

A sceptic's guide to digital assets

Part 1: Blockchain - the foundation of digital finance

Digital assets represented c.£2.2tn as at 31 December 2025 and with Bitcoin having suffered losses of c.14% in 2026 to date (as at 21 April 2026), some might think that the role of digital assets has already peaked. At XPS, we think digital finance is only in its infancy and we expect the market to rapidly develop from here, but not necessarily in the way many might expect.

If you are baffled by the jargon and unconvinced by the rationale, but curious as to what has driven the growth of this market to such heights and where this might go, the Guide to Digital Assets series is for you.

In this series, we describe the digital finance industry in our own words, and explain our view for the potential opportunities and the pitfalls that we see in this hugely interesting new area of finance. We have covered cryptocurrency in [previous briefings](#) and maintain our view that it is not suitable for institutional investment. But digital assets represent so much more than cryptocurrency.

1

In part 1, we explain how the digital asset market works and how blockchain technology could pave the way for a faster, lower cost finance industry.

2

Part 2 will look at the important role for high quality Stablecoins and central bank digital currencies.

3

Part 3 will look at how Tokenisation could revolutionise real world investing.

Blockchain highlights:

- ▶ **A fundamentally transparent way to store information** - Everyone can see everything, leading to greater trust and reliability.
- ▶ **It will save transaction costs** - Traditional finance is very labour intensive which equates to costs that might be avoidable.
- ▶ **It will increase transaction speed** - Traditional settlement and reconciliation results in days of assets being tied up, meaning forgone interest earned and reduced agility.
- ▶ **Cryptocurrency requires blockchain, not the other way round** - Contrary to conventional wisdom, block chains do not require cryptocurrency in order to operate, they can operate with fiat currencies.



We are only just at the beginning of a broader digital asset market revolution, which will ultimately lead to credible, scalable investment opportunities. This is coming whether traditional finance likes it or not.

Simeon Willis, Chief Investment Officer, XPS

What is a digital asset?

In this paper, we use the term ‘**digital asset**’ to refer to assets that are created, recorded, and transferred using blockchain technology. A blockchain is a shared digital record that in theory everyone can trust because it is protected by strong encryption and is stored multiple times across many computers (a distributed network). People can prove ownership and make transactions without relying on a single bank or central authority maintaining a trusted record. With a public, permissionless blockchain, no single entity is responsible or has control of record keeping or processing transactions. This decentralised finance system is possible because of blockchain technology.

Traditional bank accounts, although accessed digitally, are not considered digital assets in this sense. The assets they hold are part of the traditional centralised financial system, managed across multiple systems that are operated by individual institutions in a regulated market.

We think of digital assets as a term that covers four main areas:

- **Cryptocurrencies:** Digital currency that exists on a bookkeeping system, independent of a central bank. Commonly used both as a medium of exchange and as a way to compensate the entities operating the blockchain.

Whilst having a role as payment systems on blockchain, in our view, cryptocurrencies such as Bitcoin and Ether do not meet sufficient criteria to have a role as an institutional investment.

- **Stablecoins:** A digital token whose value is pegged to a stable reference asset, such as fiat currencies like US dollars. The value of a stablecoin is underwritten by assets. The quality of the underlying assets varies hugely across different stablecoins.

Because traditional currencies like the US dollar do not exist directly on blockchains, stablecoins are a common medium of exchange when buying and selling other digital assets on a blockchain. However, not all stablecoins are up to the job.

- **Central Bank Digital Currencies:** A digital form of fiat currency, issued by a country’s central bank. Whilst not yet widely adopted, CBDCs will be backed solely by the authority and credibility of the issuing central bank, just like existing fiat currencies. CBDCs are not a subset of stablecoins as stablecoins are pegged to another asset whereas CBDCs are the asset. They therefore represent a distinct category of central bank money that carries the full guarantee of the state.

Central bank digital currencies could become a meaningful form of currency issuance and streamline central banking operations, but in many respects are likely to remain conceptually similar to existing fiat currencies.

- **Tokenisation:** The process of assigning ownership to any asset recorded in digital form. The underlying asset can be physical, digital, financial, or intangible. The units of the asset are ‘tokens’ that can be traded with the use of blockchain. Traditional assets like equities and bonds wrapped in a digital token are known as Real World Asset (RWA) tokens. They have scope to dramatically change how we invest in these assets in the future through faster transactions with lower costs. Tokens have had a lot of press in relation to NFTs or non-fungible tokens. These quirky assets have both increased the profile of tokens whilst at the same time undermined the credibility, given their tendency to be associated with overpriced novelty content of negligible value.

However, tokenisation is the unsung hero and is an area that is likely to grow disproportionately, thereby radically changing the way we invest in real world assets such as shares, bonds and private market assets with cheaper, faster transactions and greater flexibility.

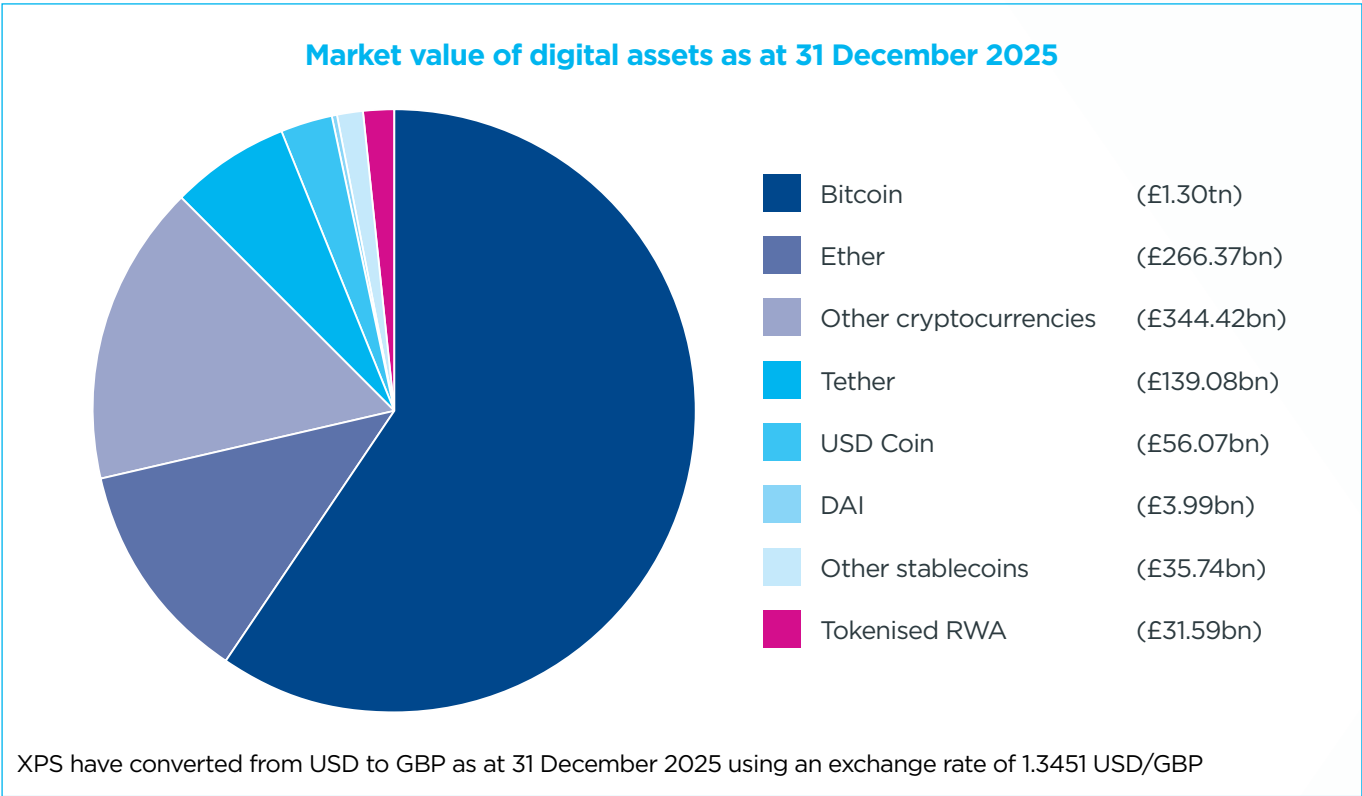
Whilst we are setting the scene, a fifth area which isn’t technically an asset but does have an important role to play in digital finance is smart contracts. A smart contract is a program stored on blockchain that automatically executes pre-agreed actions subject to certain conditions being met. For instance, a subscription agreement between an online service provider and a user can be recorded on a smart contract such that the user is only given access to the service if they have paid their subscription. The smart contract can monitor this through time and access would be revoked if the subscription is not paid.



Size of the digital asset market

The market for digital assets, whilst already substantial at **c.£2.18tn (equates to £2,180bn)** as at **31 December 2025**, is still nascent. The adoption and market of digital assets has been accelerating across both retail and institutional segments, driven by innovations in blockchain infrastructure, decentralised finance, and tokenisation.

As at 31 December 2025, the vast majority of value invested in digital assets is invested in cryptocurrency accounting for **c.£1.91tn**. Second to that are stablecoins, accounting for **c.£235bn**. Real world asset tokens account for a small portion of the current market, currently estimated to be less than **c.£32bn**, but it is an area that is likely to grow exponentially.



Source: TradingView for Bitcoin, Ether, Other cryptocurrencies, Tether, USD Coin, DAI, and Other stablecoins.
The Block for Tokenized RWA.



Institutional investors need to exercise extreme caution within the digital markets. This is the new wild west. There will be big winners and even bigger losers.

Whilst the vast majority of current digital assets should be given a wide berth, there are pockets of genius which I am convinced will revolutionise finance and grow to dominate their sectors in the coming years.



Simeon Willis
Chief Investment Officer

Blockchain technology

Digital assets work using a technology called blockchain. Think of blockchain as an online book that keeps track of all transactions.

The name blockchain arises from the way that transactions are stored as a list of transactions together in a 'block'. The contents of the block are processed tokenised to create a digital fingerprint that is specific to that set of transactions known as a cryptographic hash. This fingerprint is stored when the block is solved and corresponds precisely to the information in the block such that a slight change to the transactions would produce a different fingerprint. This means that it is easy to see if transactions are changed after the event, as the stored fingerprint and the transactions will not match. The block, including its cryptographic hash, is then joined in a chronological order to the next block in a chain, forming an evolving record through time as more transactions are processed.

Transparency

A public, permissionless blockchain is open for everyone to see, but the identity of each account owner is not recorded on the blockchain. This is fundamentally different to traditional banking where accounts are secret and the account holder is known to the Bank specifically in relation to the account. Banks are required to undertake Know Your Client (KYC) checks to ensure that their customers are real people, are not operating fraudulently and are not using the bank as a means to launder money. While the base blockchain protocol itself does not perform KYC checks, regulated service providers that allow access to digital assets are often required to.

Public and private keys

In a blockchain system, each account has a public key and a private key. The public key acts like an address or username that you can share with others to receive funds. The private key is like a password that gives you control over the account and allows you to send transactions, so it must be kept secure.

All transactions linked to a public key are visible on the blockchain, but personal identities are not held on the system. This setup makes blockchain clear and open while offering scope to keep people's identities private. However, it is important to note that anonymity is not guaranteed. For instance, if you give your public key to someone so they can pay you, they will be able to see what is in that account. Therefore, people often take steps to provide themselves with anonymity by having several accounts and moving money between them. However, this is all still observable externally. Most common privacy solutions rely on intermediaries or off chain services, which reintroduce elements similar to traditional finance; others use on chain cryptography to improve privacy without leaving the blockchain environment.

The benefit of blockchain technology

Despite appearances of high levels of digitisation, traditional financial markets remain extensively dependent on intermediaries such as brokers and custodians, with lots of manual checks and reconciliations. This slows transaction processing down and adds cost. The concept of blockchain cuts out many of these steps where all participants are interacting on one trusted system. For institutional investors, this holds the promise of faster capital deployment and reallocation, with lower transaction costs and reduced risk of error.

On ramping and off ramping: the merits of staying 'on-chain'

The efficiency gains that blockchain technology offers depends on the extent to which transactions remain 'on-chain'. What this means is that if you invest in an asset via a blockchain from a traditional bank account, the act of going 'on chain' or 'on ramping' typically incurs the similar frictional costs and delays as transacting in traditional way. It is only if you stay on the blockchain that you start to benefit from the efficiency savings by cutting traditional finance out of the equation.

Once on-chain, settlement occurs directly between parties within the blockchain system, without the need to exit into traditional financial infrastructure. As with on-ramping, efficiency is lost when you off-ramp back to a traditional bank account. Once transactions leave the chain, intermediaries such as brokers, custodians, or clearing houses must be involved, reintroducing delays, costs, and reconciliation processes.

In a nutshell: By streamlining processes that have traditionally required extensive human involvement, blockchain technology has the potential to transform financial markets into more efficient and transparent systems. As above, we note that anonymity is not guaranteed but there are methods used to try and achieve this if desired.

Programmable blockchains vs non-programmable blockchains

Different blockchains are built with different purposes in mind, and this shapes the kinds of digital assets they can support. Some blockchains are single-purpose, built around one asset, while others are multi-purpose ecosystems that enable diverse financial instruments to operate together.

Programmable blockchains have scope to host many different assets which can co-exist and trade side by side, ranging from stablecoins to tokenised securities, all using the same underlying infrastructure. These platforms allow developers to create tokens and smart contracts. Stablecoins such as USD Coin (USDC) or Tether (USDT) are typically issued on programmable blockchains like Ethereum, Solana, or Polygon.

By contrast, non-programmable blockchains, also known as single payment blockchains only offer one function. The Bitcoin blockchain was originally designed only to support Bitcoin itself. It does not natively allow for complex tokens, smart contracts, or stablecoins. While additional layers and systems have been developed to extend Bitcoin's functionality to be able to support assets other than Bitcoin, these solutions are not widely adopted and depend on extra infrastructure beyond Bitcoin's base layer. In short, Bitcoin's blockchain is highly secure but limited in flexibility.

Degrees of decentralisation

A defining feature of digital assets is their **varying degrees of decentralisation**.

At one end of the spectrum, crypto assets like Bitcoin operate without any central authority, relying entirely on peer-to-peer networks and the **Proof of Work (PoW)** consensus mechanism.

Back to the classroom: how blocks are solved

Proof of work - PoW

This mechanism can be illustrated with the following analogy. Imagine a teacher gives a class a very hard maths problem. Every student races to solve it, burning lots of energy and effort. The first student to get the correct answer wins a prize and gets to write the solution on the board. This is how Bitcoin works: "miners" compete to solve puzzles, and the winner adds the next block to the chain. The reward is an allocation of Bitcoin. All other miners receive nothing. It's secure, but it uses a huge amount of energy because everyone is racing at once, with duplicated effort.

Proof of stake - PoS

Platforms such as **Ethereum** use **Proof of Stake (PoS)**. To illustrate how this mechanism works, imagine now that the teacher picks one student to solve the problem, based on how much they've 'invested' in the class (which is equivalent to how many tokens they've staked). A smaller group of other students then check that student's work to make sure it's correct. If it is, the solution goes on the board.

This is how PoS works: validators are chosen to propose blocks, and others confirm them. It's far more efficient because not everyone is racing at once with less duplication of effort, but the system still stays secure through checks and balances.

Some critics argue that PoS can be more prone to concentration of control among large stakeholders, while others point out that PoW mining is also highly concentrated. PoS and PoW differ in their decentralisation trade offs.



The Bitcoin blockchain only really does one thing - Bitcoin, whereas other blockchains have far more varied applications in broader finance including tokens and smart contracts.



Savvas Ioannides
Investment Consultant

Paying for the blockchain's existence

As any blockchain requires processing by nodes in order to operate, this processing needs to be paid for.

Blockchains could have stopped at introducing a new means for recording transactions, but given the advanced nature of the technology, there was scope to go further and create a financial model which was not dependent on any existing currencies. A truly independent financial system. This has proved to be a highly desirable aspect of blockchain which has undoubtedly contributed to its stratospheric rise in popularity.

Consequently, blockchains typically introduce their own native digital currencies, such as Bitcoin for the Bitcoin blockchain or Ether for the Ethereum blockchain, which serve as rewards for miners or validators who contribute computing power and maintain the integrity of the network. In addition to these rewards, users pay transaction fees, commonly referred to as “gas fees”, when initiating transactions or executing smart contracts. These fees compensate validators for processing and securing transactions. This mechanism ensures that participants are incentivised to secure and operate the network as long as the remuneration is sufficient to justify the effort involved.

One confusing aspect of blockchain is that this feature is not strictly necessary. Blockchain is primarily about the technology to record transactions, not about how the system is funded. Cryptocurrency is made possible by blockchain, but blockchain can operate with fiat currency payment for validators as well, albeit this introduces inefficiencies of traditional finance in a similar way that on and off ramping reintroduces inefficiencies for investing on the blockchain.

Non-crypto based blockchains include Hyperledger Fabric and Quorum.

Permissioned vs permissionless network

Blockchains come in two main types: permissionless and permissioned. A **permissionless** blockchain, like Bitcoin or Ethereum, is open to anyone. They are open networks where anyone can join, send transactions, validate transactions, and create assets. This makes the system very transparent and decentralised, but it can also bring risks, since anonymous users may try to cheat or overload the system.

A **permissioned** blockchain, on the other hand, only allows approved members to take part. Because access is restricted, it is easier to govern, enforce compliance on, and optimise for performance, though it may rely more heavily on trust in the operating institutions, and is less open to the public.

These differences matter for investors. Some may prefer the safety and control of permissioned blockchains, while others are drawn to the openness and global reach of permissionless ones. In practice, the type of blockchain chosen determines not only the level of decentralisation but also the balance between risk, trust, and access to digital asset markets.

Limitations of blockchain

Blockchain is a powerful tool behind digital assets, but it's not without its problems. People often claim blockchain prevents fraud and solves all financial issues, but that's not true. Like any financial system, it can have weaknesses in its code that might be exploited. Since most people can't check the security of a blockchain themselves, they rely on audits or trust the platform's reputation.

Blockchains are complex and often need brokers, custodians, and other intermediaries, to connect with banks and transfer money. This brings back risks like hacking or fraud, which are present in regular finance.

Additionally, using blockchain requires handling private keys securely. In pure self-custody models, losing these keys means losing access to your assets forever, unlike banks where you can recover access with identity checks, as no identities exist. This shows that while blockchain offers a new way to do finance, it still has challenges similar to traditional systems.

Regulation and innovation

As digital assets continue to emerge in the financial landscape, regulatory oversight is essential to ensure innovation proceeds responsibly and securely.

The UK Financial Conduct Authority (FCA), on 17 September 2025, published a Consultation Paper which sets out how existing FCA Handbook rules will apply to firms conducting regulated crypto-asset activities. This consultation is part of the UK's broader effort to build a competitive and sustainable crypto-asset sector. These efforts signal a commitment to balancing innovation with investor protection, by clarifying rules around custody, disclosure, and market integrity.

In parallel, the proposed **Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS Act)**, was signed into law in July 2025. It represents the first comprehensive federal framework for regulating payment stablecoins in the United States. It seeks to create a cohesive regulatory infrastructure that enables digital assets to integrate into traditional financial systems. This includes provisions for standardised reporting, interoperability between platforms, and legal recognition of tokenised ownership.

Together, these measures address key risks such as fraud, asset misappropriation, and operational failures, while also laying the groundwork for insurance markets and investor safeguards tailored to digital finance.

Conclusion and future outlook

Digital assets represent a rapidly evolving sector in finance. Though still in their infancy, they promise substantial transformation. Institutional adoption remains nascent, yet the pace of advancement suggests significant potential for reshaping finance, supported by emerging regulations.

Looking ahead, digital assets promise an exciting future filled with innovation and potential. As regulatory clarity improves and technologies mature, these assets are set to become integral to global finance, unlocking new opportunities for growth and transformation.

Find out more

For further information, please get in touch with Savvas Ioannides, Simeon Willis or speak to your usual XPS contact.



Savvas Ioannides
Investment Consultant



savvas.ioannides@
xpsgroup.com



Simeon Willis
Chief Investment Officer



simeon.willis@
xpsgroup.com



xpsgroup

Important information: Please note the information and opinions expressed herein do not take into account the circumstances of individual investors and accordingly may not be representative of the circumstances affecting your portfolio. This note, and the work undertaken to produce it, is compliant with TAS 100, set by the Financial Reporting Council. No other TASs apply. The note has been written on the basis that decisions will not be based on its contents. Appropriate advice should be obtained before any decisions are made. The information expressed is provided in good faith and has been prepared using sources considered to be reasonable and appropriate. While information from third parties is believed to be reliable, no representations, guarantees or warranties are made as to the accuracy of information presented, and no responsibility or liability can be accepted for any error, omission or inaccuracy in respect of this. This document may also include our views and expectations, which cannot be taken as fact. The value of investments and the income from them can go down as well as up as a result of market and currency fluctuations and investors may not get back the amount invested. Past performance is not necessarily a guide to future returns. The views set out in this document are intentionally broad market views and are not intended to constitute investment advice as they do not take into account any client's particular circumstances.

Please note that all material produced by XPS Investment is directed at, and intended solely for the consideration of, professional clients within the meaning of the Financial Services and Markets Act 2000 (FSMA). Retail or other clients must not place any reliance upon the contents.

This document should not be distributed to any third parties and is not intended to, and must not be, relied upon by them. Unauthorised copying of this document is prohibited.

© XPS Group. XPS Pensions Consulting Limited, Registered No. 2459442. XPS Investment Limited, Registered No. 6242672. XPS Pensions Limited, Registered No. 3842603. XPS Administration Limited, Registered No. 9428346. XPS Pensions (RL) Limited, Registered No. 5817049. XPS Pensions (Trigon) Limited, Registered No. 12085392. Penfida Limited, Registered No. 8020393. Polaris Actuaries and Consultants Ltd, Registered No. 9640309. All registered at: Phoenix House, 1 Station Hill, Reading, RG1 1NB.

XPS Investment Limited is authorised and regulated by the Financial Conduct Authority for investment and general insurance business (FCA Register No. 528774).

This communication is based on our understanding of the position as at the date shown. It should not be relied upon for detailed advice or taken as an authoritative statement of the law.

Glossary

Given the complexity of the digital assets space, which is unfamiliar to many, we have produced a glossary with a definition of each term in a normal and simplified version.

Term	Definition	Simplified Definition
Bitcoin	The first blockchain based currency, introduced in 2009 by the pseudonymous creator Satoshi Nakamoto.	The first and biggest cryptocurrency, created in 2009.
Blockchain	A decentralised ledger system that is shared across a network, storing transactions in order and making them visible to all participants, while keeping the accounts involved anonymous.	A shared online bookkeeping record, which everyone can see and which no single person controls.
Consensus	The collective agreement among blockchain participants on the accuracy and validity of recorded transactions.	Agreement among participants in the network about the blockchain's state.
Consensus Algorithm	A set of rules that allow blockchain participants to agree on the validity of transactions and the state of the ledger.	Rules that help blockchain users agree on what's valid.
Cryptocurrency	A form of digital currency secured by cryptographic methods, designed to function without reliance on a central authority.	Digital money that works without banks or any other central authority.
Cryptography	The science of encoding information to protect data and secure communications, essential for blockchain systems.	Using maths to keep information safe and private.
Decentralisation	The distribution of authority and control across multiple participants rather than a single governing body.	Spreading control across many people instead of one authority.
Ethereum	A blockchain network that supports programmable contracts and decentralised applications through its native token, Ether.	A blockchain that lets people build apps and smart contracts.
Gas fee	A payment made to compensate for the computational effort required to process transactions or smart contracts on Ethereum.	A payment to run transactions or contracts on Ethereum.
ICO (Initial Coin Offering)	A fundraising mechanism where new blockchain projects sell tokens to investors in exchange for established cryptocurrencies.	Selling new tokens to raise money for a project.
Ledger	The blockchain's continuously updated record of all transactions, accessible to every participant in the network.	The blockchain's record of all transactions.
Mining	The computational process of verifying blockchain transactions and adding them to the ledger, often rewarded with new coins.	Using computers to check transactions and add them to the blockchain.
Native token	The primary cryptocurrency of a blockchain, typically used to pay fees and sometimes to support governance (e.g., Bitcoin or Ether).	The main coin of a blockchain (like Bitcoin or Ether).
Node	A computer that connects to a blockchain network, helping to validate, store, and distribute transaction data.	A computer that helps run the blockchain network.

Term	Definition	Simplified Definition
On chain	Any activity or transaction that is permanently recorded on the blockchain itself.	Activity that happens directly on the blockchain.
On ramping / Off ramping	On ramping: Converting fiat currency into digital assets. Off ramping: Exchanging digital assets back into fiat currency.	On ramping: Turning cash into crypto. Off ramping: Turning crypto back into cash.
Permissioned blockchain	A blockchain network where access is restricted to approved participants, often used in enterprise contexts.	A blockchain where only approved people can join.
Permissionless blockchain	A blockchain network open to anyone, allowing unrestricted participation in validation and transactions.	A blockchain open to anyone, no approval needed.
Private key	A confidential string of characters that grants control over cryptocurrency funds linked to a blockchain address.	A secret code that lets you access and spend your crypto.
Proof of Work (PoW)	A consensus method where participants solve complex mathematical problems to validate transactions and secure the network.	A system where people use their computers to solve puzzles to confirm transactions. Whoever solves it first gets rewarded.
Proof of Stake (PoS)	A consensus method where validators are chosen based on the amount of cryptocurrency they commit as collateral.	A system where people lock up their tokens to help confirm transactions. Whoever offers to lock up the most tokens will be the validator.
Public key	A cryptographic identifier that can be shared openly to receive funds.	A code you share so others can send you crypto.
Smart contract	Computer code stored on a blockchain that automatically executes agreements when predefined conditions are met, removing the need for external systems to enforce an agreement.	Code on a blockchain that runs automatically when conditions are met.
Token	A digital unit created on a blockchain that can represent value, ownership, or rights depending on its design.	A digital voucher that exists on a blockchain. The voucher can be for many different things: money, ownership of something, or even a right to vote.
Wallet	Software or hardware that manages blockchain addresses and keys, enabling users to store and transact cryptocurrencies.	An app or tool to store and use cryptocurrencies.