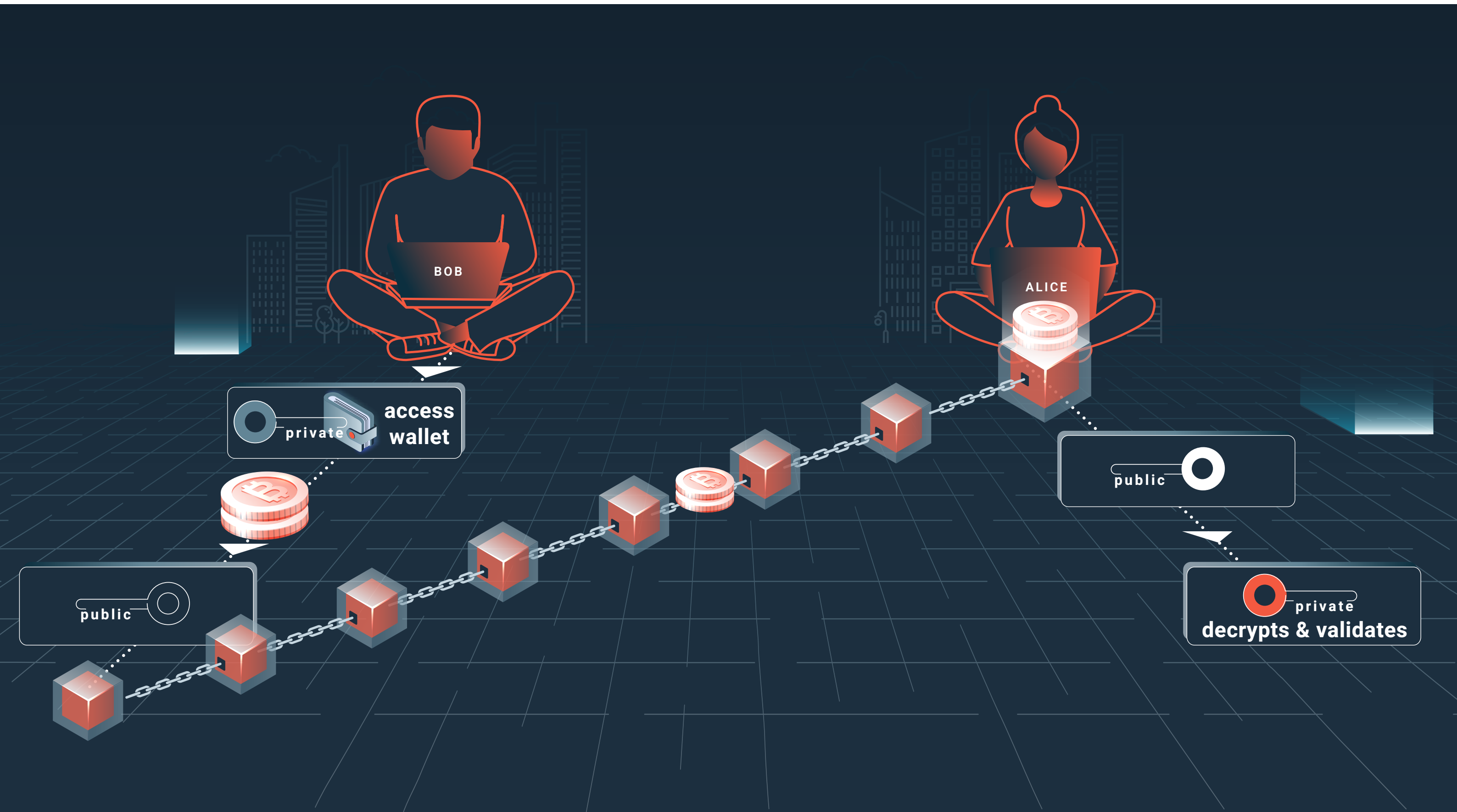
This article explains asymmetric encryption in the plainest terms possible and compares it to symmetric encryption — the standard for cypher systems before the mid-1970s

For a more light-hearted but no less hair-raising read, here are 7 unfortunate ways people compromised their private keys. One even involves an ill-advised trip to the tip

## THE METACO VIEW

> *"Proper security is crucial in decentralized systems. At Metaco, we continually look ahead to make sure we anticipate and neutralise new threats as they appear, whether they stem from technological vulnerabilities or human error."*

## ANATOMY OF A CRYPTOCURRENCY TRANSACTION



# L is for LEDGER

A ledger is the public, decentralized record-keeping system that crypto assets run on. It stores data in encrypted files called blocks. These blocks are connected, or chained, to one another, which is why crypto ledgers are known as ‘blockchains’.

The first block in a chain is created when the network goes live. This is known as the genesis block.

Network participants authenticate, verify, and record data onto a block by solving complex mathematical calculations — this is called proof of work or proof of stake. Once the data is verified and recorded onto a block, it can’t be edited, because any subsequent proof of work or proof of stake would invalidate it.

When a block is full and can’t store further data, a new block is mined and added to the chain. A copy of the ledger is stored on several network participants’ devices. These participants are called ‘full nodes’.

The first public blockchain — the Bitcoin blockchain — stores anonymised data about network participants and how much Bitcoin they possess. It also has a record of every legitimate Bitcoin transaction ever made.

But blockchains have applications that go well beyond finance, because they can record and store almost any type of data: product inventories, legal agreements, public records, and even election votes. And since every data point is verified via proof of work or proof of stake and can’t be subsequently altered, tampering and fraud are far more difficult, if not impossible.

## SOME FACTS

- The first known ledgers date back 7,000 years to Mesopotamia (modern-day Iraq). Traders recorded their inventory and expenses on clay tablets which they kept in temples for safekeeping. At the time, temples did double duty: they were places of worship and also places where people stored their valuables, essentially making them the first banks
- Ledgers remained relatively unchanged until Italian mathematician Fra Luca Pacioli popularised double-entry bookkeeping in the 15th century. This system made it possible for debits and credits to be recorded on the same ledger and for different ledgers to be reconciled.
- Lorenzo de Medici used double-entry bookkeeping to create the first merchant bank, and it soon became the cornerstone of the banking industry as we know it today
- Bitcoin inventor Satoshi Nakamoto may have brought the blockchain into mainstream consciousness, but the technology dates back to 1991, when Stuart Haber and W, Scott Stornetta described “a cryptographically secured chain of blocks” for the first time.
- Haber and Stornetta were working on a system that could irreversibly time-stamp documents, a popular blockchain use case to this day

## WANT TO KNOW MORE?

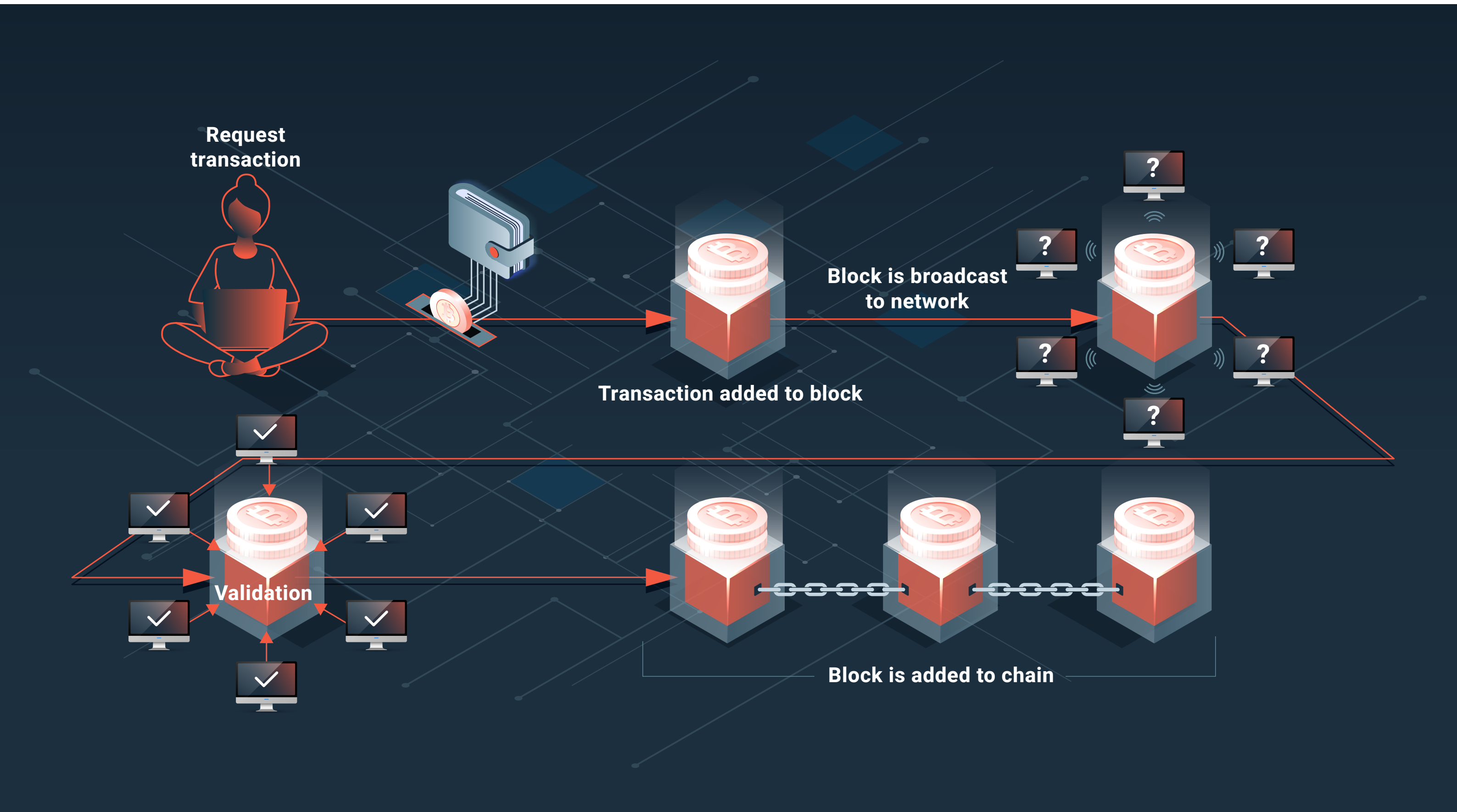
Haber and Stornetta's academic paper was published three years before the internet entered the public domain. But aside from being a fascinating historical document, it's remarkably forward-thinking

If you'd prefer a less technical blockchain explainer, it doesn't get much simpler than this video

## THE METACO VIEW

> *"The blockchain is a simple but powerful concept: an encrypted, decentralized database that could have profound implications for the world economy and for many aspects of our day-to-day lives — from how we work or run our businesses to the way we participate in civic life."*

## THE BLOCKCHAIN EXPLAINED



# M is for MINING

In the crypto ecosystem, mining serves two purposes:

- it produces new coins
- it verifies that information is accurate before it's permanently recorded onto the blockchain

Unlike fiat currencies, cryptocurrencies are decentralized, so no single organization is responsible for releasing coins into circulation. Instead, coins are awarded to miners who solve mathematical problems.

These mathematical problems are complex, and the rewards are random — your mining efforts could result in many coins, few coins, or none at all.

This is intentional. The system wants to ensure no single individual or group is in a position where they own the majority of the coins and, so, can influence the network.

Once a problem is solved — this is called proof of work or proof of stake — it has to be verified. Verifying proof of work and proof of stake is an easier process.

Again, this is by design. Easy verification means data can be recorded onto the blockchain relatively quickly. In Bitcoin, it typically takes about 10 minutes for proof of work to be verified and, so, for a transaction to go through.

In certain cryptocurrencies, there's a cap on how many coins can be mined. This is hardwired into the network's source code. For example, only 21 million Bitcoins can ever be mined. Once that limit is reached, it won't be possible for any further Bitcoins to enter circulation.

Ether, which is mined on the Ethereum platform, has a limit of 18 million coins a year, but no upper limit. So, in theory, an infinite number of Ether could be mined, provided miners stay within the yearly limit.

## SOME FACTS

- While Ether doesn't currently have a hard cap, Ethereum's creator Vitalik Buterin has proposed one. Buterin made his proposal on 1 April 2019, which led people to believe he was joking. But Buterin subsequently confirmed his proposal and encouraged the community to weigh up the pros and cons
- On the Bitcoin ecosystem, mining difficulty is adjusted every 2016 blocks — roughly every two weeks — to keep mining rates more or less constant. Difficulty increases when there are more miners on the network, and decreases when there are fewer miners
- The solution to a mining problem is typically a hexadecimal number, or hash. The Bitcoin network processes 5.5 quintillion hashes per second, which means you're unlikely to be a successful miner without access to heavy duty equipment

## WANT TO KNOW MORE?

This comprehensive resource covers everything you'd conceivably want to know about cryptocurrency mining.

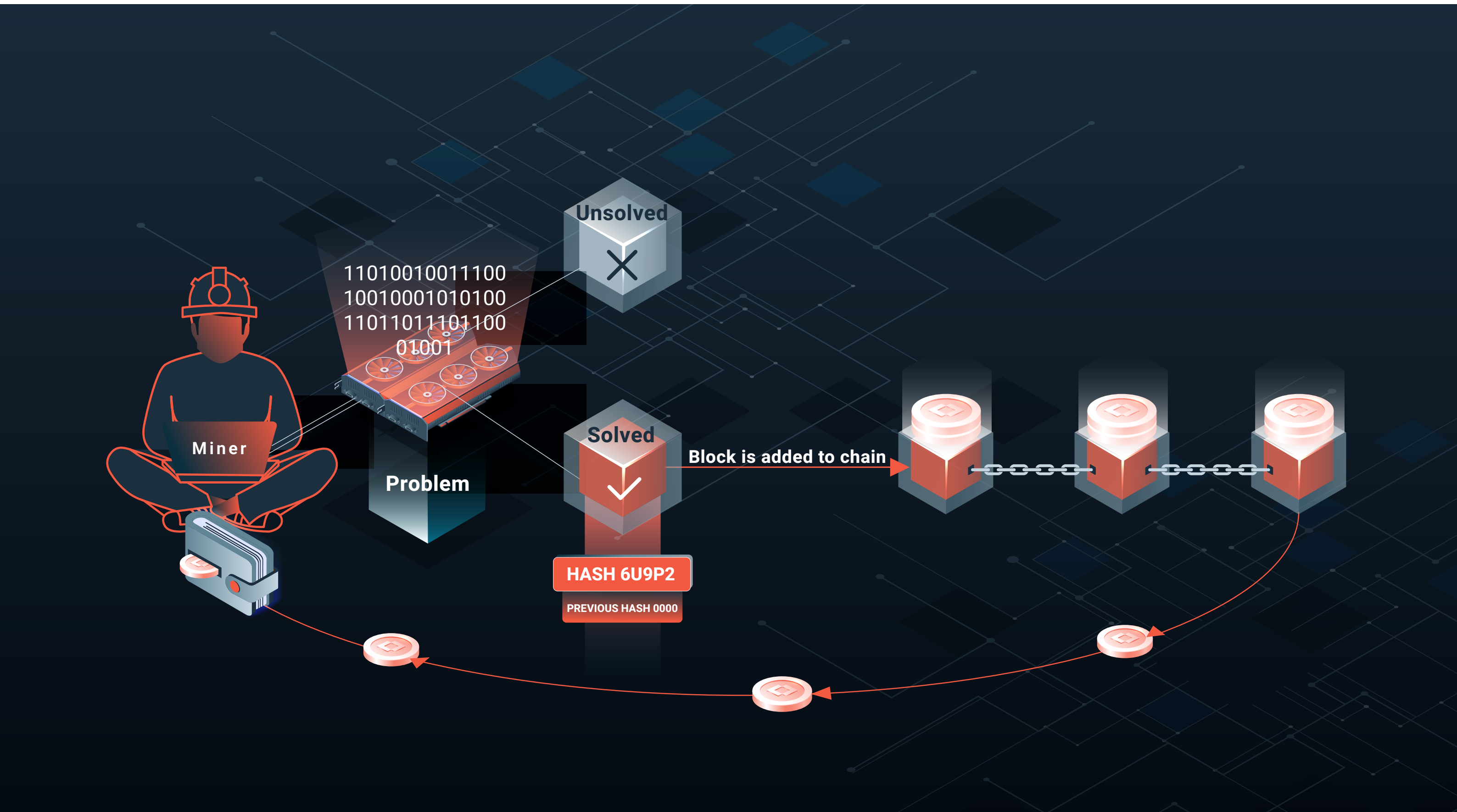
If you're wondering why Buterin proposed introducing a hard cap, here's a discussion on its pros and cons.

Of particular interest is the argument about centralisation. Mining difficulty and reward randomness should ensure no single individual or group can corner the market. But this is happening anyway because select miners have invested in high grade machinery the average miner couldn't access.
Buterin thinks switching to a fixed supply would allow the network to calibrate randomness in a way that'll make it harder for those with powerful equipment to have an edge.

## THE METACO VIEW

> *"There have been multiple times in the history of Bitcoin where mining was so centralised that the top two out of three miners were almost able to control the network. What we've seen is that, naturally, the network itself got so afraid that it fragmented by itself.*
>
> *This is as it should be. Excessive centralisation would hurt the trust and the security of the network and, ultimately the value of the coin."*
>
> **Adrian Treccani**, Founder and CEO

## MINING FOR COINS



# N is for **NON-FUNGIBLE TOKEN (NFT)**

Non-fungible tokens, or NFTs, are a type of cryptographic token — a digital representation of value that lives on the blockchain.

NFTs can represent the value of physical assets. A painting, for instance. But they can also represent the value of digital assets, such as a short story that is only available online.

NFTs have three characteristics that set them apart from other types of token:

1. **They're unique**
   Every single NFT represents a specific asset. This means there's no standard value. So, unlike other types of cryptographic token, NFTs aren't directly interchangeable.
   Even where several NFTs are similar — for example, a limited run of the same art print, or a batch of tickets for the same event — each NFT is treated as a unique asset and tracked on the blockchain separately.

2. **They're verifiable**
   NFTs can't be copied. It's also very easy to prove their authenticity. This is because their full history is recorded on the blockchain, so anyone can check it.

3. **They're tradeable**
   While NFTs aren't directly interchangeable — you can't swap one NFT for another as you would Bitcoin, for instance — there are specialised exchanges where you can buy, sell, and resell them. You can settle the transaction in fiat currency or in cryptocurrency.

NFTs' characteristics make them especially well-suited for protecting intellectual property rights.

Creatives can use NFTs to monetise their work while staying in control of who can use and reproduce it.

Similarly, selling tickets as NFTs has been touted as a solution to scalping — the practice of buying large numbers of tickets for sought after events and reselling them at a high markup.

## SOME FACTS

- NFTs exploded in early 2021, reaching $389 million in sales. But they've been around since at least 2012, when Bitcoin Coloured Coins started being traded. These were satoshis — fractions of a Bitcoin — that were marked, or coloured, with information that linked them to real-world assets.
- Bitcoin Coloured Coins were primarily used to trade 'Rare Pepe' digital cards — artwork of Pepe the Frog. At the time, Pepe the Frog was a popular meme. It would eventually be appropriated by and become synonymous with white nationalist groups and the alt right. Pepe's creator Mark Furie "killed" Pepe in 2017 to protest its continued use as a hate symbol.

- Nowadays, most NFTs are created and traded on the Ethereum blockchain. One of the first Ethereum-based NFTs was a game called CryptoKitties, in which users could sell virtual kittens.
- In 2018, an anonymous user bought a CryptoKitty called Dragon for 600 Ether. At the time, this was equivalent to $172,000.

## WANT TO KNOW MORE?

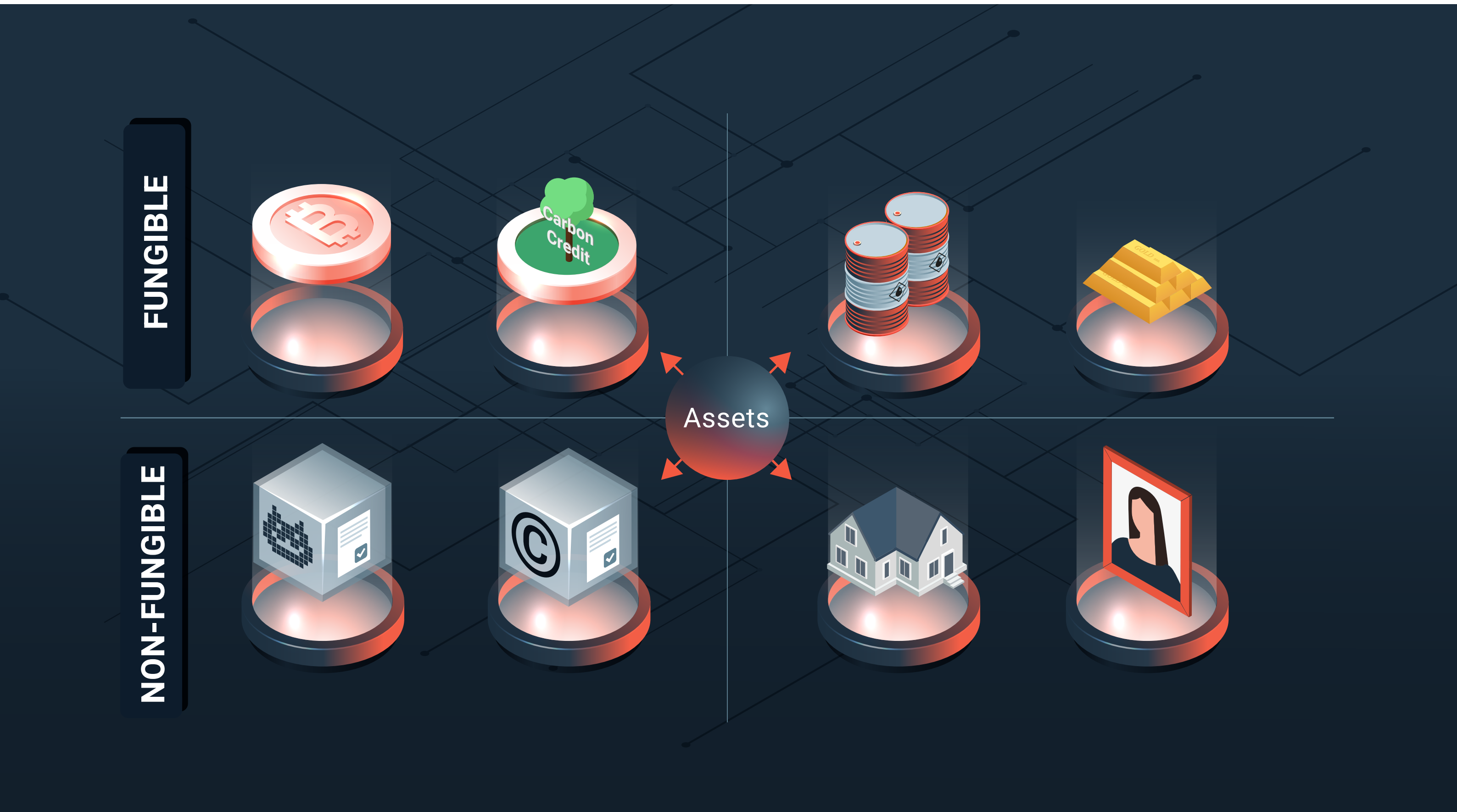
NFTs became technically possible on the Ethereum blockchain thanks to ERC-721, which was proposed by William Entriken, Dieter Shirley, Jacob Evans, and Nastassia Sachs in 2018. The authors had a wide range of use cases in mind, including real estate transactions and trading 'negative value assets' like loans.

Want to dip your toes into the NFT game? This article walks you through the process of creating, selling, and trading them.

## THE METACO VIEW

> *"Far from being a fad, NFTs are another step towards the digitalisation of everything. At some point, the explosion of NFTs means banks will be facing the same threats the post office faced with the rise of the internet, so they'll need to adapt and rethink their role in the value chain."*

## FUNGIBLE VS NON-FUNGIBLE TOKENS



# O is for OPEN

Open can mean two things in the crypto space:

- an open blockchain
- open source software

Most major blockchain-based projects — including Bitcoin and Ethereum — are both open and open source.

**Open blockchain**
An open blockchain is a public blockchain. Anyone can join and participate in the network, as long as they follow its rules. The blockchain's record is also public. Anyone can see it. But once a block of information is verified and added to the blockchain, it can't be changed.

Open blockchains are also known as permissionless, or trustless blockchains. This is because there are no gatekeepers. Data is recorded or rejected based purely on mathematical calculations. In comparison, you can only gain access to a closed blockchain if you have permission. Some — or all — of those who have access act as administrators and may edit the records.

Closed blockchains are also known as private or permissioned blockchains.

**Open source software**
Like the blockchain itself, open source software is decentralized. No single person or entity owns the software. Instead, it's created collaboratively, and anyone can use it as it is or alter it free of charge.

Open source software has three advantages over closed software.

Firstly, anyone can scrutinize the code, make improvements, and identify and fix bugs and other vulnerabilities.

Secondly, developers of closed software may get blind spots over time or stop caring about the project. But in an open source setting, new people are constantly coming in and bringing fresh perspectives with them.

Thirdly, developers who work on open source projects typically also use the software themselves. This means they can often flag issues and come up with practical solutions more quickly, because they have a deeper knowledge of the software's real world applications.

## SOME FACTS

- The open source movement dates back to 1983. The story goes that programmer Richard Stallman had been trying to get an office printer fixed but couldn't because the manufacturers wouldn't share the source code. Feeling frustrated, he launched the GNU Project with the goal of writing an operating system that anyone could use. The GNU Project is still active today.
- In 1991, Linux beat GNU to the punch and became the first open source operating system to go public. Ironically, the original version of Linux didn't have a free-software licence. Founder Linus Torvalds relicensed it as public in 1992 under a GNU public licence.
- Open and closed blockchains are often compared to the internet and intranets respectively. Like the internet, open blockchains seem destined for dominance. But closed blockchains still have useful applications.

## WANT TO KNOW MORE?

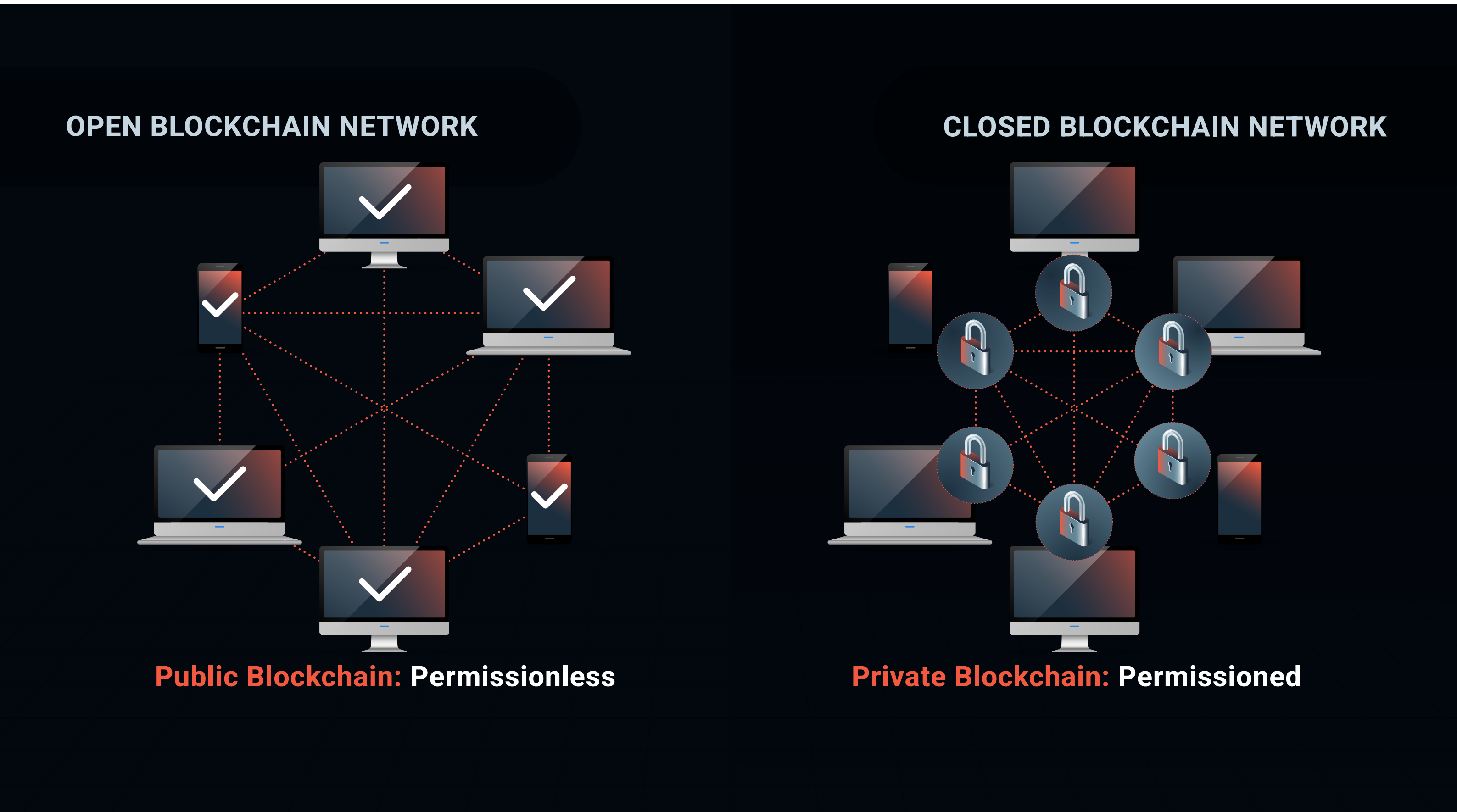
This article offers a look at the philosophy behind open source software and how it underpins blockchain technology.

In this article, our own Seamus Donoghue, VP of Sales and Business Development, discusses the merits of permissioned and permissionless blockchains and whether the two can coexist.

## THE METACO VIEW

> *"There are those who argue that open blockchains are the future and that closed blockchains will become obsolete. But the blockchain isn't an all or nothing proposition. Ultimately, the best option is the one that works for you."*

## OPEN VS CLOSED BLOCKCHAINS


OPEN BLOCKCHAIN NETWORK
CLOSED BLOCKCHAIN NETWORK
Public Blockchain: Permissionless
Private Blockchain: Permissioned

# P is for **PROOF OF WORK / PROOF OF STAKE**

Proof of work and proof of stake are two mechanisms through which cryptographic transactions can be verified and new blocks added to the blockchain. Blockchain platforms use either one or the other.
For example, Bitcoin uses proof of work, while Tezos and NEO use proof of stake. Ethereum used proof of work but switched to proof of stake in December 2020.

### Proof of Work

Proof of work is the solution to a mathematical problem. It has two functions:

- Creating new coins. This happens when miners on a cryptocurrency network compete against each other to solve a mathematical problem. The first miner to find the correct solution is rewarded with the new coins
- Verifying that individual transactions have followed the network's rules. In particular, proof of work prevents users from fraudulently inflating their cryptocurrency holdings by creating coins they haven't earned or spending the same coins twice (double-spending)

Proof of work is intentionally very complex to produce and its rewards are random. This is to ensure no single miner or group can gain an unfair advantage and be in a position to influence the network. But proof of work is also easy to verify. This allows transactions to get approved and new blocks to be added to the blockchain relatively quickly.

### Proof of stake

Proof of stake is the main alternative to proof of work. In proof of stake, miners have to deposit a number of coins — the stake — in a special wallet to get the chance to validate transactions and mine new blocks. Every network that uses proof of stake has its own rules around this, including the minimum stake you must deposit. Your stake remains frozen for as long as you're mining or verifying transactions. And you lose it if you try to game the system, for example by submitting a faulty block or trying to spend the same coins twice. But unlike proof of work, it's not the first miner to find the right solution who wins the reward in proof of stake. The network's algorithm chooses the winner.

The algorithm chooses the winner randomly. But your chances of winning are linked to the size of your stake as a percentage of the total number of coins in circulation. So if there are 5,000 coins in circulation and you've staked 500 coins, for instance, you have a 10% chance of winning.

## SOME FACTS

Proof of work was fundamental to getting Bitcoin off the ground, because it solved the issues — particularly double-spending — created by the fact there's no central authority to regulate the system. While proof of work may have solved issues that had previously made cryptocurrencies unworkable, it has problems of its own. In particular:

- It's resource intensive. Bitcoin miners, for instance, use more energy than Ireland and five times the output of Europe's largest wind farm in a given year.

- It has vulnerabilities. If a miner (or a group) manages to gain control of 51% of the network's computing power, they can break the network's rules, including blocking valid transactions and double-spending. This is known as a 51% attack.
- There have been no known successful 51% attacks to date, but they're theoretically possible.
- Because you need huge amounts of computing power to be a miner, networks that use proof of work have become somewhat centralised. On the Bitcoin network, for example, about 50% of the computing power is currently split between just three mining groups.

Proof of stake aims to solve proof of work's flaws, particularly electricity consumption. But it also has weaknesses. Specifically, some argue that miners have nothing to lose and everything to gain by staking multiple versions of the same blockchain, because their interest lies in ensuring their stake holds or increases its value. This could prevent new blocks from being validated. This is known as the 'nothing at stake' problem.

## WANT TO KNOW MORE?

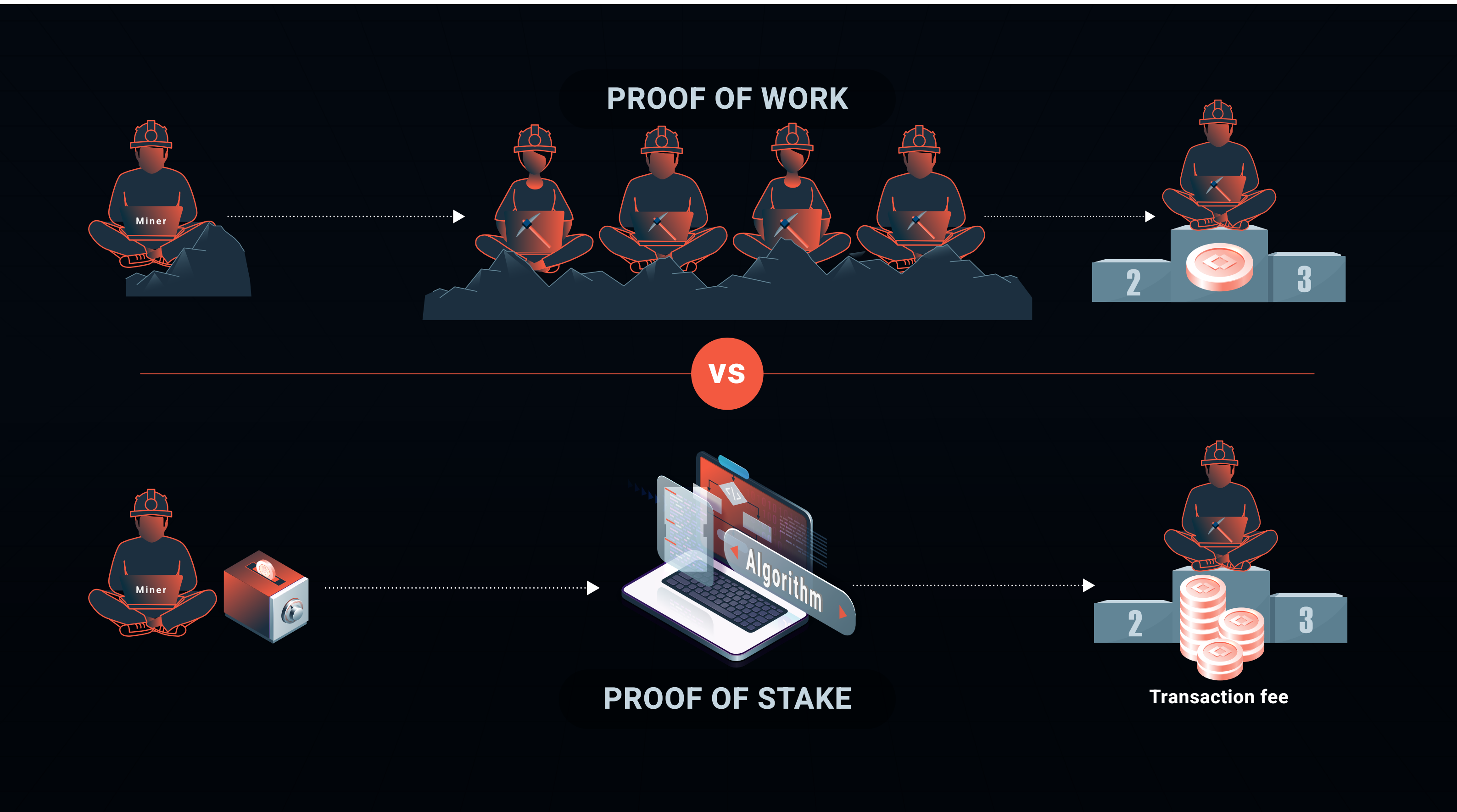
CoinTelegraph's Proof of Work explainer is highly readable and thorough. It walks you through the rationale behind proof of work, how it works — including what sorts of mathematical problems miners have to solve and how they solve them — and discusses the mechanism's flaws.

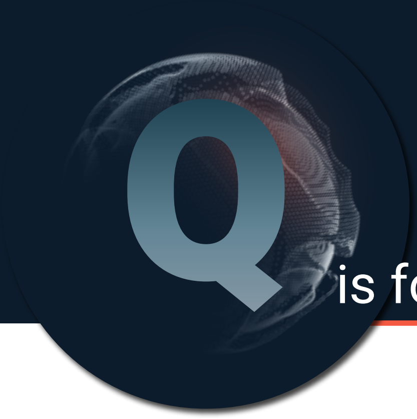
Proof of stake's creators Scott Nadal and Sunny King explained their thinking in this white paper published in 2012. Their prediction that proof of stake would become more competitive than proof of work seems remarkably prescient: Ethereum's switch in December 2020 has made proof of stake a dominant force in the crypto space. Proof of stake-based networks now collectively make up 15% of the total crypto market cap.

## THE METACO VIEW

> *"Proof of work is often criticised for being energy-intensive. But with 30% of it now powered by renewables, I think there's incredible potential for mining to be a boon for sustainable, eco-friendly technologies."*

## PROOF OF WORK VS PROOF OF STAKE





# Q is for QUANTUM RESISTANCE

Quantum-resistant algorithms — also known as post-quantum, quantum-secure, and quantum-safe — are cryptographic algorithms that can fend off attacks from quantum computers.

Quantum computers are machines whose processing power far outstrips even the most powerful supercomputers available today.

Traditional computers process information in bits — strings of 1s and 0s represented as electrical or optical pulses. By contrast, quantum computers use qubits. These are subatomic particles, typically electrons or photons.

Today's public blockchains, including Bitcoin, are secured using asymmetric cryptography. This means a user needs a public key and a private key to access their wallet.

The mathematical relationship between users' private and public keys is too complex for traditional computers. But a quantum computer could figure it out and gain access to users' wallets in a matter of days.

Quantum computers are still a highly specialised area. But experts think they could become commonplace and, so, an imminent threat to cryptographic security by the end of the 2020s. Blockchain networks will need upgrading before this happens.

A number of projects aimed at increasing cryptographic security and creating blockchain networks that can resist quantum computers' attacks are already underway.

## SOME FACTS

- The first quantum computing algorithm was published by Peter Shor in 1994 — three years before the first quantum computer was built. But the idea that quantum computers could solve problems traditional computers can't was first put forward by Richard Feynman, Paul Benioff, and Yuri Manin in the early 1980s.
- While the first quantum computer was built in 1997, the field became an arms race during the 2010s. IBM unveiled the first quantum computer for scientific and commercial use — IBM Q System One — in January 2019. In October of the same year, Google made history by announcing they'd achieved quantum supremacy. Their quantum computer had solved a mathematical problem it would take a traditional machine 10,000 years to solve.
- Researchers at the University of Singapore have said that Bitcoin's cryptographic algorithm could be under threat by quantum computers as soon as 2027.
  But some crypto experts aren't especially worried. When Google announced it had achieved quantum supremacy, Ethereum's founder Vitalik Buterin was unimpressed.

He tweeted:

*"My one-sentence impression of recent quantum supremacy stuff so far is that it is to real quantum computing what hydrogen bombs are to nuclear fusion. Proof that a phenomenon and the capability to extract power from it exist, but still far from directed use toward useful things."*

## WANT TO KNOW MORE?

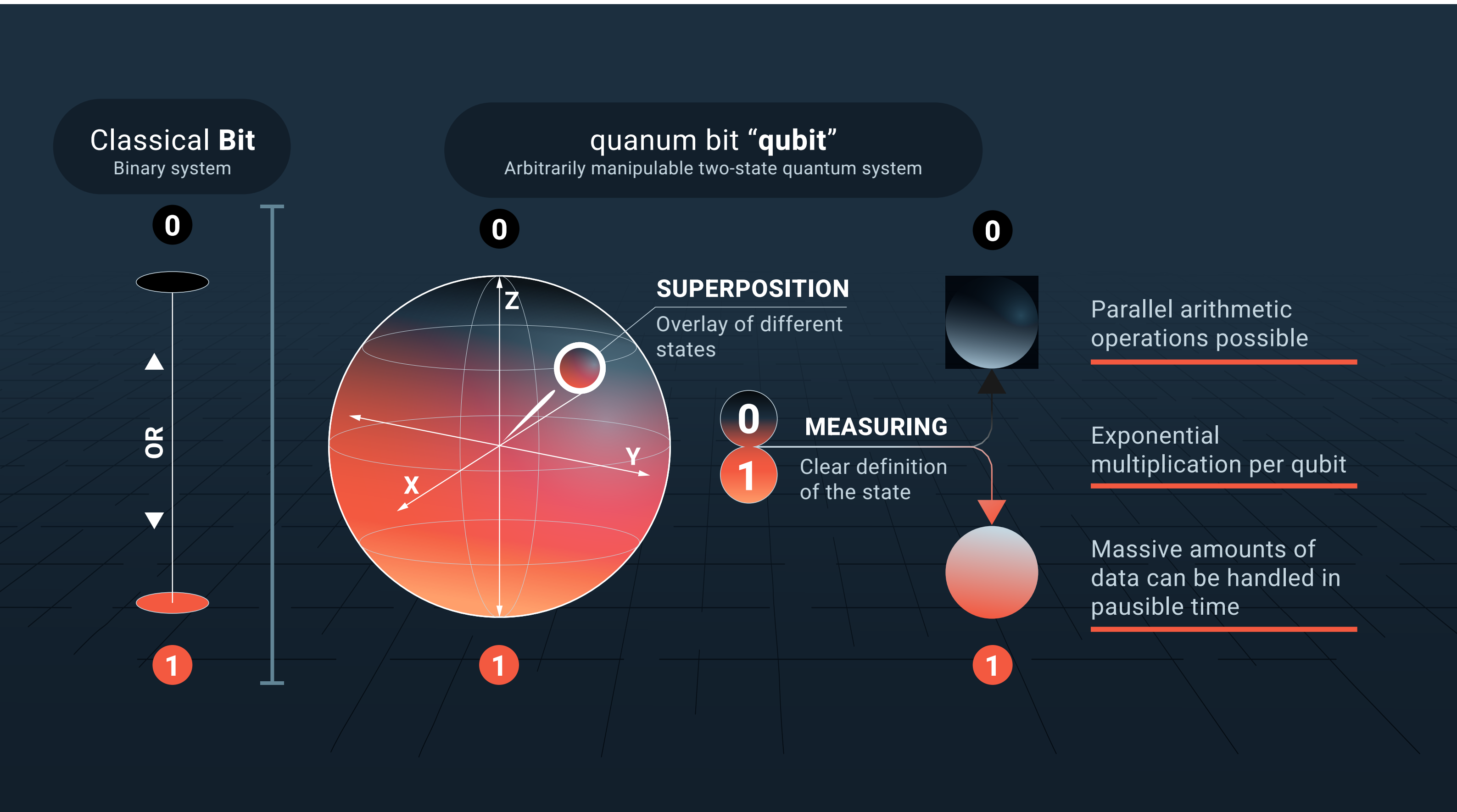
This article by Deloitte explains the threat quantum computers pose for the blockchain in great detail. The authors speculate that about 4 million Bitcoin, currently worth $40 billion, are vulnerable to a quantum computer attack.

Want to learn more about quantum computers? This article from MIT Technology Review is a highly readable explainer. Quantum computers are especially promising when it comes to improving electric vehicles' performance and creating new drugs.

## THE METACO VIEW

> *"Wherever there's a threat, there's also an opportunity to innovate. The risks presented by quantum computing are a chance to devise ever more secure infrastructure which will strengthen cryptocurrencies and boost their legitimacy as an asset class."*

## CLASSIC COMPUTER VS QUANTUM COMPUTER


Classical **Bit**
Binary system
0
OR
1
quanum bit "**qubit**"
Arbitrarily manipulable two-state quantum system
0
Z
X
Y
1
SUPERPOSITION
Overlay of different states
0
1
MEASURING
Clear definition of the state
0
1
Parallel arithmetic operations possible
Exponential multiplication per qubit
Massive amounts of data can be handled in pausible time

# R is for RIPPLE

Ripple is an exchange platform with a decentralized ledger and its own cryptocurrency. The platform is called RippleNet, and the cryptocurrency is called XRP.

**RippleNet**

RippleNet is an open source, peer-to-peer network that allows users to exchange any type of value, whether it's cryptocurrency, fiat currency, or something else. So, the parties to a RippleNet transaction might exchange XRP for Bitcoin, Ether, or US Dollars, for instance. They could exchange British Pounds for Ripple's own cryptocurrency XRP. In theory, they could even exchange things like airline miles for currency or something else they consider valuable.

RippleNet makes these exchanges happen through a system of gateways.

Let's say Party A wants to offload some Bitcoin and acquire Canadian Dollars.

Party B has Canadian Dollars they want to sell and wants some Ether.

Party C has Ether and wants Bitcoin.

All three would submit their bids and offers on specific RippleNet gateways. RippleNet would then find the fastest, most cost-effective way to make the exchange happen so all three get what they want.

The network verifies the transactions, after which they're recorded on Ripple's ledger. But unlike other decentralized platforms, RippleNet doesn't use proof of work or proof of stake for verification. Instead, the platform uses a network of independent nodes. These nodes constantly compare transaction data among each other until they all agree on the current state of the ledger.

**XRP**

XRP, Ripple's cryptocurrency, represents the transfers of value that take place on RippleNet. Think of it as a bridge between one unit of value and another.

Let's go back to the previous example.
C wants A's Bitcoin. But they have Ether while A wants Canadian Dollars, so they can't transact directly with each other. Similarly, B can't transact directly with A or C.

In a traditional scenario, it simply isn't possible for such an exchange to happen. But RippleNet gets around this by converting A's Bitcoin, B's Canadian Dollars, and C's Ether to XRP.  When the XRP reaches the other party, it's converted back into the unit of value that party wants. So, Canadian Dollars for A, Ether for B, and Bitcoin for C.

RippleNet gateways are typically owned by banks who guarantee the exchange. So, in a way, XRP works like IOUs or promissory notes.

## SOME FACTS

- Ripple was launched as OpenCoin in 2013 by programmer Jed McCaleb and angel investor Chris Larsen, who is considered the richest man in cryptocurrency. But the protocol dates back to 2004, when Ryan Fugger created the prototype for a decentralized digital monetary system he called RipplePay.
- Because Ripple doesn't use proof of work or proof of stake, no mining takes place. XRP is pre-mined: Ripple owns it and controls how many coins are in circulation, which means Ripple effectively acts as a central authority.
- Ripple has recently made headlines for all the wrong reasons. The US's Securities and Exchange Commission has sued the company, Chris Larsen, and current CEO Bradley Garlinghouse, arguing that because of the way it works, issuing XRP amounts to an unregistered and, so, illegal securities offering. As a result of the lawsuit, XRP was delisted from Coinbase and several other exchanges and plunged in value.

## WANT TO KNOW MORE?

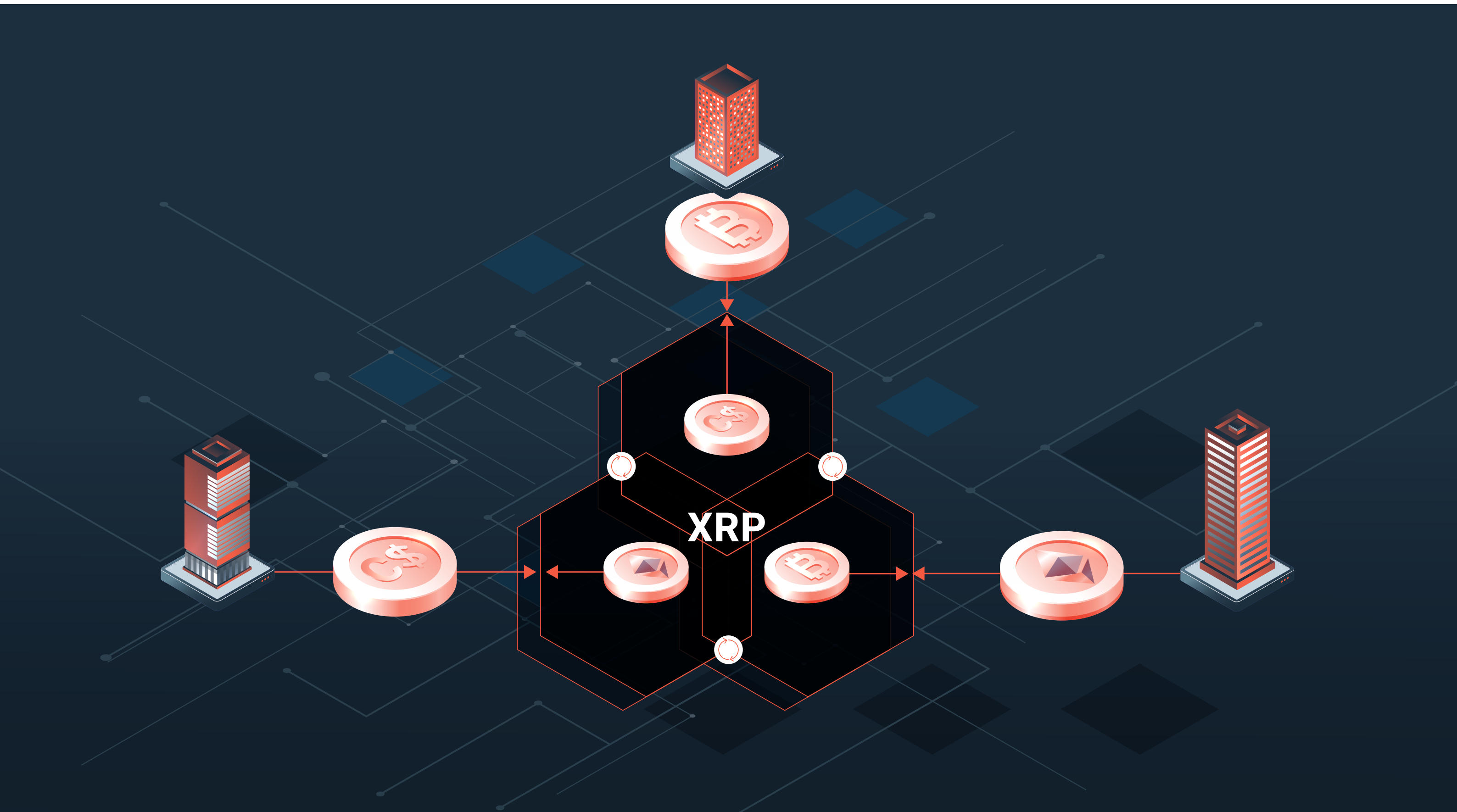
The Securities and Exchange Commission has published their full complaint against Ripple here. Interestingly, their central argument is that XRP isn't a currency, but an asset that compensates the holder for assuming a risk.

Legal Briefs analyse the issues in more depth and speculate on the lawsuit's likely outcome in this YouTube video.

## THE METACO VIEW

> *"The SEC's lawsuit may be bad news for Ripple, but it shines a spotlight on just how far crypto assets have come. If this had happened a few years back, the whole market would have probably crashed. But the total market cap has continued rising — a clear sign the market is maturing."*

## ANATOMY OF A RIPPLENET TRANSACTION



# S is for **STABLECOIN**

Stablecoins are asset-backed cryptocurrencies. By linking their value to a more stable asset, stablecoins aim to avoid fluctuating as much or as often as traditional cryptocurrencies like Bitcoin.

The most popular stablecoins — Tether and USD Coin — are both pegged to the US Dollar at 1:1. This means that 1 Tether Coin and 1 USD Coin are both worth $1. Alternatively, some stablecoins are tied to a commodity like gold or silver. In either case, a ‘reserve’ of the asset that backs the cryptocurrency has to be deposited with a traditional bank in an amount proportionate to the number of tokens in circulation. So if a stablecoin is pegged 1:1 to the US Dollar and there are 10,000 coins in circulation, the reserve must be $10,000.

This reserve acts as collateral. So, in theory, you could exchange one unit of a stablecoin for one unit of the asset that backs it. Less commonly, stablecoins are backed by one or more other cryptocurrencies or by an algorithm. Here, the process happens entirely on-chain. Let’s say you want to buy stablecoin that is backed by Ether. To get the stablecoin, you’d tie a predetermined amount of Ether to a smart contract. This would then release the stablecoin.

Many crypto-backed stablecoins are over-collateralised. The excess collateral acts as a buffer in case the cryptocurrency that backs the stablecoin falls in value.

By contrast, algorithmic stablecoins aren’t collateralised. Instead, they simply track another asset. When the asset goes down in value, the algorithm decreases the number of coins in circulation. Conversely, when the asset’s value goes up, the number of coins in circulation increases.

## SOME FACTS

- BitUSD, the first stablecoin ever created, was launched in 2014 by former Ethereum Foundation CEO Charles Hoskinson and father-son duo Stan Larimer and Daniel Larimer. But the idea dates back to 2012, when JR Willett came up with the idea for Mastercoin, an open source protocol that aimed to remedy Bitcoin’s volatility and illiquidity.
- Mastercoin, which was rebranded as Omni in 2015, was one of the first platforms to allow ICOs and ITOs. Tether, the biggest stablecoin by market cap, is built on the Omni protocol.
- While stablecoins are theoretically less volatile than traditional cryptocurrencies, counterparty risk is a serious problem. Many issuers aren’t transparent about where they hold their reserves. And Tether has refused to allow a full audit.

## WANT TO KNOW MORE?

Despite its popularity, Tether is hugely controversial. According to this study, at the height of the 2017 cryptocurrency boom it manipulated the price of Bitcoin and other cryptocurrencies. Several multimillion dollar class-action lawsuits have been filed against Tether and cryptocurrency exchange Bitfinex on the basis of these findings.

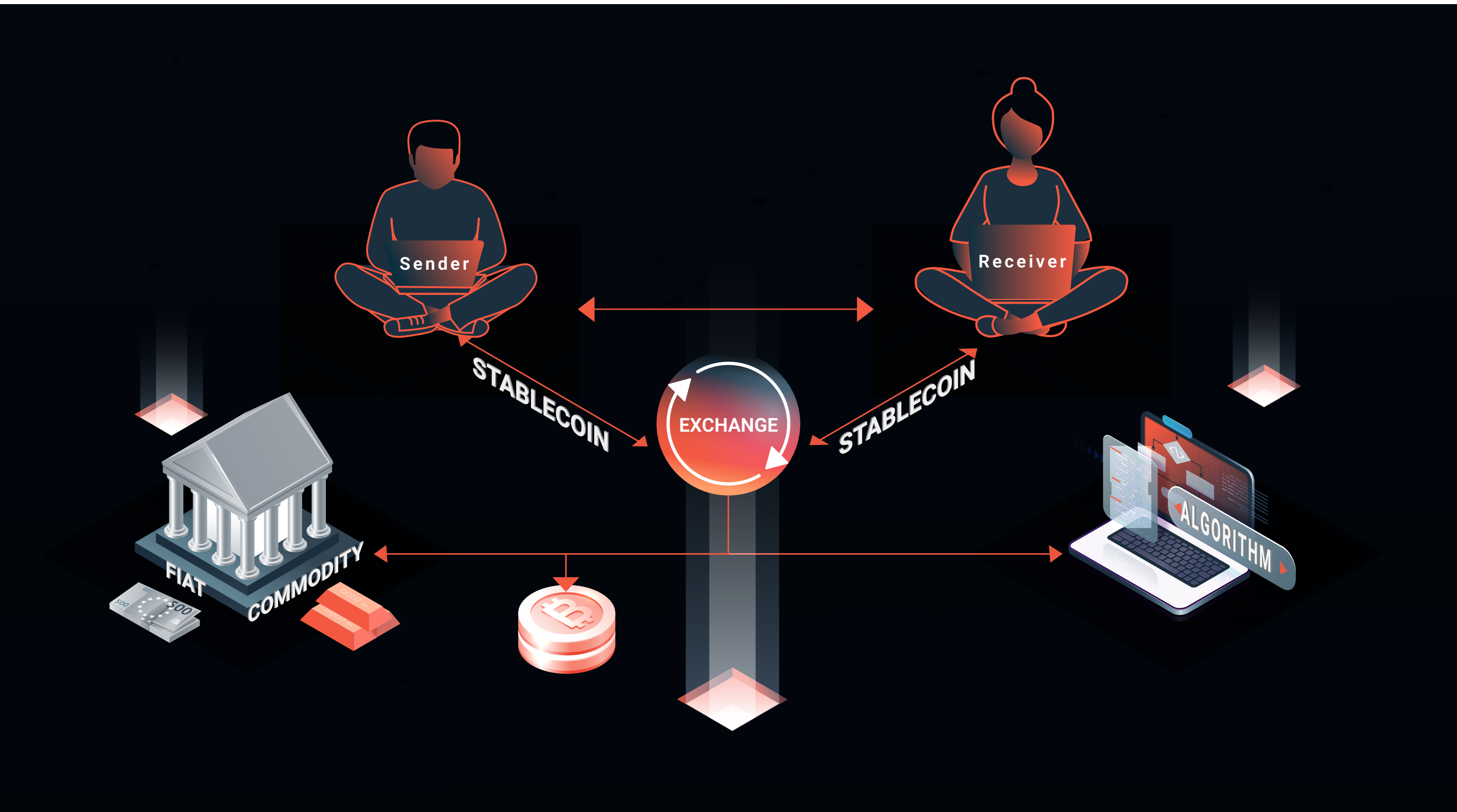
Speaking of manipulating prices, the Mastercoin white paper — which author JK Willets ambitiously called “The Second Bitcoin White Paper” — was remarkably prescient about the risk of market abuse.

Unfortunately, it falls short of suggesting mechanisms to prevent this. The white paper’s Appendix A, aptly headlined “Horrible, Awful, Very Bad Things” simply notes that: “*...it should be clear by now that MasterCoins can be used for some very bad things. Anyone working on an implementation of the MasterCoin protocol should be very careful to warn users to not break the law of their country of residence. It is up to the user to know the laws of their country...*”

## THE METACO VIEW

> *“It’s neither helpful nor desirable to see cryptocurrencies and traditional currencies as being in competition with — and trying to eradicate — each other. The market will be much more resilient if the two co-exist and complement each other. In this respect, stablecoins are very much a bridge to the future...”*

## STABLECOINS EXPLAINED



# T is for TOKEN

A cryptographic token is a digital unit of value that lives on the blockchain. There are four main types:

| Payment tokens | Utility tokens | Security tokens | Non-fungible tokens |
|---|---|---|---|

### Payment tokens

Payment tokens are coins. Their main purpose is to serve as a medium of exchange, store of value, and unit of account. Major cryptocurrencies like Bitcoin and Litecoin are payment tokens. Like fiat currencies, payment tokens gain or lose value based on the laws of supply and demand. Greater demand and lower supply increase value, while lower demand and greater supply decrease value. The twist is that some cryptocurrencies have a finite supply. Only 21 million Bitcoin can ever be mined, for instance. This means that, as more people start paying for goods and services with cryptocurrencies and the supply of new coins dwindles, their value should rise sharply, at least in theory.

### Utility tokens

These are tokens that give the holder access to a blockchain-based product or service.
For example, you can use Ether to access dapps or to pay for smart contracts to be executed on the Ethereum blockchain. Similarly, Gas coins give you access to the NEO network.

### Security tokens

Security tokens are traditional assets like stocks and shares that have been converted into a digital token on the blockchain. Like traditional securities, security tokens give the holder ownership rights. For this reason, a growing number of regulators are controlling how they're to be issued and traded. Most regulators determine whether a token is a security token using some version of the Howey test — a test developed by the US Supreme Court in a case brought by the Securities and Exchange Commission.

According to this test, a token is a security token if it meets three criteria:

- The holder has received the token in exchange for money that has been invested in a common enterprise
- They expect to make a profit
- They won't do any of the work required to generate that profit

### Non-fungible tokens

A non-fungible token is a digital representation of something unique. Each token represents a specific asset, so there's no standard value. This means you can't exchange one non-fungible token for the other directly.

That said, because data that lives on the blockchain can't be duplicated or altered, non-fungible tokens are ideal for proving ownership rights, identity, and authenticity.

## SOME FACTS

- Rock band Kings of Leon recently announced they'll be releasing their new album as a non-fungible token. They'll issue an Initial Token Offering that'll last for two weeks, after which no more tokens will ever be issued.
  Each token will cost $50 and will entitle the holder to a vinyl and digital download. There will also be "golden tokens" that'll grant the holders front-row seats to all the band's concerts for life.
- While Ether was primarily designed to be a utility token, it's also a payment token. A growing number of merchants and service providers accept payment in Ether.
  Unlike Bitcoin, Ether doesn't have a lifetime supply limit. But it does have an annual cap — only 18 million coins can be mined in a single year.
- Bitcoin is very close to hitting its lifetime cap. As of February 2021, around 18.5 million Bitcoin have been mined, which means there are only 2.5 million Bitcoin left.
  Nobody is sure what will happen when the limit is reached. In theory, the supply of Bitcoin will have been exhausted. But some members of the Bitcoin community believe the protocol should be changed to allow for a larger supply.

## WANT TO KNOW MORE?

Matt Luongo was the first person to float the idea of raising Bitcoin's supply cap. This Twitter thread explains his reasoning and shows just how controversial that proposal turned out to be.
What determines the value of a cryptocurrency? This Cointelegraph article explains the main drivers in clear, straightforward language.

## THE METACO VIEW

> *"Digital tokens have huge implications for the democratisation of finance. Not only is the blockchain more transparent and efficient, but fractionalising ownership broadens access to financial instruments to a wider swathe of customers, which in turn boosts their liquidity."*

## ANATOMY OF A RIPPLENET TRANSACTION

PAYMENT TOKENS
UTILITY TOKENS
SECURITY TOKENS
NON-FUNGIBLE TOKENS
Service A
Goods
Goods
Service B
*****

# U is for **UTILITY TOKEN**

Utility tokens are one of four types of cryptographic tokens that represent digital units of value on the blockchain. It's helpful to think of them as coupons or vouchers. The asset a utility token represents is a certain level of access to a product or service which the holder can gain by redeeming it.

For example, you can exchange filecoins for access to Filecoin's decentralized digital storage capabilities. Similarly, you can exchange Ether for access to dapps or to execute smart contracts on the Ethereum blockchain.

Some utility tokens also work like reward points. Brave browser users, for instance, can earn Basic Attention Tokens (BATs) by viewing targeted ads. They can exchange these BATs for premium services on the Brave network.

Utility tokens are often used in initial offerings. Investors get preferential access to products or services in exchange for helping to fund blockchain-based projects. But because they don't fit the traditional definition of an investment, they're largely unregulated. And this makes them prone to being exploited by scammers and fraudsters.

Tell-tale signs that an initial offering might be a scam include:

- The developers are anonymous
- Claims that a high profile crypto figure — typically Ethereum's founder Vitalik Buterin — is involved
- The main sources of publicity are bounty posts or threads — these are posts or threads asking people to spread positive information about the initial offering in exchange for a reward
- Few or vague project details

## SOME FACTS

- Utility tokens are the most common type of cryptographic token, mainly because most of the initial offerings that took place during the initial offering boom of 2017 used utility tokens. Sadly, 46% of projects that made initial offerings in 2017 either didn't meet their funding targets or didn't gain traction, so the utility tokens they issued became essentially valueless. It's estimated that a further 13% of projects that launched initial offerings in 2017 have now 'semi-failed'.
- ERC-20, which lives on the Ethereum network, is by far the most popular standard for creating utility tokens. As of December 2020, there were 829 projects based on it.
- Because utility tokens give the holder access to a product or service, their value is tied to that product or service's popularity. This is known as 'token utility'.
- If more people want to use the product or service, demand for the utility tokens that grant access to that product or service increases. In turn, this makes the utility token more valuable. The opposite is also true. If users lose interest in the product or service, the value of the utility tokens decreases.

## WANT TO KNOW MORE?

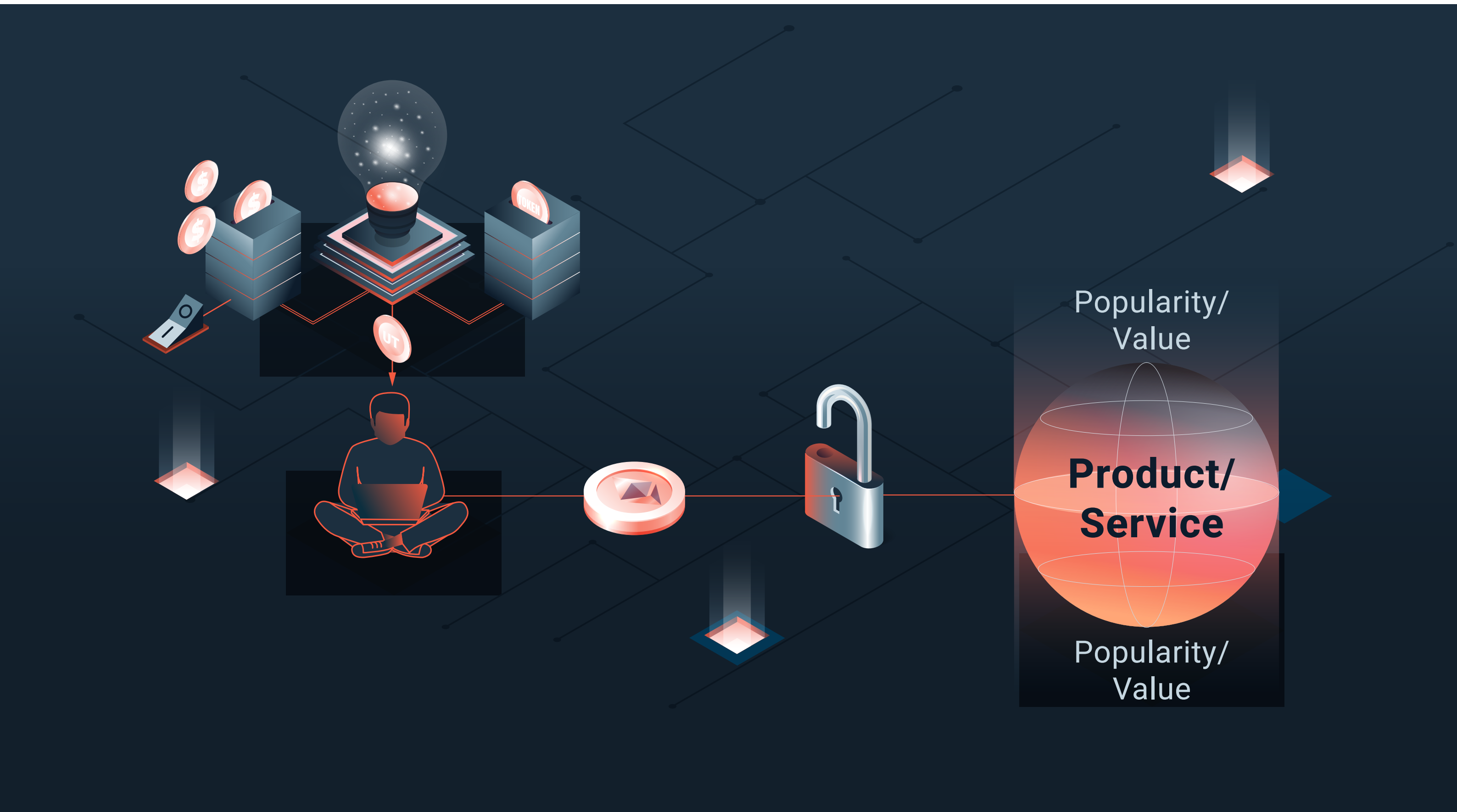
This article by solicitors Michael Jünemann and Johannes Wirtz discusses the legal classification of utility tokens. Interestingly, they argue that, while utility tokens can't be considered investments, the fact that they can be redeemed for goods or services means they should be subject to consumer protection law.

Brave Browser ran one of the most successful initial offerings of 2017, raising $35 million in 30 seconds. The Basic Attention Token white paper explains their vision to fix the issues inherent in the current digital advertising model, including privacy issues, middlemen, and slowdowns caused by cookies, pixels, and other types of internet trackers.

## THE METACO VIEW

> *"While it's true that many utility tokens are tied to speculative projects, they also have many exciting practical applications. When you boil it down, a token is a string of code. So any token can be hardwired with sophisticated logic that could transform many aspects of our everyday lives for the better — from enhanced security and privacy to democratising access to highly sought after but scarce resources."*

## THE UTILITY TOKEN'S LIFECYCLE



# V is for VOLATILITY

Volatility is the degree to which an asset fluctuates in value. If an asset is highly volatile, it can be prone to sudden, extreme price fluctuations.

At the other end of the spectrum, the value of an asset with low volatility remains relatively stable. Its price increases or decreases steadily and only within a fairly defined range. Sudden, extreme movements are rare. Cryptocurrency markets are notoriously volatile, with prices skyrocketing and crashing at a moment's notice. For instance, Bitcoin was worth over $20,000 at the end of 2017, only for its value to drop by 65% between January and February 2018. As in other markets, volatility in cryptocurrencies is largely influenced by the laws of supply and demand, which in turn are shaped by real world events. Certain events — or even rumours or speculation — drive up demand. And high demand increases value, especially if there isn't enough supply to meet it.

The opposite is also true. If something happens that makes cryptocurrencies seem less desirable, more people will want to sell off their holdings and less people will want to buy. And if supply is high and demand is low, value will go down. In cryptocurrencies, the effect of supply and demand is amplified — and, so, volatility is higher than it is in traditional assets — for three main reasons:

**The value of cryptocurrencies is highly dependent on 'network effects'**
At the risk of stating the obvious, the success or failure of a cryptocurrency depends on how many people are willing to use it. If more people pay for their purchases in a cryptocurrency — and more merchants are willing to accept it as payment — its value will increase. But if a cryptocurrency doesn't generate interest, it's essentially valueless.

Use of cryptocurrencies is becoming more widespread, but we're still a long way away from reaching critical mass. As a result, a fair amount of cryptocurrencies' value is speculative, which makes them more prone to rumour-based price fluctuations.

**They're still relatively new**
While there's growing evidence that the market is maturing, it's still early days. It's only recently that institutional investors have started looking at cryptocurrencies as a legitimate asset class with the potential for steady returns. The lack of a strong network of institutional investors also makes the market illiquid. And lack of liquidity tends to worsen volatility, because it takes longer for investors to offload their holdings.

**The average investor profile**
Cryptocurrency investments have low barriers to entry — anyone with an internet connection and some cash to spare can open a wallet and start trading. Meanwhile, institutional investors have historically been wary of buying crypto-assets.

The upshot is that the average cryptocurrency investor is fairly inexperienced. And this means they can panic in situations where professional investors would hold their nerve.

## SOME FACTS

- Bitcoin suffered its biggest ever decline in September 2018, when it lost 80% of its value. The event is known as The Great Crypto Crash of 2018. In comparison, when the Dot-Com bubble burst in 2002, the decline was a slightly lower 78%.
- Since 2018, cryptocurrencies have turned a corner. Bitcoin in particular has been the stablest it's ever been, with its value staying mostly between $9,000 and $10,000 in the first part of 2020 (though it did drop 39% in March, when the first wave of Covid-19 lockdowns hit).
- Institutional investment in cryptocurrencies has also started gaining traction. At the end of 2020, long Bitcoin — where investors bet on Bitcoin's value going up — was the third "most crowded trade", ahead of traditional positions like long gold and long corporate bonds.

## WANT TO KNOW MORE?

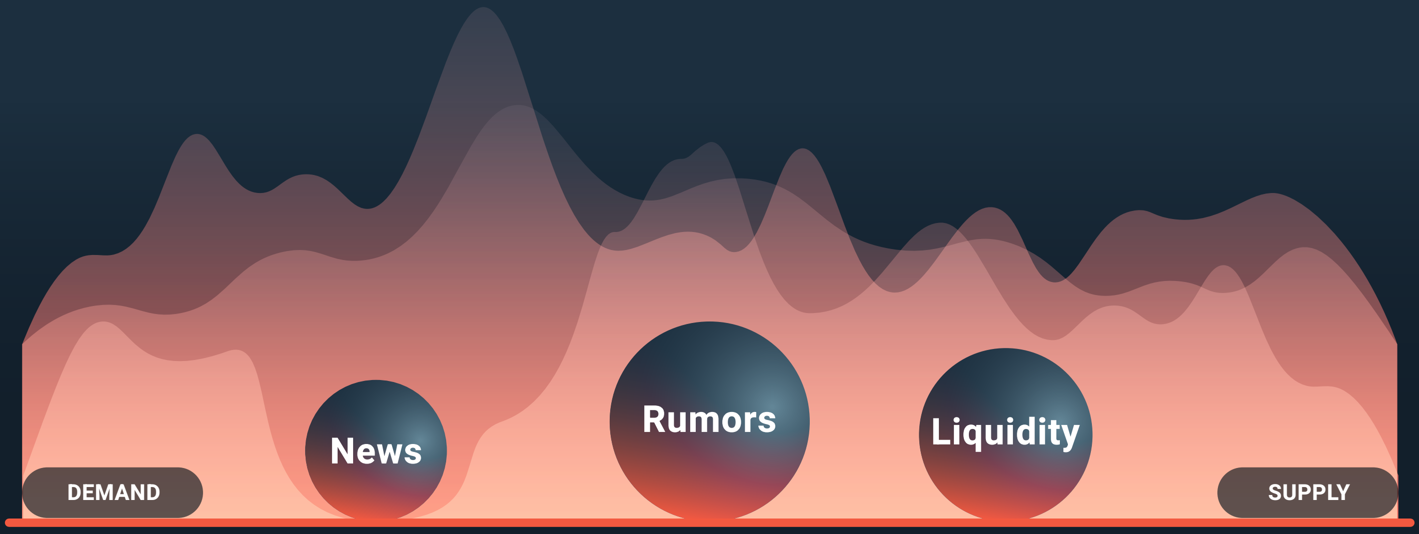
This article is a deep dive into the issues that make Bitcoin — and cryptocurrencies more generally — such a volatile asset class.

The Covid-19 pandemic has been a litmus test for cryptocurrencies, particularly when it comes to their value as alternative 'safe haven assets'. This article discusses how this unprecedented event took Bitcoin from being "*a fringe investment, disparaged by the likes of billionaire investor Warren Buffett...*" to being *"...the centre of conversations among big investors and Wall Street firms."*

## THE METACO VIEW

> *"Bubbles are an essential stage in any market's development, because they generate the funds needed for the next, more productive stage. As the market matures and attracts more institutional investors, the value of crypto-assets will stabilise and the focus can finally shift to the exciting possibilities these new assets can unlock — specifically a more democratic, accessible, and transparent financial system."*

## CRYPTO VOLATILITY EXPLAINED



# W is for WALLET

A wallet is a system that allows you to send, receive, and store cryptocurrency. Technically, because cryptocurrencies are completely digital and live on the blockchain, you can't own the coins themselves. What you own are the private keys that grant access to them — secret numbers that point to the digital addresses of the coins they correspond to.

Wallets keep your private keys safe, while also facilitating cryptocurrency transactions, whether it's paying for goods or services or speculative trading. They can be digital or physical.

There are three main types of cryptocurrency wallet:

**Hot wallets**
These are apps that store your private keys in the cloud, such as Coinbase Wallet.
Because they're always connected to the internet, it's quick and easy to access your keys when you need them. But that convenience comes at a cost: hot wallets are more vulnerable to attacks by cybercriminals. It's helpful to think of hot wallets as the digital equivalent of the physical wallet you carry around with you. Chances are, you use it to store your debit card, your credit card, and maybe some cash for day-to-day purchases. But you wouldn't keep all your life savings in it. You'd store those somewhere safer, like a special savings account.

The same goes for hot wallets. While you might want to store some private keys in a hot wallet for practical reasons, it should only ever be a small portion of your overall holdings. You should store the bulk of your holdings more securely.

**Cold wallets**
If a hot wallet is like the wallet you carry around with you so you can pay for your day-to-day purchases, a cold wallet is like a savings account that doesn't have a debit card. Or a bulletproof safe in a bunker built of reinforced concrete.Cold wallets are always offline, so they can't be hacked. The flipside is that they're not practical. Where a hot wallet lets you transact instantly, with a cold wallet you'll need to transfer your private keys to a wallet that can connect to the internet before you can use them. There's also the danger that you could lose or misplace your private keys.

A cold wallet can be as simple as a piece of paper on which you've written down your private keys. At the other end of the spectrum, there are specialised air-gapped servers — standalone servers that aren't connected to the internet or an unsecured network.

**Warm wallets**
Warm wallets are half-way between hot and cold wallets. They can be connected to the internet, but only when you need them. The rest of the time, your private keys are stored offline. Typically, you'll also need a password, a code, or some other form of authentication to access it.

Warm wallets are very secure when they're offline. But they're at risk of getting attacked by cybercriminals when you're online.

## SOME FACTS

- Apple have a chequered history when it comes to hot wallets. In 2014, they banned all Bitcoin wallets from the App Store, only to reverse course a few months later. The issue reared its head again in 2016, when they banned Ether wallets, reportedly because they didn't consider Ether an 'approved' currency. More recently, in February 2021, a man named Phillipe Christodoulou accused Apple of 'enabling a scam' after he downloaded a fake hot wallet. The app was listed on the App Store as a companion app to Treznor, who manufacture cold wallets. Except Treznor don't make apps. And when Christodoulou realised his mistake, it was too late — he'd already transferred Bitcoin worth $600,000 to the scammers.
- The first cryptocurrency wallet was the Satoshi Client, which eventually became Bitcoin Core, software which allowed you to create your own wallet. But as Bitcoin started growing in popularity, larger exchanges popped up.
  One of these, Mt Gox, would go on to handle almost 70% of the Bitcoin in circulation. It went bust in 2014, after announcing $450 million worth of Bitcoin had disappeared from its servers. Ironically, their tagline was "Trade with confidence".
- Around 200,000 Bitcoin that Mt Gox lost have since been 'found'. It's still unclear how they went missing, but it's likely that most were stolen from MT Gox's hot wallets over several years.

## WANT TO KNOW MORE?

This video runs you through the basics of cryptocurrency wallets in 5 minutes. The "best cryptocurrency wallets" are a topic of much discussion... and list-type blog posts. This one from TechRadar has fairly comprehensive, unbiased reviews and a good mix of hot, warm, and cold wallets.

## THE METACO VIEW

> *"Hot and cold wallets have equally important roles in cryptocurrency transactions. We've built SILO with this in mind. As the first hot-to-cold asset management platform, SILO is designed to strike a seamless balance between liquidity and security."*

## THE UTILITY TOKEN'S LIFECYCLE

HOT
WARM
COLD

HOT

✗ Easy access
✗ 100% secure

WARM

✓ Easy access
✓ Can store offline
✗ 100% secure

COLD

✓ Offline
✓ 100% secure
✓ Hard to access
✗ Can be lost or replaced

# X is for **XBT**

XBT is an abbreviation for Bitcoin.

Historically, Bitcoin has been represented on exchanges by the abbreviation BTC. The main difference between XBT and BTC is that the former has been prescribed by ISO, the International Organization for Standardisation.

ISO prescribes the official three-letter codes that represent specific currencies and other assets. These are published in standard ISO 4217.

The vast majority of codes follow the same format.

For currencies, the first two letters are the official ISO country code, and the last letter is the first letter of the currency's name. So, in USD, for example, US stands for United States and D stands for Dollar. Similarly. in GBP, GB stands for Great Britain and P stands for Pound Sterling.

When it comes to assets that aren't connected to a country, and commodities such as gold and silver, ISO uses the letter X. In the case of gold and silver, X is followed by the official symbol for their chemical element. So the symbol for gold, for instance, is XAU — X followed by AU, which is the chemical symbol for gold.

Bitcoin, of course, isn't a chemical. So ISO followed the letter X with the first two letters of the currency: BT.

## SOME FACTS

- While most currency codes follow the same format, there are exceptions. The ISO code for the Euro, for instance, is EUR not EUE, because EUR rolls off the tongue more easily.
  Similarly, the code for the Russian Rouble is RUB, not RUR. This is because the current Russian Rouble has replaced the old Russian currency, which was also called the Rouble. ISO gave the new Rouble a new code to avoid confusion.
- There's more to an ISO-certified currency code than just the name. When ISO adopts a currency code, it enters the official database that clearing networks like SWIFT, Visa, and MasterCard rely on. This means Bitcoin is now a selectable clearing and settlement unit for any business that wants to accept it as a payment method.
- Even if ISO didn't have an official standard format for assets that aren't tied to a country, Bitcoin wouldn't have been able to keep the code BTC. This is because BT is the official country code for the Kingdom of Bhutan. The code for the Bhutanese currency, called the Ngultrum, is BTN.

## WANT TO KNOW MORE?

Go here for a comprehensive explanation of the ISO 4217 standard and how it works.

The abbreviation XBT has been in unofficial use for several years. But in this article from 2014, the Bitcoin Foundation's Jon Matonis argues that obtaining official recognition from ISO would be a crucial step towards mainstream adoption of Bitcoin.

## THE METACO VIEW

> *"Having a standard ISO code can only be a good thing for Bitcoin. It gives it legitimacy and reflects its status as an increasingly popular alternative to traditional currencies."*

## ISO 4217 CODES

| | | | |
|---|---|---|---|
| £ | 0.5117 | 0.5121 | 0.5611 |
| € | 0.6527 | 0.6531 | 0.7225 |
| NZD | 1.0623 | 1.0634 | 1.1498 |
| ¥ | 93.1470 | 93.4230 | 103.700 |

# Y is for YIELD FARMING

Yield farming allows cryptocurrency holders to earn rewards — typically other crypto tokens — in exchange for lending out their coins. It's helpful to think of yield farming as the crypto equivalent of investing in interest-bearing loans. But while the basic concept is the same — you lend your funds to somebody else and get paid a premium for it — there are two key differences.

Firstly, the process is completely trustless and permissionless.

The person who holds the coins, called a 'liquidity provider', locks up the coins in a smart contract, called a 'liquidity pool', that lives on a decentralized finance app.

The smart contract has a set of rules encoded into it. And both the coins and rewards are released automatically only when a series of mathematical calculations confirm that those rules have been met. There are no human gatekeepers to decide who can pay into a liquidity pool or who can borrow from it.

Secondly, while the size of the reward partly depends on how much the liquidity provider has paid — or staked — into the liquidity pool, the reward itself isn't necessarily interest. It can be a cut of the underlying fees the decentralized finance app charges to execute the smart contract. Or something else altogether. The reward is also not necessarily paid in the same cryptocurrency. It could be a utility token, or even a token that hasn't been released on the open market yet.

Liquidity pools — and yield farming in general — can get extremely complex. And the process can vary quite widely, depending on the type of smart contract and how its rules have been encoded.

Users can also diversify by investing their rewards into different liquidity pools that reward them with different tokens.

## SOME FACTS

- Yield farming exploded onto the crypto scene in June 2020 with the launch of COMPOUND, a protocol that makes it possible to lend and borrow crypto tokens. The protocol was an instant success, accumulating almost $6 billion worth of funding in under 2 months. So several copycat protocols quickly followed. Popular ones include MarketDAO, which lets users use crypto as collateral to borrow DAI, a USD-pegged stablecoin, and Uniswap, which also functions as a crypto exchange.
- Alongside interest and other rewards, most yield farming protocols distribute governance tokens to liquidity providers. These tokens can be traded on exchanges. They also give the holders a say in how the yield farming protocol is governed. For example, users who hold at least 1% of the total supply of COMP, COMPOUND's governance token, can vote on proposals to change the protocol
- The vast majority of yield farming protocols live on the Ethereum blockchain. But work is underway on technologies that could allow liquidity pools to run on any blockchain that supports smart contracts

## WANT TO KNOW MORE?

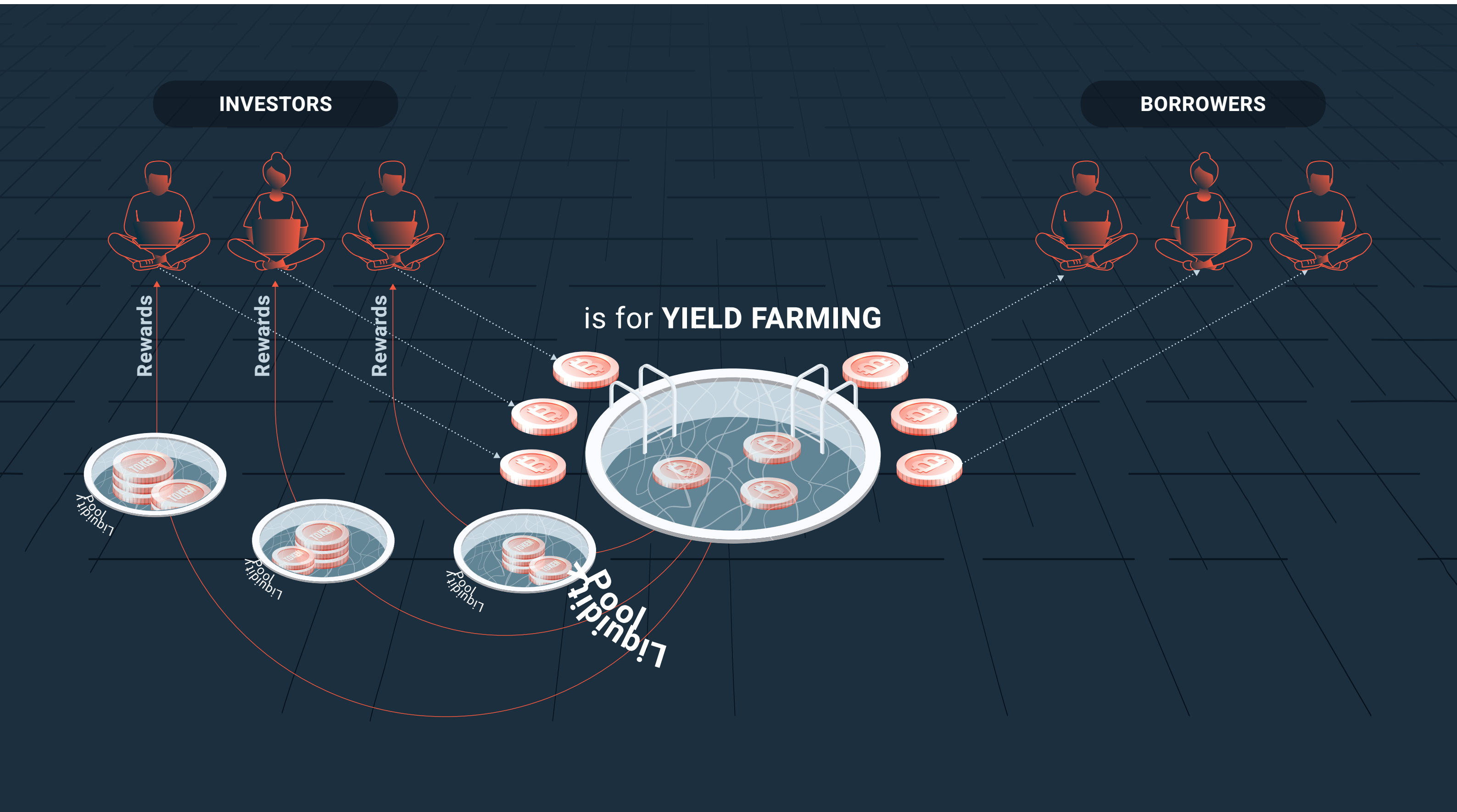
This white paper explains the rationale behind COMPOUND — the protocol that made yield farming possible. In particular, COMPOUND's creators Robert Leshner and Geoffrey Hayes argue that limited borrowing mechanisms and investment opportunities have contributed to volatility and crypto assets being wrongly priced.

The leading metric for quantifying the growth of yield farming is TVL — total value locked. This represents the total value of assets in a particular liquidity pool. But this article argues that, while growing TVL is a good sign, it can be misleading.

## THE METACO VIEW

> *"Yield farming is an exciting development. It's the proof of concept for a trustless, permissionless, and more democratic way to raise funding and unlock liquidity. And it makes it possible to generate passive income at significantly higher rates of return than you'd find on traditional markets.*
>
> *The flipside is that, at the moment, it's still highly complex and unpredictable. But as the market matures, the mechanism will become more efficient, which will in turn attract more users."*

## YIELD FARMING IN A NUTSHELL



# Z is for **ZERO KNOWLEDGE PROOF**

Zero knowledge proof, also known as a ZK protocol, is a verification method in which knowledge can be proven without its content being revealed.

There are two main parties to a ZK protocol: a prover and a verifier. The verifier authenticates the prover by asking it to perform tasks it can only do if it has the knowledge that is being verified.

Zero knowledge proof is especially useful in situations where privacy and security are critical, for example in authentication systems. Case in point, traditional banks use a similar approach when they ask you to verify your identity by giving them specific letters from a memorable word.

You never reveal the full word. But because you wouldn't be able to answer accurately without knowing it, fulfilling this request proves you have the knowledge and confirms your identity.

A ZK protocol needs to fulfill three requirements.

The first of these is completeness. In other words, the prover must demonstrate their knowledge to a high degree of accuracy.

The second is soundness. This means the verifier must be able to show it is highly probable that the prover knows the information.

Lastly, the knowledge isn't disclosed. The only thing the verifier will learn is that the prover's claim that they have the knowledge is true.

## SOME FACTS

- Shafi Goldwasser, Silvio Micali, and Charles Rackoff first developed zero knowledge proofs in 1985. But the concept was only applied to the blockchain for the first time in 2016.  Indeed, while Bitcoin is widely believed to be anonymous, all the information stored on the Bitcoin blockchain is publicly accessible. And Bitcoin transactions are easy to trace. In 2018, for example, the US Department of Justice busted a drug trafficking ring worth $12 million by tracking their Bitcoin transactions.
- The first blockchain to use a ZK protocol was Zcash, a cryptocurrency designed to facilitate anonymous digital payments. It was created in a 'ceremony' during which the first private key was split into six pieces — or 'shards' — that were subsequently destroyed together with the computers that created them. Unlike other privacy-focused cryptocurrencies, Zcash hasn't faced too much regulatory scrutiny, mainly because transactions can also be sent publicly. As a result, when it launched on the Gemini exchange in 2018, it did so with the full backing of the New York State Department of Financial Services.
- A network of developers have been looking at bringing privacy-focused smart contracts to the Ethereum blockchain. These smart contracts could be used to create private tokens and private decentralized organizations.

## WANT TO KNOW MORE?

Goldwasser, Micali, and Rackoff's paper — 'The Knowledge Complexity of Interactive Proof-Systems' — is particularly noteworthy for introducing the concept of 'knowledge complexity'. This measures how much knowledge about the proof is transferred from the prover to the verifier.

The project seeking to bring zero knowledge proof to the Ethereum blockchain is code-named Aztec. This article explains how the project works in detail, including the rationale for it and specific use cases.

## THE METACO VIEW

> *"Zero knowledge proof has the potential to be a huge step forward in blockchain technology. From fraud prevention to keeping sensitive personal information safe, there's a vast number of use cases where it could greatly enhance security and data privacy."*

## WHAT IS ZERO KNOWLEDGE PROOF?

PROVER
VERIFIER
***
???

# METACO

**USD5 bn**
Assets Managed by METACO clients

**20,000**
Transactions per day

**5**
Countries where our clients are regulated

Founded in 2015 and headquartered in Switzerland, METACO enables financial institutions to capitalize on the burgeoning digital asset economy. METACO's main product, called Harmonize, is an orchestration system for digital assets. From cryptocurrency custody and trading to tokenization, staking and smart contract management, the platform seamlessly connects institutions to the new world of decentralized finance.

METACO brings together a highly experienced team of software, security, finance and cryptography specialists with close links to the banking and academic sectors as well as to the fast-growing DeFi entrepreneurial ecosystem. The management team combines a unique experience in DLT, banking and consulting, with senior profiles coming from Accenture, Standard Chartered Bank, Santander Bank, JP Morgan, Bank of America Merrill Lynch, and Barclays.

standard chartered | BBVA | DBS | SYGNUM | avaloq | NORTHERN TRUST | Börse Stuttgart | SICPA

"In BBVA our purpose is to bring the age of opportunity to everyone, therefore it is important to offer our customers access to the new world of digital assets, creating value not only in how we exchange money, but any valuable asset or piece of information. Leveraging METACO's institutional-grade infrastructure for the custody and management of digital assets, BBVA now enables its clients in Switzerland to combine traditional financial assets with digital assets."

Javier Rubio
CLIENT SOLUTIONS DIRECTOR AT BBVA SWITZERLAND

# For financial and non-financial institutions of all sizes

Enterprise-ready suites with packaged digital asset use-cases.

### For banks and finserv providers

Integrate digital asset use cases into your business model, irrespective if you're a large retail, corporate, private bank or a fast-growing challenger bank.

### For custodians and infra providers

Use your traditional custody expertise to provide an infrastructure enabling institutions worldwide to operate in the emerging digital asset space.

### For exchanges, brokers and OTCs

Expand into trading and secure custody of digital assets, including all the main cryptocurrencies and DeFi tokens.

### For asset managers

Get exposure to new asset classes and diversify custody risks across a network of trusted custodians in all major jurisdictions.

### For corporates

Adopt crypto as part of your treasury strategy. Issue and manage equities, bonds, derivatives and other asset tokens.

### For qualified investors

Transform unbankable assets into liquid tokens, unlocking capital while re-directing it towards alpha generating investments.

## Find out how other leading institutions are using METACO to safely enter the digital asset space.

To access a demo of our platform or to discuss with our digital asset experts, simply fill out this form or contact us at info@metaco.com

**METACO SA**
Avenue de Tivoli 2, 1007 Lausanne, Switzerland

www.metaco.com