Crypto, Parts 1 and 2

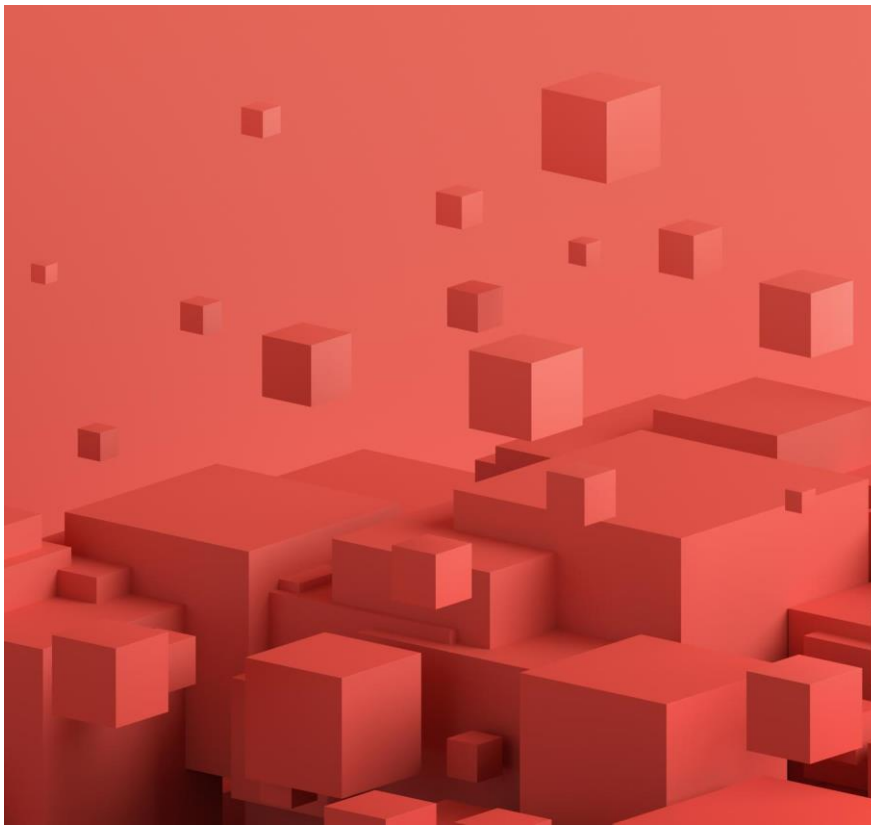
Charles Kerrigan

CRYPTO, PART 1

- How did this start?
- Before Bitcoin (BB)
- The genesis of Crypto
- The Bitcoin Whitepaper
- What was different about bitcoin?
- Bitcoin
- After Bitcoin (AB)
- The kaleidoscope—why does everything in Crypto make no sense?
- Ethereum
- Smart contracts
- What followed Ethereum—technical
- The price of bitcoin
- Social and political points
- Fun for lawyers
- International issues
- Finally…

CRYPTO, PART 2

- The same things, with more technical explanation



Published in association with Sweet & Maxwell, a Thomson Reuters business.

Sweet & Maxwell is the publisher of *Crypto and Digital Assets Law and Regulation*, by Charles Kerrigan (2024, ISBN 9780414115101)

Charles Kerrigan is a Partner at CMS LLP, a Board Member of RAK DAO, and the author of publications including *Crypto and Digital Assets Law and Regulation*

Crypto, Part 1

Charles Kerrigan

Introduction

Hello. I'm a normal person, but I like Crypto. It's the most interesting thing I've found in many a long year. It's also my job. I'm a corporate finance lawyer who found that Crypto answered some of the intractable problems I used to deal with. In 2024 I published a legal textbook on Crypto.

People ask me how to start to understand Crypto. The textbook might be too much as a start so the publisher and I decided that a short explainer could be the way. This is it. It doesn't require you to have any background beyond curiosity. You don't need to have any strong opinion about Crypto, either before or after reading.

If Crypto is a city, this is a transcript of what one of the guides of one of the bus tours might say. All aboard!

How did this start?

Once we got the Internet, Bitcoin was inevitable.

Let us start at the beginning. In the beginning people created the computer. This was the first time that we could store and manipulate information in digital form. To create the computer people had to solve a series of engineering problems. Once there was one computer it did not want to be alone. Once there was more than one computer, people wanted to solve the problem of how to transfer information between them. This connection is a network. At scale, it is what we now know as the internet. Once that was done, people investigated the problem of how to transfer value between computers. Can something like money move directly between computers on a network? Yes! … Bitcoin.

Like the first computer, Bitcoin was the result of combining the solutions to a series of engineering and maths problems.

Let us clear up how transferring value between computers is different to online banking. When you use your banking app to send money to your friend, you are not sending money to your friend. You are sending a message to your bank to determine your account balance (a record of a chose in action owed by your bank to you, as an unsecured creditor of the bank's legal entity that holds accounts), then initiate the transfer by checking your friend's account details at their bank, then send a message through the Faster Payments system to your friend's bank, then both banks to run their transaction monitoring steps to make sure you are not money launderers, then your friend's bank to verify the transaction, then your bank to debit the funds from your account and your friend's bank to credit the funds to their account (a record of a chose in action owed by your friend's bank to them, as an unsecured creditor of the bank's legal entity that holds accounts).

Transfer of value, aside from crypto (and cash, on which more below), involves intermediaries. This is where we get the concepts of centralisation and decentralisation from. The financial system is a centralised system. Crypto enables decentralised finance (finance without intermediaries).

The example above is the simplest example that can be given—no international transfers, no foreign exchange, no overdraft, no mistakes in any of the information, no IT or other failure at either bank.

The story of Crypto is not really the story of an eccentric pastime and haven for criminals. It is the story of a series of technical innovations, each building on the last, relating to secure messaging and the ways in which communities influence how commerce and law develops. This is our story.

Before Bitcoin (BB)

The concept of digital money goes back to the 1980s when cryptographers and computer scientists began to explore the possibilities of creating secure and private digital currencies. David Chaum's DigiCash aimed to provide a secure and anonymous digital payment system. It used public and private key cryptography and was based on digital signatures, both elements that were further developed in Bitcoin. Commercially it was ahead of its time and failed to gain widespread adoption due to regulatory challenges and limited user interest. But this starts to give us the nature of the technical challenge.

In the 1990s, the cypherpunk movement emerged, advocating for the use of cryptography to enhance privacy and individual freedom. Visionaries introduced groundbreaking concepts such as Wei Dai's Bmoney: a proposal for an anonymous, distributed electronic cash system, and Nick Szabo's Bit Gold: a proposal for a decentralized digital currency. Both were proposed in 1998. Neither got beyond the concept stage, but they laid the groundwork for Bitcoin by introducing key principles like decentralised consensus and proof-of-work. A significant early project that did launch was Hashcash, created by Adam Black in 1997. It established a technical way that computational effort could be required to send email messages (and thereby do away with spam emails by making them uneconomic).

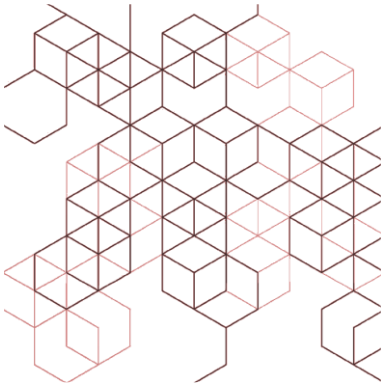
The genesis of Crypto

The Bitcoin network officially launched on January 3, 2009, with the mining of the first block (known as the "genesis block"). The first Bitcoin transaction occurred on 12 January 2009, when Satoshi Nakamoto sent 10 bitcoins to Hal Finney, a famous cryptographer. Satoshi Nakamoto is a pseudonym, a made-up name, not the name of a person. It is famously untranslatable but is made up of words meaning smart-friends-beginning (the words can have other meanings and this is my choice, rather than anything formally adopted).

The breakdown:

- the person (or entity, since references are to "we") responsible for Bitcoin did not want to claim public credit for it;
- its origin contains games and puzzles;
- it implicitly links itself with non-western culture (although all early messages are written in flawless American English);
- it has a "creator" and the creator has a meaning; that meaning is designed to be elusive but relates to doing cool new things with a group.

One of the themes of this chapter, because it is one of the themes of Crypto, is that it is kaleidoscopic. Depending on your prejudices and context and perspective, you will see different things. This can make it seem a difficult topic—but really it makes it fun. You need to understand that aspect of it and orient yourself each time you approach it and be comfortable that some things that can seem inconsistent can be true at the same time. I will point out this theme as we go.



The Bitcoin Whitepaper

The Bitcoin whitepaper is the most famous document in Crypto. It was published on 31 October 2008. It is a short, accessible document, just nine pages long and containing only a couple of mathematical formulae, right at the back. (A whitepaper is a customary name for a policy document that aims to foster consensus on a topic by setting out problems and potential solutions.)

> This email, signed "Satoshi Nakamoto", was sent to a cryptographer's mailing list:
>
> "I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party. A purely peer-to-peer version of electronic cash would allow online payments to be sent from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent doublespending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone."
>
> All the major elements of Bitcoin are contained in the first sentence. The email describes:
>
> a) a new product, which has a technical explanation: a decentralised digital currency; and a social explanation: enabling peer-to-peer transactions without the need for intermediaries like banks; and
> b) a new technology, which combined a ledger, with a shared network, with a cryptographic technique that linked groups (blocks) of transactions in a way that established they were verified and secure. This new technology is blockchain.

The whitepaper sets out in 10 sections (with an introduction and a conclusion) the elements of the new system:

- *Transactions*: transfer of value is achieved by verification using digital signatures.
- *Timestamp Server*: a distributed timestamp is used to generate proof of the chronological order of transactions.
- *Proof-of-Work*: a system that secures the network and prevents double-spending has been created, working on the basis that participating computers must simultaneously perform calculations to create new blocks and check the content of those blocks.

- *Network*: since the system is peer-to-peer, the broadcasting of transactions and the formation of blocks must be communicated via a network made up of participating computers.
- *Incentive*: since it costs money (i.e. the cost of the electricity running the participating computers that are needed to make the proof-of-work, ahem, work) the system is only economically rational if participants are rewarded (through the issuance of new bitcoins and transaction fees) in an amount that is (on average, over time) greater than the cost of their electricity.
- *Reclaiming Disk Space*: the blockchain must be kept for so long as is needed to ensure its security but not so long that participating computers run out of storage; so the system shrinks information while it is useful and then discards when it is not.
- *Simplified Payment Verification*: relates to establishing reliable methods for verifying payments without needing to check the history of the blockchain.
- *Combining and Splitting Value*: is the process by which the system does not require payments to be in the same denomination as underlying currencies in which things are priced (i.e. to ensure that the system does not fail because you want to pay $1 to your friend but the system only works in minimums of the equivalent of $100).
- *Privacy*: describes the pseudonymous nature of the system in that payments are apparent on the network but the parties are not (making the contrast with traditional banking where parties are known but only to their banks).
- *Calculations*: some complex maths to show that it might just work.

The paper addressed some famous problems in cryptography. The Byzantine Generals Problem says that decentralised systems have an inherent problem. Some participants may act in their own interests rather than of the system as a whole, so they may send inaccurate messages.

The Byzantine Generals are imaginary generals camped round a city deciding whether to attack or retreat. They communicate via messengers. Any messenger or general may be unreliable.

The solution (expressed in non-technical terms, the actual solution is an algorithm) is a requirement for: (a) a test to establish what counts as agreement on the state of information in the system, in this case the group of generals—this is “consensus”; and (b) a rule for what counts as a sufficient number of generals being in agreement that a general (apologies, this pun is irresistible) agreement can be assumed with an acceptable level of safety—this is “fault tolerance”.

Linking all this back to our description of the original email, we can see that the whitepaper also describes:

a) a new product, electronic cash, with a built in incentive to make it viable without further investment (unlike a start-up company, which burns money until it makes a profit), and with a network secure enough to be trustworthy without the need to trust any particular person (unlike the banking system, which is susceptible to human frailty—it is not a coincidence that the whitepaper was published during the Global Financial Crisis and the Genesis Block embeds the text “The Times 03/Jan/2009 Chancellor on brink of second bailout for banks,” to avoid any doubt); and
b) a new technology, with our blockchain now being explained by refence to its operations and a mathematical proof that it would not be possible to game the system by doing enough “work” (in Proof-of-Work) to overwhelm the rest of the network and anticipating some of the theoretical and practical objections that would be raised in the minds of readers.

There were many objections, both at the time of publication and in the years since. The makers of Bitcoin were scientists who were experimenting by building on the work of the peers who had gone

before them and looking for rigorous testing by their peers in the cryptographers' mailing list. Bitcoin was never intended to be anything like your bank moving from signatures on cards to chip and PIN.

But maths and electricity created value. That was shocking and we are still trying to come to terms with it. There are famous YouTube videos of early users mining bitcoin on their PCs and seeing the value of their bitcoin pass $10 then $100. They are shocked and, of course, also delighted. But it was shocking.

To summarise, a blockchain is a database made up of a chain of blocks, each containing a list of transactions. These blocks are linked and secured using cryptographic techniques, ensuring the integrity and immutability of the data. Once a block is added to the chain, it cannot be altered. The decentralised nature of blockchain means that no single entity controls the network, making it resistant to censorship and fraud. There is no central point of failure that hackers can target. The transparency of blockchain allows all participants to view the entire transaction history, intended to create trust and accountability.

What was different about bitcoin?

If we compare bitcoin to its illustrious predecessor Hashcash we can get an idea of the developments. Hashcash was built to prevent email spam and denial-of-service attacks by making it computationally expensive to send mass emails. Bitcoin had far more expansive aims as we saw above. But we can see the development of certain technical features in comparing the two projects.

Both use a hashing algorithm. Hashcash used SHA-1. An email sender had to solve a computational puzzle (finding a hash with a certain number of leading zeros) to generate a stamp that proves they expended computational effort. Making an emails cost something (anything) is enough for Hashcash to achieve its aim. Bitcoin needed something much more challenging to be good enough security to power what is in effect internet money. It uses a double SHA-256 hashing algorithm, which involves hashing the data twice with SHA-256. At a basic level, it is a much harder algorithm to solve so it would take the same computer longer to do so. Both are Proof-of-Work systems. Hashcash generated proof-of-work stamps for individual emails or requests, but without a complex structure. Bitcoin used transaction history as a proof. Each block of transactions includes a reference to the previous block. This is what creates the secure and immutable chain—the blockchain.

Only Bitcoin uses incentives and mining. In Hashcash there are no built-in incentives for solving the proof-of-work puzzles other than the intended purpose (sending an email). Bitcoin incentivises users (especially early users, when bitcoins could be mined on a PC) with newly created bitcoins and transaction fees for validating and adding new blocks to the blockchain. Why else would someone use electricity that they have to pay for to operate a system that is by design computationally intensive?

Only Bitcoin uses network consensus. Hashcash has no need of it because it is used for individual proof-of-work tasks. Bitcoin uses a decentralised consensus mechanism where nodes in the network agree on the validity of transactions and the state of the blockchain through the proof-of-work process.

Bitcoin

You will see references to both Bitcoin and bitcoin. When used properly, the terms refer to different things: Bitcoin is the software and bitcoin is the currency.

What is most interesting is that Bitcoin is even more than two things. Some of them overlap and some of them are separate one from another. Bitcoin is a piece of software: it is an example of open

source software; it is a secure communications system; it is a decentralised software system; it is a currency; and it is an investible asset.

Time for a common sense break. Bitcoin brings together some elements that are not strange in the wider online world. In a digital economy, money is information—most simply the information comprising the balance that your bank stores in its systems attributed to your account. Maintaining that accurately is an information problem. The transfer of money is just an example of secure messaging. If the message relating to the transfer of funds between your bank and your friend's bank is hacked or corrupted, your respective balances will not be accurately updated. Making the message secure and accurate is an information problem.

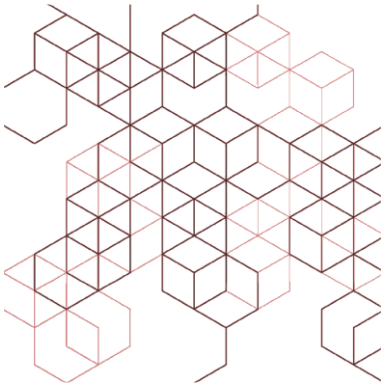
Rather than asking how bitcoin is like money, we can ask how money is like bitcoin. At the level of transactions, money is information. At the level of society, money is a social tool. We could go on, but the point is that, just like bitcoin, money is more than one thing.

At the fundamental level Crypto is concerned with the verification and transmission of information. Crypto asks (and answers) the question: can we prove that:

- I am me;
- you are you;
- the thing, say a bitcoin, is what we both think it is;
- we can be sure that if you transfer your coin to me and I pay for it, you no longer have it—this sounds trivial but it is fundamental—all electronic money projects are most concerned about the "double spend problem" referenced in the original Bitcoin e-mail.

If so, we can transact as safely as if we are exchanging central bank notes or using retail banks we trust. The amount of effort running behind the scenes in the traditional financial system to establish the same thing is enormous.

This is the next place where we stop to admire the kaleidoscope. When people talk about why Crypto is hard to understand, it is often not because of a technical difficulty, but because they are at cross-purposes talking about different aspects or characteristics of the topic. If you are discussing the benefits of bitcoin as electronic money with someone who is critiquing as aspect of the software, you will both be frustrated and won't get far.



After Bitcoin (AB)

Now we can talk about dumb money and smart money. Bitcoin delivered on its promise as a technical matter. It really did enable the transfer of value peer-to-peer, without a centralised intermediary. This is quite some technical achievement. But if all it could do is transfer value, it is dumb money. It is like cash. The next problem that people turned to was making money smart.

Ethereum is the answer to the question: if I can send a bitcoin *today*, why can I not also agree *today* to send a bitcoin *tomorrow*? In the first case, I can incur and satisfy an obligation in real time. In the second case, I can incur an obligation for satisfaction in the future. This is familiar to lawyers. It is the difference between executed and executory contracts. Contracts 101 is part of the history of Crypto.

Ethereum has since changed what is possible not just with digital money but also with digital accounts. Accounts themselves can now be programmed with smart contracts to improve the security, accessibility, and functions of the account.

The kaleidoscope—why does everything in Crypto make no sense?

The whitepaper only refers to "bitcoin" in its heading and its web address. It refers to cash or money more than 10 times. That suggests that the authors expected people to use it to pay for things. I said above that Bitcoin delivered on its technical promise. It is internet money. It still is. But it did not deliver on its social promise because people do not in fact use it to pay for things. So, we could say that it is a technical success but a social failure. Its failure, however, has come about because it increased so much in value. It seemed like a good idea to pay for pizzas when you mined it for the cost of some electricity. You are taking advantage of an electricity/pizza arbitrage. But, paying 10,000 BTC for a pizza when today's BTC price is over $70,000 … looks expensive.

Ethereum

While bitcoin was designed as a digital currency, Ethereum built on the logic of the technology to create:

- a decentralised platform that enables developers to create and deploy smart contracts—smart contracts are self-executing code, in other words terms of agreements are directly written into code and operate automatically;
- with its own (native) digital currency, Ether (ETH);
- used to power the network and pay for transaction fees
- all of which enabled decentralised applications (dApps) —digital services that could operate without intermediaries—which services could be combined to create wider financial ecosystems (if bitcoin is money without intermediaries, Ethereum is banking services and financial market infrastructure without intermediaries, hence, decentralised finance, DeFi).

The point was to create a more versatile and programmable blockchain platform. Showing how this work builds on the existing state of the art, the whitepaper begins:

> "When Satoshi Nakamoto first set the Bitcoin blockchain into motion in January 2009, he was simultaneously introducing two radical and untested concepts. The first is the 'bitcoin', a decentralized peer-to-peer online currency that maintains a value without any backing, intrinsic value or central issuer. So far, the 'bitcoin' as a currency unit has taken up the bulk of the public attention, both in terms of the political aspects of a currency without a central bank and its extreme upward and downward volatility in price. However, there is also another, equally important, part to Satoshi's grand experiment: the concept of a proof of work-based blockchain to allow for public agreement on the order of transactions. Bitcoin as an application can be described as a first-to-file system: if one entity has 50 BTC, and simultaneously sends the same 50 BTC to A and to B, only the transaction that gets confirmed first will process. There is no intrinsic way of determining from two transactions which came earlier, and for decades this stymied the development of decentralized digital currency. Satoshi's blockchain was the first credible decentralized solution. And now, attention is rapidly starting to shift toward this second

part of Bitcoin's technology, and how the blockchain concept can be used for more than just money."

The whitepaper is structured in four main parts:

History— discussing Bitcoin's blockchain technology and its limitations.

Ethereum—a more generalised blockchain platform, featuring:

- Accounts, of two types: one controlled by private keys and used for transactions, the other controlled by contract code and used for executing smart contracts.
- Messages and Transactions: describing the internal communications whereby smart contract code is executed (by messages) to transfer value and data (in a transaction)
- Ethereum State Transition Function: split into a record of the status of all accounts and their balances, and a record of how the state changes as blocks are added
- Code Execution in Ethereum: introducing the Ethereum Virtual Machine, an important (and still operating) system that executes contract code. Plus, the concept of "gas", the computational work (and therefore cost) to execute transactions.
- Blockchain and Mining: describing the structure of the Ethereum blockchain; and the consensus mechanism used to validate transactions and secure the network. (The consensus mechanism was originally proof-of-work, like bitcoin, but has since been changed to proof-of-stake).

Applications of Ethereum—how it was envisaged to be used in practice, in particular through the introduction of:

- Smart Contracts: which were identified as being able to be used for token systems, financial derivatives, identity systems, file storage systems etc;
- DApps: describing the potential if elements of the existing financial system could be replicated on a decentralised basis/

Miscellanea And Concerns—because, remember that at this stage everything was still experimental and challenge was welcomed in order to enable community-led improvements.

From this paper, the speed of technical development increased as we will see next.

Smart contracts

You may hear some rude people say that smart contracts are neither smart nor contracts. Do not listen to them. They are referring to the fact that the term was adopted by programmers without asking lawyers for permission.

The objection to "smart" is that the contracts follow predefined rules without the ability to adapt or interpret context. So, they are not smart like a person is smart. (You can read the previous sentence in your head in either a neutral or sarcastic voice depending on whether you are or are not an AI maximalist.)

The objection to "contracts" is that the term implies a legal agreement. Smart contracts automatically enforce the terms written into the code, but they do not inherently have legal recognition.

The term smart contracts is not a bad phrase in our context though. Compared to money, or bitcoin, smart contracts are smart. And, as the UK Law Commission wrote in its work on smart contracts, it is quite possible for a smart contract to have the legal characteristics of a contract (parties, intention to create legal relations, certainty, consideration) and therefore be enforceable as a contract in an English court. People making the distinction refer to smart contracts (all of them) and smart legal

contracts (the ones that ae legally enforceable, presumably in the jurisdiction they are in or know the rules of contracts in).

What followed Ethereum—technical

We have seen that Bitcoin was first a solution to an engineering problem—can we transfer value peer to peer using networked computers? Ethereum was a solution to another engineering problem—can we include terms in the transfer of value?

You are probably getting the idea by now. The story of developments from 2015 followed the identification of new problems and the release of new solutions. Let us listen in on the conversations …

> "The problem with blockchains is that you can't trust them because the whole thing is just a load of students or crooks hiding in their basement so you can't trust anything they're doing."

Cardano launched in 2017. It is known for a research-driven approach to blockchain development. Its research addressed what was known as the "blockchain trilemma": can blockchains be more secure against hacking threats; can they be more scalable, so that more people can use them; and can they remain decentralised, so that they are community assets rather than owned by a big tech firm? The protocol has a layered architecture to allow for flexibility and scalability. It uses proof-of-stake instead of proof-of-work to reduce energy consumption.

> "The problem with blockchains is that they can't take nearly as many transactions per second as Visa or Mastercard and gas fees are expensive and unpredictable."

Solana launched in March 2020. It has a high throughput and low transaction fees, this was enabled by a new consensus mechanism, Proof-of-History (PoH).

> "The problem with blockchains are that you need to be a PhD level mathematician to work with them". NEAR Foundation launched in April 2020. It prioritises usability and interoperability, that is the ability to avoid working with a blockchain but getting stuck in a 'walled garden'.
>
> The problem with blockchains is that the infrastructure isn't what we'd get in a bank."

Avalanche launched in September 2020. A highly scalable and interoperable platform, Avalanche aims to provide a robust infrastructure for DeFi and enterprise applications with a consensus protocol designed for high transaction throughput and low latency. (Latency is a big thing in blockchain development. It is equivalent to friction in the real world. If you did not already know that then you are not playing enough Fortnite.)

> "The problem with blockchains is that there are now just loads of them when all we really ever wanted was just for Ethereum to just be faster and better."

Polygon launched in 2021. Polygon is a "layer 2" solution. This means that it sits on top of other chains and fixes some issue with them. Polygon improves Ethereum by enabling faster and more cost-effective transactions. Therefore, you can have the upside (security and functionality) of Ethereum without the downside (lack of scalability and unpredictable cost of transactions).

To illustrate the practical effect of all this engineering we can use settlement times as a proxy for the type of improvements that were being made by new chains. In any financial transaction settlement finality is critical. Settlement finality tells you that your transaction cannot be unwound. That cannot be a charge back or rewriting of accounts such that funds you thought you had received in your account were taken back from it. The operation of the Bitcoin system, in particular the fact it uses proof-of-work consensus, means that settlement finality is achieved around one hour from the time of the transaction. In the case of Ethereum, settlement finality is achieved around 15 minutes from the time of

the transaction. In the case of Solana, settlement finality is achieved less than one second from the time of the transaction.

These are simplifications and I am not advocating for any particular chain (everyone has their favourite chain—you will know you have become a true Crypto person when you have yours …). But you get the idea: engineers solving technical problems.

What followed Ethereum—practical

Crypto is confusing because it has everything going on all at the same time. While the engineers were working on the technical issues we have just discussed, other parts of the community were trying to fix different kinds of issues.

For example, Crypto is a volatile asset. On the day that I am writing this bitcoin is at an all-time (postTrump election win) high—nearly $90,000. But within the last 12 months the price of bitcoin has been as low as $36,000. The price of bitcoin is often the only thing that people outside Crypto know about Crypto. Inside Crypto, it is considered important for that reason, but it is only one of a thousand things that people are thinking about each day.

The first rule of Crypto is that you do not talk about the price of bitcoin. Mainly because it is the surest way to look like a fool within the week. One of the challenges of cryptocurrencies is their volatility. To address this, Crypto developed stablecoins. Like bitcoin, they were a technical solution to a social problem. Stablecoins are cryptocurrencies pegged to a stable asset, such as the US dollar, to maintain a consistent value. Unless there is a technical or economic failure in a USD stablecoin, it can always be exchanged for the equivalent of USD 1. Either $1 for 1 USD stablecoin. Or 1 USD stablecoin for an equivalent of bitcoin or another cryptotoken. Because this was driven by a market not a government, different solutions emerged. The largest USD stablecoins at the time of writing are Tether (USDT) and USD Coin (USDC). An issue (volatility) has been solved, but the price we paid for that was to have multiple competing solutions (which, depending on your viewpoint is either good news because you can decide for yourself which meets your needs by reference to its security, privacy etc; or it is bad news because, as well as all the other confusing things, we now have “different flavours of dollars”.)

Since Crypto is outside the banking system but cryptocurrencies are money-like in some respects, developers copied banking products that people liked but could not get in Crypto. If you deposit your money in a bank, it will pay you interest on your deposit. Crypto did not originally have this feature. The value of your cryptotokens might rise or fall but you could not hold them and earn from them. So, engineers and the market developed staking. In a proof-of-stake network “staking” your cryptocurrency tokens means making them available to participate in the validation and security of the network, thereby supporting the functioning of the network for a period. At the end of the period, the tokens are returned together with additional tokens.

To a banking regulator this looks similar to earning interest on a bank account but it is not. There is no chose in action relationship, as referenced above in the context of a bank account. In contrast, staking involves actively participating in the processes of the network verifying transactions by proposing and accepting blocks. Rewards are generated and distributed as a result of this participation in the consensus mechanism. The work done by stakers is what makes the network secure on a decentralised basis. If we are using a banking analogy, staking is more like working in the bank than being a customer. Regulators that view staking as interest are looking at the return rather than the activity. We have another example of how you get a different answer depending on the perspective from which you ask the question.

I hope you will see that we are still just trying to solve problems to improve the system (with the system being defined by different people in different ways).

The price of bitcoin

There is no such thing as the price of bitcoin. Goods have a recommended retail price. The price of services is set by the person who is offering to provide them. The price of shares is set by the company in an initial offering and set by the market in secondary offer. Offering shares to the public must be done through a recognised investment exchange. There are relatively few of these and they are all well known. Therefore, there are only a few places you can go to get a price for a share. Therefore, any difference in price would very quickly be arbitraged away.

Bitcoin is offered by exchanges, particularly the famous Crypto exchanges (which are centralised exchanges, i.e. there is some sort of legal entity, that has staff, running them). There are many exchanges, large and small. There are also many decentralised exchanges that operate with smart contracts and code performing the role performed by legal entities and departments in centralised exchanges. Since you can own your own bitcoin rather than relying on a third party custodian, you can also sell it to whoever you want for any price that you want. There are certainly arbitrage opportunities in Crypto and lots of people have made fortunes from them, but they take more work and involve more risk to exploit than with listed company shares.

Therefore, the quoted price of bitcoin in the news may be a price quoted on one of the exchanges. In our legal agreements it is a price we describe usually by reference to averages of a number of exchanges that are all accessible by the parties in our transaction.

This is the point at which we can explain why bitcoin is so special in legal terms. Always running in the background of the story of Crypto is an argument between the Crypto industry and the SEC about whether cryptotokens are securities. The SEC regulates the issuance of securities in the US. If Bitcoin is a security, the SEC has oversight of it.

While bitcoin appears to have some characteristics of a security in the sense that people treat it as a financial asset and trade it on exchanges, it also has some fundamental differences. There is no issuer of bitcoin, only code. There are no articles of association that could set out rights of holders, for example to vote or receive dividends or capital on a winding up, as for an equity instrument. There are no contract terms describing a right to interest or to redemption, as for a debt instrument. There is only code.

Many people have tried analogies to explain what ownership of a decentralised digital asset is like. Bitcoin is like digital gold or digital cash. Since Ethereum, digital assets are smart and this functionality is part of the value. Tokens give rights to use a network that has practical value being tradeable; those rights therefore also have economic value. It is not a perfect analogy, but one I think can help to explain the distinction in this context is the difference between owning shares in BT and owning rights (which can be traded, held for later use or used at any time) to use the BT fibre network. The value of data and the value of server time in data centres is now starting to make the analogy clearer. Don Wilson, who set up DRW, a trading firm, is quoted in the 15 November 2024 Financial Times saying: “Will compute become the largest commodity in the world? I think that it’s a reasonable argument.”

I am aware that this section appears to break the first rule of Crypto but that is okay we can break some rules.

Social and political points

As we said initially, when you send money to your friend, what you are doing is sending instructions to a bank to take steps that will end with your friend having money in their account. That suggests that banks simply follow instructions they are given. As you might now expect, there is more to it than that. Banks will (because they are legally obliged to) check you out. Know Your Customer (KYC) checks verify the identity of both the sender and the recipient of funds. Banks must also check out the money. Anti-Money Laundering (AML) checks are required to detect and prevent money laundering and terrorist financing. Banks may also need you to declare the source of the funds and their intended use. That covers the regulatory side of things. Your relationship with your bank is one of contract. The banks' terms and conditions set out the contract relating to your account. Both the bank's and your legally-binding obligations in relation to your account are set out there, and the bank is also bound by consumer protection regulation.

This is all now quite familiar to people: you cannot just send money. Your bank performs a role on behalf of your government to stop you making a transfer that is illegal or suspicious. But, of course, you can give money to your friend without being subject to all of this.

If you hand your friend a £20 note, chances are they will thank you and put it in their pocket. They are less likely to: ask where you got it; want to see your passport; make you tell the government what you are about to do; or insist that you give it to a large corporation and tell them to give it to you as soon as they have looked up who you are.

Some people think that it is not a legitimate role of government to know what you are doing with your own money and stop you if they do not like it. Since bitcoin is decentralised, transferring money to your friend actually involves transferring money to your friend, without intermediary involvement. That is why Crypto appeals to libertarians. The political philosophy of libertarianism argues that individuals should have the freedom to make their own choices about their lives, as long as they do not infringe on the rights of others. It emphasises civil liberties, including freedom of speech, freedom of association, and the right to privacy. When speaking to libertarians about Crypto, you are talking to them about their right to privacy.

Fun for lawyers

For lawyers in the UK, the Law Commission work on digital assets is subtle and brilliant. You can download for free from their website hundreds of pages of exposition on the English law of property, without a single reference to real estate.

The Law Commission says:

> "Digital assets are increasingly important in modern society. They are used for an expanding variety of purposes — including as valuable things in themselves, as a means of payment, or to represent or be linked to other things or rights — and in growing volumes. Electronic signatures, cryptography, smart contracts, distributed ledgers and associated technology broaden the ways in which digital assets can be created, accessed, used and transferred. Such technological development is set only to continue.
>
> Some digital assets (including cryptotokens and cryptoassets) are treated as objects of property by market participants. Property and property rights are vital to modern social, economic and legal systems and should be recognised and protected as such."

We do not need to go into much detail for me to make a point to illustrate why I love Crypto. Crypto tests the boundaries of our terminology and mental models. A neat way to show this is with the concept

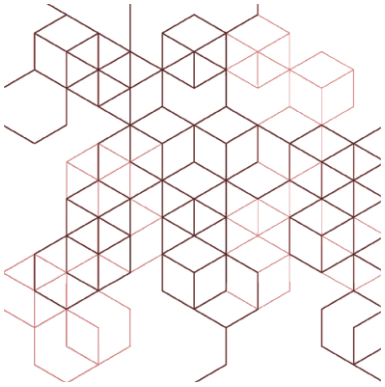
of fungibility. Fungibility is a simple concept. Fungibility refers to the quality of being mutually interchangeable with other items of a similar kind, quality, and grade. In law a good or asset whose individual units are interchangeable and indistinguishable from one another is fungible. Debts can be repaid using the class, not the individual item. Shares in a company have numbered share certificates but these are irrelevant to the rights attached to those shares.

A bitcoin is a fungible token. They are all the same as each other because they are representations on the same ledger. Bitcoins are not NFTs (tokens that are non-fungible by design). Hence, bitcoins are technically and legally the same one with another, just like dollars. But you would not pay the same price for all of them. Because the blockchain is transparent and immutable, bitcoins have a history. A bitcoin that has been used in an illicit transaction may be at risk of confiscation by a law enforcement body. You can still buy but would not pay the same price as for a bitcoin that had no such history. Therefore, people will pay more for a freshly minted bitcoin.

What if the bitcoin was involved in illicit activity, then confiscated by the FBI, then the FBI offered to sell it to you. What would you pay for that bitcoin? We have now a distinction between legal, technical, and economic fungibility. Until Crypto, fungibility was fungibility. Bitcoin has updated how we now need to think about fungibility.

The same boundaries are tested a different way for dollars. US dollars are definitely fungible. US federal law strongly restricts private money within the borders of the country and its politicians want to protect the country's monetary sovereignty. For these reasons US dollars are all the same. However, USD stablecoins are digital tokens backed by US dollars, but also in practice by other collateral. They are not dollars. If the Federal Reserve issued a digital dollar, that would be a dollar. But stablecoins are not dollars and they're all different because they have different backing and the issuers have different legal structures. As a result we have non-digital US dollars, which are fungible. And digital US dollars, which are (usually) worth a dollar, but are not dollars. Crypto has expanded the concept of fungibility in unexpected ways and give us different flavours of dollars.

If you think this is interesting, you'll probably like Crypto.



International issues

This book is published in the UK. Some of the benefits of Crypto that are obvious elsewhere are less apparent in the UK because of its relatively stable financial system and currency, plus relatively well-functioning banking system. In other countries these things cannot be taken for granted.

If you talk to anyone who lives in a country:

- with very high, persistent inflation;
- with a currency that has a history of significant depreciations;
- with exchange controls;

- where the government may appropriate amounts from bank accounts of the population;
- where a substantial number of the population do not have access to bank accounts;
- where banks are unsafe for reasons of undercapitalisation, corruption, mismanagement or otherwise;
- with high crime;
- with a government that sets rules for what citizens are permitted to spend money on;
- with a government that surveils its population's activities;

they will likely tell you that Crypto is popular in their country and everyone knows why it is.

Finally…

Do not be put off. This is a fun topic. The people are smart and interesting. It is relevant to how we understand money (projects often branded as stablecoins), how the financial system works (tokenisation), how and why trust is established between people (decentralised governance, DAOs), the future of the Internet (Web3), how commerce will develop (Web3 again), sociology, politics, economics, and much else.

You can find your people. It does take a while to untangle things but when it is explained in a way that makes sense to you, keep going in that direction. Once you dive into it, things may still seem confusing at first. However, you start to let go of that worry and appreciate it for what it is. If you're a cricket fan, think of explaining the game to someone who does not know it well—when you try to explain it, it sounds odd, but once you play it, it all clicks. Learning about crypto can feel like that. And if you are not a fan of cricket, don't worry—crypto is nothing like it. Enjoy the journey!

Crypto, Part 2

Part 2 is not really footnotes to the first part of the story—it is the same story told from a different perspective. People can learn to understand crypto better by having different explanations of it. This second part of the story is a different explanation of the same story. The first part was from the standpoint of the people doing the things, their motivations and aims. The second part shifts the focus to the technologies themselves. In Part I tried not to use intimidating terminology but we can now hear the story though the language of the terminology. I hope that you now have enough context to not be put off by this second explanation. By the end of it, you will have heard the terminology in context making it easier to recognise and understand in future contexts. Think of this section as a structured dictionary of crypto—not organized alphabetically, which assumes prior knowledge, but following the same logical flow as Part 1, allowing concepts to build on one another naturally.

Before we start with our dictionary of Crypto, we should address if this is worth the effort. I have explained Crypto from an engineering perspective and described how the engineers love solving problems. This experiment is all great fun to work on, pushes forward the state of the art in messaging, and creates more value than it destroys. But is there a point to it beyond the experimentation. Do we actually need it?

A way to look at that is to justify the benefits of blockchain by comparing them to the current alternative. It's a cliché that fish do not know what water is. The question we must ask ourselves is whether our financial system involves us all swimming in water despite having a better alternative.

I have tried to avoid the usual approach to explaining blockchain—blockchain is a transparent, immutable and secure system of records. These seem like necessary criteria but also obvious ones. Surely the banking system has all this covered?

Transparent means trustable. Wirecard, a German payment processing company, failed in 2020 after it was revealed that €1.9 billion supposedly held in trustee accounts did not exist. Blockchain records, including balances, can be viewed and cannot be hidden.

Immutable means unfakeable. Employees at Wells Fargo created millions of unauthorised bank and credit card accounts without customers' knowledge in 2016 to meet targets and earn bonuses. To cover up these activities, employees forged signatures and altered records. Blockchain records cannot be forged or altered.

Secure means unhackable. In 2016, the Bangladesh Bank was hacked using malware so that fraudulent transfer requests for more than $80m were actioned. Hackers like to say that even if it is difficult to penetrate the systems of large enterprises, they can try many times and only need to be successful once; then when they are inside everything is open to them. Decentralised systems cannot be compromised in the same way. If one computer node is penetrated, the rest maintain the system.

International funds transfers can also be optimised by using bitcoin. In a famous example, in 2020 Bitfinex exchange transferred 161,500 BTC—$1.1 billion at the time—for a fee of $0.68.

It sounds like Crypto might be able to improve some things. But, like any topic where experts have worked in the dark for 10 years, everyone else needs some help to catch up before they can join in. Crypto is full of jargon. Some is technical, some financial, some social (including many memes). It is difficult to engage with Crypto without some familiarity with the jargon. This section tells the story of Crypto through its terminology.

Our starting point is, of course, **cryptography**: the practice of securing information through mathematical techniques, ensuring confidentiality, integrity, and authenticity.

The technical foundation of using cryptography to create and transfer value and digital assets is **public and private key cryptography,** which for decentralised digital currencies, works in this way.

Public key cryptography (also known as asymmetric cryptography) is an encryption scheme that employs two mathematically related, but different, keys: a public key and a private key. These keys are typically structured as long strings of data. The generation of the key pairs relies on cryptographic algorithms based on mathematical problems that are deliberately computationally difficult to solve.

Each key serves a unique function: the public key encrypts, the private key decrypts. In a public key cryptography system, anyone can encrypt a message using the recipient's public key, but only the recipient can decrypt it with their private key.

Bitcoin relies on cryptographic key pairs:

- **public key**: a long string of alphanumeric characters that is visible to everyone in the system;
- **private key**: a different long string of alphanumeric characters that is known only to the owner of the key—specifically, it is a 256-bit number, represented as a string of 64 hexadecimal characters.

The public key:

- is a destination address for receiving bitcoin from other users—like an email address or bank account number;
- can be freely shared, without any risk to account security—it is mathematically derived from the private key, but the process is not reversible (see above, this is "asymmetric cryptography").

The private key:

- is a unique digital signature for a Bitcoin wallet—like a password (it controls the account so anyone with access to a private key can control the wallet) ;
- authorises transactions on the address.

When we talk about **wallets**, as a technical matter we are talking about addresses on the network (although there are now other ways to store and access your bitcoin such as specialist hardware "wallets"). A commonly used analogy is that: your public key is your home address, and your private key as the key to your front door:

- anyone can know your address (public key) to send you mail (bitcoin), just as anyone can see a house from the street;
- only you should have the key (private key) to open your door and access what's inside, just as only you should be able to spend your bitcoin;
- if you give someone a copy of your house key (private key), they can enter your house (bitcoin wallet) and take your stuff (spend your bitcoin);
- you can change your locks (create a new key pair) if your private key is compromised (someone has a copy of the characters), but you cannot change your address (public key) without moving to a new house (creating a new bitcoin address).

How to send Bitcoin:

- create a transaction specifying the recipient's public key and the amount to be sent—use your private key to digitally sign this transaction—*Bitcoin is based on secure digital signatures*, as described in Part 1;
- this signature proves to the Bitcoin network that you are the owner of the bitcoin being sent;
- the network verifies the signature using your public key;
- the network processes the transaction.

How to receive bitcoin:

- share your public key—your public key does not contain your name or identifying information—this is the basis on which *the network is described as pseudonymous*;
- the sender uses it as the destination, as described above;
- the transaction is verified, processed and recorded on the bitcoin blockchain;
- the sent bitcoin is associated with your public key—transactions are visible—*the network is transparent*—but your identity is not.

The cryptographic key system is what allows Bitcoin to function as a *-secure, -peer-to-peer -digital currency*. There have been technical developments relating to **keys** since the release of the Bitcoin protocol. For example:

- **Sharding** involves splitting a single key into multiple pieces, allowing subsets of these pieces to be recombined to use the key for signatures and transactions. This is useful as a security measure, for example to reduce the risk of a wrench attack.
- A **wrench attack** involves an attacker physically coercing a keyholder to transfer tokens or relinquish control, often by surrendering their private key. It is called a wrench attack because a criminal might use a wrench to threaten someone to hand over their private key.

We have described Crypto as an open ecosystem where it is possible to enter into financial transactions with people that you have not met. It would be obvious from this that security is an issue of great concern to the community and the industry. Outsiders often think that, since Crypto relates to technology and security is a big issue, the problem must be related to hackers' ability to exploit bugs in the system. As the example of the wrench attack shows, it is far more common for hackers or criminals to exploit people than technology. We can be sure that the best hackers on the planet have tried to crack bitcoin's security because doing so would be so valuable but it has been around for 15 years and no one has managed it yet. It is elegant, high-end technology. Do not take my word for it:

> "Bitcoin is a remarkable cryptographic achievement, and the ability to create something that is not duplicable in the digital world has enormous value." (Eric Schmidt)
>
> "Bitcoin is a technological tour de force." (Bill Gates)

As a technical matter, the problem in Crypto is not that code is inherently insecure. It is that people can be hacked and that some projects rush out improperly tested new products and spend too little on security.

Multi-signature arrangements, or M-of-N arrangements, require a specified number of signatures or keys (M) out of a total number (N) to authenticate a transaction.

This is the point at which we move from the underlying technology itself to how it is categorised in forms that people interact with.

Blockchain technology is a type of distributed ledger technology (DLT) that records transactions in a chain of blocks. There are many different blockchains, for example Bitcoin, Ethereum, and the others referenced in chapter 1. They have technical similarities but they are different. Think of CHAPS vs Faster Payments etc. in banking.

Consensus is the process by which all computers in a blockchain network agree on the validity of transactions and the state of the blockchain. This is why all computers can share the same ledger without the need for reconciliation. There is one ledger updated and viewed by all computers in the system. A **shared ledger** provides huge savings by removing the need for every party involved in any step of a transaction to each do their own reconciliation of their ledger and compare notes until they get them to all match. There is therefore no need for a central authority. The shared ledger is the "single source of truth". The integrity and security of the network is agreed between all the parties. See the reference in chapter 1 to the Byzantine Generals Problem for how this happens.

Peer-to-peer transactions are by definition decentralised. For value to transfer safely in a decentralised system requires some technique by which all users of the system can agree on information in the system.

Consensus is a characteristic of true decentralisation. Crypto natives think everything should be decentralised—existing onchain only. In the real world some transactions have elements that are represented only on a blockchain and some that are represented elsewhere.

Onchain and Offchain transactions are distinguished by how they are recorded. Blockchains record data by grouping it into timestamped "blocks" each mathematically linked to each other, going back to a "genesis" block. Onchain transactions are recorded on the blockchain. Offchain transactions are not recorded on the blockchain; they occur externally (for example, through a written sale and purchase agreement) or on secondary protocols interacting with the blockchain.

That completes the terms relating to blockchain . Let us now look wider at the categories of related technologies that you may come across in Crypto.

Hashgraphs are an example of DLT but are not blockchains. They use a different type of consensus algorithm. The reason that hashgraphs have been used in certain cases is because they achieve high throughput and low latency. In other words they are another way to address the issues that are referenced in chapter 1 in the technical section about what followed Ethereum.

DLT refers to a broader category of technologies that distribute data across multiple nodes. A distributed ledger is a **digital store of information** or data, **shared among a network of computers** and potentially accessible to other participants. Additions to the ledger are approved and synchronised through an agreed consensus mechanism. The parts in bold above are common between DLT and blockchain, but only blockchain features timestamped blocks as referenced in the blockchain definition above.

Blockchain technologies are a type of DLT but not all DLT are blockchain. Expressed pictorially DLT is a big circle and blockchain and hashgraphs are both smaller circles inside the big circle but not overlapping with each other.

Now for some terminology related to the operations of the systems.

Nodes is the term used for the computers participating in DLT (which includes blockchain) networks.

State Change, occurs when a records on a distributed ledger are updated. The "state" of the ledger is the transaction history at a point in time. A state change is the name given to what happens

when the ledger has new information added, blocks in the case of a blockchain. Those changes must be in accordance with the rules of the system.

The **Protocol** is the terminology used in Crypto for the set of rules of the system.

Permissioned systems are those that require authorisation from an administrator to perform activities onchain. They are therefore analogous to centralised systems and exchanges in traditional finance.

Permissionless systems are those that do not require authorisation from an administrator to perform activities onchain. This is a characteristic of true decentralisation.

TradFi is what a Crypto person will call traditional financial markets, institutions and technology.

Open-Source Software is software where the creators voluntarily give up their copyright. It is released under a licence that grants users rights to use and modify the software and source code for any purpose.

This brings us to the heart of the matter: cryptocurrencies, cryptotokens, cryptoassets and digital assets.

Cryptocurrencies are digital assets that have some characteristics of money (such as being able to be used as a medium of exchange or a store of value) and use cryptography to secure transactions and control the creation of new units. They operate on their own blockchain (e.g. Bitcoin, Ethereum). Cryptography replaces a centralised intermediary (such as a bank or a government) in the creation and transfer of these currencies. Cryptocurrencies are like money but money on the internet.

Bitcoin is the ur-example of a **-public**, **-permissionless -cryptotoken system**; it facilitates electronic transactions without a centralised intermediary to authenticate them.

bitcoin (BTC) is the currency of the Bitcoin system.

Unspent Transaction Outputs (UTXOs) are a technical characteristic of (certain) cryptocurrencies. They are balancing items when cryptocurrencies are spent. They occur when an amount to be spent (outputs of transactions) is not exactly equal to the amount that is spendable due to available denominations in a wallet (so that a remainder should be available for use as inputs for new transactions). Think of using a £20 note to buy something costing £15. Originally, not much of a problem in practice but obviously more so as the price of one bitcoin appreciated into tens of thousands of dollars. This was a technical challenge that Bitcoin solved.

Ethereum is a **-public**, **-permissionless -blockchain system**; it operates as a transaction-based state machine that facilitates decentralised applications built using smart contracts.

Ether (ETH) is the currency of the Ethereum system.

Cryptotokens are digital assets that can represent various forms of value, including utility, governance, or security. They are issued on existing blockchains, often representing assets or utility within that ecosystem (e.g., ERC-20 tokens on Ethereum).

A technical explanation would be that a cryptotoken is a notional quantity unit manifested by the active operation of software and network-instantiated data. Cryptotokens are cryptocurrencies (like money) and also digital assets.

Cryptoassets and digital assets. A digital asset is any asset represented digitally or electronically. Not all digital assets are cryptoassets. For example, in-game currency or music downloaded onto a computer are digital assets because they are assets (they can be owned) and they are digital (they exist only on a computer or similar electronic device or system). A cryptoasset is a cryptotoken that is recognisable within a legal system. Not all cryptotokens are cryptoassets. Tokens are how computers talk to each other. A cryptotoken can send a message, but does not have or represent value aside from this. A cryptoasset does.

Cryptoasset is therefore a term more often used by lawyers than true Crypto-natives and cryptotokens is the term more used by Crypto-natives.

Digital assets is an all-encompassing term, although in the context of Crypto, a digital asset is normally a cryptotoken (with native value or representing some valuable off-chain thing), in other words in practice it is used more narrowly than how I have defined it three paragraphs above.

Expressed pictorially, **cryptotokens** are the big circle—**cryptoassets** are a smaller circle within it—**cryptocurrencies** are a smaller circle within that.

You should be aware that even experts use the terms loosely, interchangeably and inconsistently (including within a single piece of writing or conversation).

When you reach a certain level of confidence, you will enjoy arguing with people about how these terms are being used and whether they should have initial capitals, be one or two words, or be hyphenated. When you are a Crypto-native you will stop bothering. At this point you might want to have a short break and make yourself a cup of tea.

Welcome back.

Just a couple more definitions of types of assets, but these are clearer and therefore used in a much less confusing way than the ones above.

Real-World Assets (RWAs) are physical (art, classic, cars etc.) or traditional financial assets (stocks, bonds, etc.) that have been tokenised and represented on a blockchain. Tokenizing RWAs can enhance liquidity, transparency, and accessibility, making it easier to trade and manage these assets. They are a smaller circle inside the cryptoassets circle. More on this below under Tokenisation.

Non-Fungible Tokens (NFTs) are unique digital assets that represent ownership of a specific item or piece of content, such as *digital* art, music, or virtual real estate. Cryptocurrencies are fungible by design. It is important that one bitcoin is the same as any other in the same way that one £20 note is the same as any other for economic purposes. NFTs are not interchangeable and have distinct value. It is important that an NFT is not the same as any other because they are identifiable and collectable. This explains their use in art and entertainment.

In Part 1 we described how technical developments designed to improve the speed or security or some other aspect of how our existing blockchains worked led to both new blockchains and add-ons to existing ones. This ecosystem has now been subject to a customary categorisation.

The “original” blockchains are those that operate bitcoin and Ethereum.

Blockchains that operate on the same basis as those (that is being themselves the network on which information, including value and contracts, move), are referred to as layer 1. They got this name when technical solutions built on them started appearing, since these were then called layer 2.

Completing the picture for now, layer 3 blockchains build apps on layer 2. Layer 0 blockchains run services between layer 2 blockchains to avoid them developing as walled gardens.

So, to make an imperfect analogy for the sake of using one that everyone will know, the picture is something like: your iPhone is layer 1; layer 2 an upgrade to your iPhone; layer 3 is the Apps on your phone; layer 0 is tools that allow your iPhone to communicate with Android phones.

Blockchain layers

Layer 0 (L0) is foundational infrastructure that supports multiple blockchains, providing functions such as interoperability of transactions and communication between different blockchains.

Layer 1 (L1) blockchains are **t**he base layer—the cryptotoken architecture, system, network, or protocols—of a blockchain network, responsible for consensus, security, and transaction processing (the best known examples are bitcoin and Ethereum).

Layer 2 (L2) describes a secondary protocol built to interact with an underlying L1 by using it to perform certain critical functions, such as settlement of transactions and transaction security. These protocols are described as being "built on top of" the L1. Their purpose is to improve scalability and efficiency. They do this by, for example, aggregating transactions before sending them to the L1 for recording on the L1 blockchain.

Polygon (for example) processes transactions off the main Ethereum chain, which helps to reduce the number of transactions on Ethereum. This off-chain processing allows for faster and cheaper transactions. Polygon is an example of an L2. It is considered an L2 because it uses the Ethereum main chain security system and maintains a decentralised network of validators. It is designed to be highly compatible with Ethereum (but, as one of its technical innovations, it also supports other scaling solutions and is compatible with other blockchains.)

Other technical approaches to achieve speed and scalability are not considered L2s because: (a) they are blockchains but, for example, use their own chains and do not rely on the security system of the main chain; or (b) they use technology other than blockchain for to communicate. Examples of these are sidechains and state channels.

Sidechains are independent blockchains that run parallel to a main blockchain (e.g. Ethereum) and are attached to it through a connection that allows assets to be transferred between the "main chain" and the "sidechain". Sidechains' purpose is usually scalability; their approaches are often experimental, testing different consensus mechanisms and security models.

State channels are off-chain communication channels (not blockchains) that allow multiple transactions between parties to be conducted off the main blockchain, with only the final state (that is, the outcome of all the transactions, like making up accounts at the end of a day) being recorded onchain. State channels are a way of improving transaction speed and reducing costs.

Layer 3 (L3) is the application layer, where dApps and user interfaces interact with the underlying blockchain infrastructure.

Each layer plays a role in the overall functionality and scalability of blockchain networks. As we saw in Part 1 1 where the story of blockchain development was the story of engineering problems being identified and then solved, the same thing has happened in developments alongside the new blockchains.

Rollups execute transactions outside an L1 before recording batches on the L1. Rollups therefore (a) make transactions faster and cheaper, using their system, (b) still make transactions benefit from the high security standards of the L1, where transactions are ultimately posted.

There are two main types of rollups: Optimistic Rollups and ZK-Rollups.

Optimistic Rollups assume transactions are valid by default and only run computations if there is a challenge to the validity of a transaction.

ZK-Rollups (Zero-Knowledge Rollups) use zero-knowledge proofs to validate transactions, ensuring that all transactions are correct without needing to post all transaction data on-chain.

State channels and rollups do the same thing in different ways. Rollups do it using L2 chains. State channels do it using a private channel between parties. We're going down the rabbit hole here, but the point is that Crypto is about how engineers solve problems. They do it different ways.

Decentralised finance operates without centralised authorities because it runs on code. Part of the reason that this code was called smart contracts is that it reflects analogies between DeFi and TradFi. In TradFi, transactions and relationships are based on contracts. For your bank account you have a contract represented by terms and conditions with your bank as we described in the example in Part 1.

In DeFi., we can see that the equivalent is not possible. You do not necessarily know the party that you are dealing with. Therefore, the system cannot have a requirement that you must formally contract with them. In DeFi, this role is undertaken by code. And we call the code (smart) contracts. Smart contracts are therefore critical to the operation of decentralised finance.

Some of the history of commercial contracts is replayed in DeFi and smart contracts. Early contracts developed alongside early bookkeeping (ledgers) to provide for simple bargains such as the sale of commodity goods, like crops. Transactions developed to take account of developing requirements of business parties, for example the sale today of wheat after this summer's harvest—a futures contract. The same has happened in decentralised finance: developers have deliberately copied (with adaptations) some traditional commercial contract transactions using blockchains and smart contracts because they are the building blocks of commerce; in addition they have inadvertently copied (with adaptations) some other commercial and financial contracts because they are obvious or useful whether or not you are trying to build a parallel financial system; and, also, there have been developments in the technology that have, while designed to solve technical issues, have given rise to new types of products, such as decentralised exchanges, and lending and borrowing platforms.

For lawyers, the analogy with commercial contracts is useful, in particular because the operation and implementation of smart contracts in all these various contexts is giving rise to a kind of Lex Mercatoria for Crypto which, as for contracts and smart contracts, will in some ways track traditional case law and, in some ways, will differ. For those who are not legal historians, Lex Mercatoria is a system of customary law developed by merchants during the early Middle Ages to regulate trade and resolve disputes. It emerged as merchants from different regions needed a common set of rules to facilitate trade. What developed is recognisable to us today as freedom of contract and protection of property rights. Common rules meant lower transaction costs. More transactions meant more confidence in transactions which then led to the development of credit products. This further increased trade and more innovation followed. What we see today in DeFi is the development of a Lex Mercatoria for Crypto.

Professionals working in financial services should note that DeFi now has equivalent or competing services to payments, trading, lending, investments, insurance, and asset management.

Decentralised Finance (DeFi) can therefore be defined as code-based financial services built on blockchain technology as a settlement layer and without the need for or the possibility of human intervention in transactions. From a social perspective, using blockchain means that users access financial services without intermediaries. The argument for this is that it brings greater transparency

and accessibility for users; in theory users are owners of the networks, because they can acquire cryptotokens native to the networks and these give an involvement in and interest "stake") in the network.

The term stake is broadly defined and, although it varies project to project, it would generally be expected to include rights to use the network, to take part in network operations by acting as a validator, and to have a say on strategic matters affecting the network. This is not like owning shares in the bank where you have your current account: I think I'm safe to assume that your bank does not want you as part owner of its IT or showing up to board meetings and telling them what you think they should be doing.

The code that "runs" the blockchains—in the sense that it is coded digital instructions (we can say "agreements" when they interact between wallets) using special blockchain programming language that execute and store actions on a blockchain – is what we call smart contracts.

I keep saying that Crypto is still an experiment. Well DeFi is definitely still an experiment. With that in mind, how can we expect it to develop?

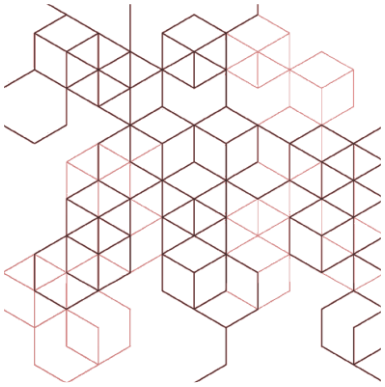
DeFi has shown that it can create product innovations that could not have been easily imagined in Tradfi. **Automated market makers** fill orders without using an order book. Traditional securities brokers are intermediaries finding buyers for stock their clients are selling. AMMs are decentralised exchange protocols that use algorithmic formulas to determine the price of assets and let users trade directly with a pool of assets made available by other users who earn fees for providing this liquidity. **Liquid staking protocols** allow users to earn rewards for helping secure a blockchain by locking up their tokens, while still being able to trade or use a derivative token that represents their staked assets. Users can benefit from staking rewards but still access or move their funds.

Once you have the language you can see how people put things together. So, a liquid staking protocol can be understood like this:

- protocol tells you it's running on code (smart contracts);
- staking tells you that its purpose is to generate yield;
- liquid tells you that tokens are not locked.

A Crypto person would know that staking is valuable but requires giving up access to the staked tokens. Therefore, they would know right away that the innovation here is liquidity in the context of staking.

Again, the products are natural outputs of applying engineering solutions to fill in logical gaps in these emerging markets. In the case of automated market makers, this is to continue following the logic of removing intermediaries. In the case of liquid staking protocols, it is to slice the Gordian knot between accessing yield for cryptotoken investors without losing access to them. Imagine a bank account that paid you interest on your balance but at the same time didn't stop you spending it.



The shape of the next experiments are already apparent. These combine on the one hand integration with TradFi, and on the other pushing the boundaries of the logic of DeFi.

In the first case, **Real World Asset tokenisation** puts assets on chain as digital tokens. This partly makes old markets more efficient because of the technical upgrade in the background. It also makes new markets because new products can be created with more online markets, more liquidity and the ability to split assets into parts, such as cash flows from the floors of a high rise building that have different types of tenants—gyms in the basement, shops on the ground floor, apartments higher up, hotel rooms at the top being traded separately—fractionalisation. More on this below, under Tokenisation.

In the second case, the engineers are already at work on innovations such as:

- yield AMM protocols—tokenizing future yield;
- yield aggregators—find the best yield opportunities across platforms
- derivatives DEXs x borrowing and lending markets—all encompassing trading.

I am not going to even attempt to explain those. The point is: Crypto Never Sleeps! People work across timezones and borders (and also a meme) it is customary to start any conversation with a Crypto person with the greeting "GM" (meaning good morning), because it is always morning somewhere in Cryptoland.

The preceding paragraphs provide an explanation why regulators break out in a cold sweat when they think about Crypto. If we want true institutional adoption, we are going to have to fix this.

Do we want institutional adoption? You would get as many answers to that questions as there are people working in Crypto.

Smart Contracts are computer codes that run automatically (no need for people to intervene—when the conditional event happens, the code executes the action) and deterministically (they always perform the action and only the action when the pre-programmed condition occurs).

Although smart contracts operate automatically, they are infinitely adaptable.

Composability is a design principle concerning relationships in a system. Blockchains are highly composable systems, allowing components to be selected and assembled in various combinations to meet specific user requirements. Composability in DeFi and Crypto arises from the fact that it uses open source software, open standards, shared protocols, and smart contracts.

Technical developers have worked on features that improve the functioning and security of the systems. For example,

Hash Time Locked Contracts require recipients to acknowledge receipt of cryptotokens by generating cryptographic proof of receipt in order for it to be effective. These contracts combine hashlocks, which restrict transactions until a hashed public key is unlocked with the associated private key, and timelocks, which specify the earliest time or block for a transaction to be capable of inclusion in the blockchain.

Although we say that DeFi does not require intermediaries, that is not to say that DeFi is not populated by its own entities. This is just as the traditional economy (following the innovative standards of the Lex Mercatoria, with theoretical and entity innovations such as legal personality and joint stock companies) developed entities through which people do business.

Decentralized Autonomous Organizations (DAOs) are governed by smart contracts and decentralised decision-making, enabling collective management and ownership. The "organisation" can

be an emergent property of those features, involving no form of legal entity taken from the list of options from the worldwide lists of options. DAOs represent a new model of organisational structure, where decisions are made by tokenholders through a transparent and democratic process.

Tokenomics—as cryptocurrencies are money, so protocols are economies, analogous to the economy of a country or a region.

Token economies and real world economies both include:

Monetary policy: money supply and interest rates to achieve economic stability, achieved (in a token economy) through token supply and token distribution.

Token Supply is the maximum number of tokens that can ever be issued (contrast with the circulating supply, which is the number of tokens currently issued). By issuing (called "minting") new tokens or withdrawing (called "burning") existing ones, the supply of money can be controlled over time which, in the same way as with fiat money, causes inflation (more tokens in circulation) or deflation (less tokens in circulation). We all know about this because we just lived through QE.

Token Distribution is created by a combination of Initial Coin Offerings (ICO) —issuance to the first investors; airdrops—free distribution of tokens to promote adoption; and mining or staking rewards - the incentives for network participants to secure and validate transactions.

Fiscal policy: taxation and spending to influence the economy, achieved (in a token economy) by all tokenholders voting on proposals for the project, including how it spends its available resources (with a view to generating more resources). To give a couple of examples:

- Bitcoin (BTC) has a fixed total supply of 21 million BTC. It is therefore disinflationary by design. Its distribution through mining rewards, which halve approximately every four years, slows the rate at which new BTC reaches the market.
- Ethereum (ETH) has no fixed total supply, but its issuance rate is controlled through network upgrades.

It was initially distributed through an ICO but ongoing distribution is through mining and staking. Holders of ETH use it to pay the costs of using the network, that is transaction fees (called "gas"), and as a medium of exchange within the Ethereum ecosystem.

Polkadot (DOT), the native currency of the Polkadot network which is another Layer 1 blockchain, had a supply that was initially uncapped, with a controlled inflation rate to incentivise network participation. Holders of DOT use it for governance, staking, and bonding (similar to staking, locked tokens perform a different technical function in the operation of the blockchain) within the Polkadot ecosystem.

We can see that tokens are not just economic instruments in the protocols that followed Bitcoin. They can be:

- a medium of exchange, that is used as money for transactions with other participants in the ecosystem;
- for access, that is to pay for using features or services in the ecosystem;
- for governance, that is as a credential to enable holders to vote on proposals in the ecosystem—as incentives, that is to reward users for specific actions.

Regardless of the economics, however, the success of a project is ultimately dependent on its utility and adoption.

Token design varies by project but some points are considered in relation to every project, by developers and by potential investors and users:

- successful projects have clear and compelling use cases for their tokens;
- fair and transparent distribution methods create trust, and therefore participation;
- properly designed incentives ensure that network participants are motivated to contribute positively;
- active and engaged communities, along with decentralised governance, create long-term sustainability;
- the mechanisms that create scarcity (e.g. token burns) and drive demand (e.g. utility) create value in the token.

This is a lot to take in. Read some old whitepapers to see how projects pitch their benefits. Read the community responses to see how potential investors and users reacted to the design.

There is an analogy I sometimes use when asked why projects do not just issue shares, like everyone else does in the global economy. Going back to the example about the difference between owning a share in BT plc and owning rights to use, and benefit from others' use of, and take decision in relation to, the cable in the ground … perhaps you will not be surprised at this point in the explanation to know that technologists will always choose the cable.

This means that Crypto is an experiment in economics as well as in finance. Economics is the science of decision-making. It considers choices that people and organisations make in the real world of limited resources. Economics developed by testing theory against practice, learning that actions not words reveal true preferences. This is what Crypto is also doing. Voting your tokens is the only signal that a tokenomics market needs. Feedback is given by use, and price is determined by use.

That is as far as we need to go following the logic of DeFi in an introduction book. We now swing to the opposite end of the spectrum of Crypto to discuss one of the biggest developments in Crypto in 2024. This has been the engagement of traditional financial products and markets with Crypto. It takes two forms.

First, we learnt that investors want exposure to Crypto. The bitcoin ETFs launched in 2024 very successfully. Tens of billions of dollars was invested.

Second, we saw the application to financial markets infrastructure of what has been learnt from the experiments of Crypto. The digital bonds issued by the EIB run on blockchain. The bonds are issued on chain. They give bondholders the same kind of economic rights as all previous EIB bond issues. But they use a different technical system. This is tokenisation.

Tokenisation is the process of converting real-world assets or rights into digital tokens on a blockchain. As we saw before, these real world assets include traditional financial assets: bonds, equities, money market funds, interests in investment funds, and anything else that markets can conceive since the technology is an enabling rather than a limiting factor. The main argument for the use of blockchains in TradFi is market efficiency.

These real world assets also include what the financial systems calls alternative investments: commodities, art, whisky and wine, classic cars, and so on. The main argument for the use of blockchains in alternatives is reducing barriers to entry by making it easier to trade and manage assets on platforms that can be made open to the widest range of investors. This is done by enabling fractional ownership, increased liquidity, and easier transferability (all related points, and the holy grail of the asset management industry—I will tell you a secret: in markets, every problem is a distribution problem.

Technology that powers up distribution is not the whole answer but it is second only to having products that people want.).

Blockchains are also used to establish the provenance of scarce assets: these could be diamonds (to prove they are not blood diamonds), food (to prove the "farm to fork" journey|), luxury goods (to prove that this handbag or that watch is not counterfeit). If you think about their distinctive characteristics: immutable, transparent, unhackable record-keeping systems, this will make sense. Blockchains are information verification machines.

Stablecoins solve the problem that we saw in chapter 1 caused by the volatility in Crypto prices. Stablecoins are cryptocurrencies pegged to stable assets like fiat currencies (initially the dollar—Americans think the dollar is stable because they have no FX risk in life, unless they choose to take some), providing price stability and reducing volatility. Stablecoins are widely used in the crypto ecosystem for trading, payments, and as a store of value.

Stablecoins are therefore cryptoassets pegged to another asset, currency, commodity, or financial instrument, maintaining a stable value over time, often on a 1:1 basis. These are other types—but the experiment of using only algorithms to generate stability did not work—they were not stable.

They also solve the oldest problem in TradFi: **settlement**. Settlement of any financial trade is a core problem in because it involves a complex, multi-step process that can take several days to complete:

- intermediaries, such as brokers, clearinghouses, and custodians, each need time for verification, reconciliation, and transfer of ownership—slow and expensive;
- clearinghouses remove credit risk, but only by making sure they are pre-funded by the paying party—ties up money;
- custodians manage the ownership records, often with multiple custodians if there are multiple jurisdictions—that is any cross-border transaction;
- Everyone has to check trade details, with discrepancies resolved before proceeding to settle the trade—slow and expensive;
- risk and compliance teams have to check everything else going on in the background—the who, what, why when and where of the trade—you get the idea by now;
- if all this is automated and the settlement currency is equivalent to US dollars and runs on a blockchain, it can be real time;
- this is what stablecoins can do—consistent with the experiment, they are not the only way. You will hear about tokenised deposits and others;
- the argument for this is that faster money creates more economic activity, a boost to global GDP—a big prize;

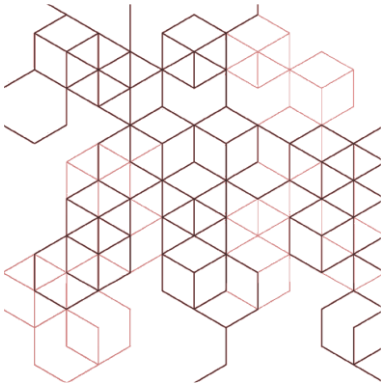
The argument against it is the concern that at this point the system has been taken over.

Hence, **Central Bank Digital Currencies** Central bank digital currencies (CBDCs) are digital fiat currencies issued by a country's central bank. Central banks see the benefit of digital money. They would just prefer that they control it, rather than groups of pseudonymous, rather anarchic, people gathering through the internet around the world to build their own economies, communities and ways to permit new social and commercial models.

This brings us full circle. We have started with Crypto as an alternative to banks and ended with central banks using blockchains.

I could have started with this point, but it makes the most sense to end with it. Why have I been capitalising Crypto throughout? Where I have it shows that I am implying it is a defined term. That is

deliberate: Crypto is a technology, a product, a kind of money, and so on. It interests mathematicians, investors, economists, sociologists, politicians, and more. It is also a community. I did not want to make it lower case and explain the particular usage each time. Most of the time I use it, I am talking about multiple contexts. So, I called it Crypto to reflect this and, because I am a lawyer, I can say that Crypto means, mutatis mutandis, all those things and, also, whatever you want it to mean.



Crypto, Parts 1 and 2

charles.kerrigan@cms-cmno.com

https://www.linkedin.com/in/charles-kerrigan/

Published in association with Sweet & Maxwell, a Thomson Reuters business.

Sweet & Maxwell is the publisher of *Crypto and Digital Assets Law and Regulation*, by Charles Kerrigan (2024, ISBN 9780414115101)