Aaro Capital

Introductory Guide to Cryptoassets and DLT

September 2023

Aaro Capital

Disclaimer

Aaro Capital is the trading name of Aaro Capital Limited (“Aaro”), a private limited company, registered in England and Wales with number 11419585, whose registered office is at 5th Floor 10-12 Eastcheap, London, United Kingdom, EC3M 1AJ.Aaro is not authorised or regulated by the Financial Conduct Authority (“FCA“) or any other financial regulator.

The material provided in this guide is being provided for general informational purposes. Aaro does not provide, and does not hold itself out as providing, investment advice and the information provided in this guide should not be relied upon or form the basis of any investment decision nor for the potential suitability of any particular investment. The figures shown in this presentation refer to the past or are provided as examples only. Past performance is not reliable indicator of future results.

This guide may contain information about cryptoassets. Cryptoassets are at a developmental stage and anyone thinking about investing into these types of assets should be cautious and take appropriate advice in relation to the risks associated with these assets including (without limitation) volatility, total capital loss, and lack of regulation over certain market participants. While the directors of Aaro have used their reasonable endeavours to ensure the accuracy of the information contained in this guide, neither Aaro Capital Limited nor its directors give any warranty or guarantee as to the accuracy and completeness of such information.

Please be sure to consult your own appropriately qualified financial advisor when making decisions regarding your own investments.

Aaro Capital

Introductory Guide to Cryptoassets and DLT

Blockchain technology (also known as DLT) and crypto are now widely regarded as an inevitable part of finance's future. Multiple authoritative sources estimate that Blockchain technology will deliver Trillions of Dollars of value by 2030. The numbers and implications of this technology are tremendous[1,2,3,4]. Fidelity found that three quarters of institutional investors plan to buy or invest in cryptoassets in the future.[5] This is a powerful growth story and a great long-term strategic opportunity.

The Eureka moment which led to crypto as we know it today happened in the depths of the 2008 Global Financial Crisis, with the release of the Bitcoin white paper by pseudonymous programmer Satoshi Nakamoto.[6] Bitcoin was not, however, the first attempt at a purely digital and decentralised currency. There were many attempts to design purely electronic money from the early '90s onwards, but they all failed to gain traction.[7] Back then, the term "crypto" was usually associated with the branch of computer science called cryptography. This technology is used to secure all data online, from online banking to different types of online commerce.

Only after the emergence of Bitcoin and the subsequent influx of new digital currencies was the term crypto popularised in reference to cryptocurrencies, which were digital only currencies enabled by novel application of cryptography. Even though the first generation of digital only currencies from the pre-Bitcoin era also used cryptography, an essential component to enable them to function successfully was missing. Bitcoin and most of its alternatives, have one thing in common that previously was not available - Blockchain technology. Together with clever economic design, blockchain made possible the first digital only currency with no central controller.

Deployment of blockchain methodologies allows Bitcoin and other cryptocurrencies to operate in a distributed manner and to remove the unnecessary middlemen. Instead of a central authority keeping control of the records of all transactions in a database they control, the transaction data in Bitcoin are stored on its users' computers, also called nodes, connected around the world. Anybody can join the network, download all the data and validate new transactions. Blockchain is a form of distributed database.

---

[1] For more information, see: https://www.pwc.com/gx/en/industries/technology/publications/blockchain-report-transform-business-economy.html.
[2] For more information, see: https://www.pwc.com/gx/en/industries/technology/publications/blockchain-report-transform-business-economy.html.
[3] For more information, see: https://www.ledgerinsights.com/ihs-market-blockchain-forecast-2-trillion/.
[4] For more information, see: https://www.weforum.org/agenda/2018/09/blockchain-set-to-increase-global-trade-by-1-trillion.
[5] For more information, see: https://www.fidelitydigitalassets.com/sites/default/files/documents/2022_Institutional_Investor_Digital_Assets_Study.pdf.
[6] For more information, see: https://bitcoin.org/bitcoin.pdf.
[7] For an overview of the key predecessors to bitcoin, see: https://en.aaro.capital/Article?ID=Before%20Bitcoin:%20A%20History%20of%20Digital%20Currencies.

Figure 1: Centralised Databases vs Distributed Databases such as Blockchain

Source: Aaro Capital Research

As the transaction data on a node are batched up into collections, called blocks, which are cryptographically linked (or chained) together, the resultant data structure resembles a chain of blocks and thus was named blockchain. The copy of a blockchain is distributed over the network of thousands of nodes, that synchronise and actualise it in real time.

Figure 2: A Chain of Data Blocks, or Blockchain

Source: Aaro Capital Research

As the whole crypto space evolved at breakneck speed, a lot of effort went into researching and improving different technical and economic aspects of blockchain technology. As discoveries and improvements were made, the “blockchain” term was no longer able to capture the full breadth of the technology and a need for a broader term emerged.

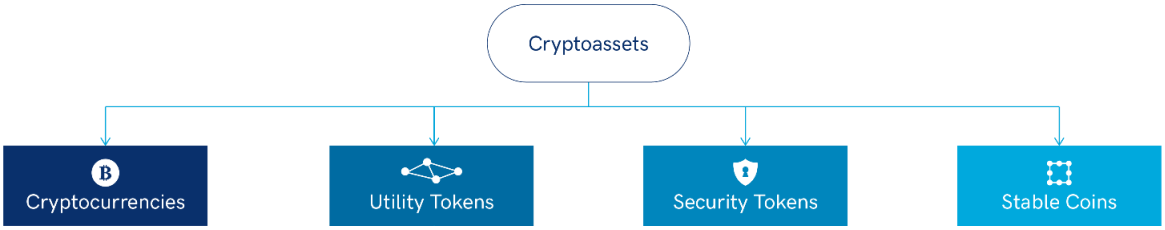
This is where DLT, or Distributed Ledger Technology, comes into play. As blockchain technology has been tweaked and implemented in various applications and use cases, some of the modifications to it abandoned the idea of the particular data structure where transactions are stored in a chain of blocks. Thus, the term “DLT” was coined to refer to all technologies that utilise a distributed database of records, but do not necessarily use blockchain per se.

Importantly, DLT shares the same core benefits as blockchain:

1. Elimination of a central authority
2. Distributed architecture, making it most resilient to outside attacks
3. Harder to tamper with data
4. More transparency and easily auditable
5. Greater control and democracy for users

Similar to the evolution of blockchain into DLT, the technology has evolved beyond just cryptocurrencies like Bitcoin. A new term has been coined, cryptoassets. This covers the wide range of assets which live digitally on the distributed ledger.

Figure 3: The Key Types of Cryptoassets



Source: Aaro Capital Research

Cryptoassets and DLT go hand in hand. While DLT is the technological innovation, cryptoassets are the economic innovation. While cryptocurrencies remain the application for DLT which receives the most publicity, the implications of this innovation go far beyond just a digital currency. The core proposition of cryptocurrencies is not to be used in the same way as a fiat currency is. It is a different form of money.

Cryptocurrencies enable something which was not previously possible, which is effective decentralised governance through clever economic design. In the absence of a centralised authority who can unilaterally enforce "the rules", a cryptocurrency's design must ensure that it is profitable for participants to add value to a crypto platform and also that it is very expensive to undermine it. A cryptocurrency's core role, like traditional money, is to incentivise economic activity. Crypto is the next evolution of a more inclusive and, ultimately democratic economy.

This decentralisation allows the technology to solve three key fundamental economic issues:[8]

1. The disintermediation of trusted intermediaries, helping cut out expensive middlemen who may also gain excessive market power. Think of how transformative this will be in the financial sector, where a trusted intermediary, might, be, for example, a bank.
2. The disintermediation of the hold-up problem, enabling multiple companies to undertake investments together with a higher degree of confidence in mutually beneficial projects, without fearing that the "rules of the game" could be changed unilaterally by a network owner. Granular reorganisation of innovation and production network around DLT is already happening.
3. The disintermediation of network monopolies, providing a potential solution to the competition concerns regulators and legislators globally have around the tech giants, who benefit massively from the network effects of their platforms. The shared ownership of the network can also generate a virtuous cycle of growth, using tokens to incentivise participation and contribution to the network.

Looking at the bigger picture, cryptoassets and DLT are key to the fourth Industrial Revolution and its use cases are intertwined with technologies such as the Internet of Things, Big Data and Artificial Intelligence. Crypto is a next-generation, value-based internet. As HTTP and HTML are the platform of the World Wide Web, Ethereum and other crypto networks are the platforms of Web 3.0. Web 3.0 is the integration of Industrial Revolution 4.0 technologies and native value management, for example, internal native payments, into the internet. So far, in finance, the financial payment rails have been kept separate from the Web, but in a digital world where data, money and value are so intertwined, this separation makes less and less sense. In the same way that the Web today enables many services, software built on Web 3.0 is already providing a wide range of valuable services to consumers. Decentralised crypto ecosystems are an evolution of traditional companies and cooperatives. Tokenisation is the next evolution of securitisation. Integrated stablecoin payments are the next evolution of

[8] For more information, see: https://en.aaro.capital/Download.aspx?ID=2e6e0048-f80d-4c95-89e8-e7f5b2869306&inline=true.

digital payments. Decentralised finance is the next evolution of many traditional financial services, from payment processing to trading infrastructure to borrowing and lending.

This technology has the potential to disrupt virtually every industry and has applications throughout many different value chains. Key areas for disruption are finance, insurance, healthcare, supply chains and digital identity. Governments, banks, and other large corporations are now getting behind both cryptoassets and DLT. Many established companies, ranging from Amazon to JP Morgan to Paypal, are now involved.

McKinsey has identified over 90 use cases across 14 industries. For example, HSBC has put $10B of Private Placements on the Blockchain. The HSBC platform, known as Digital Vault, gives investors real-time access to records of securities bought in private markets. This has digitised the paper-based records of private placements. HSBC has also been settling $15 – 20 billion of transactions daily in internal FX trades on blockchain, cutting trading costs by 25%. In early 2023, Goldman Sachs announced that the bank's new Digital Asset Platform (GS DAPTM), in which it can tokenize traditional financial products in order to increase transaction efficiency and liquidity, is now live. ING has launched its blockchain-based trade finance platform, Contour, to simplify letters of credit, reducing the amount of time needed to process them from 5 to 10 days to under 24 hours. Franklin Templeton now offer various digital asset products; a tokenized and onchain fund (FOBXX), a Private Equity vehicle, and liquid digital asset Hedge Fund. The Franklin OnChain U.S. Government Money Fund (FOBXX), the first U.S.-registered mutual fund to use a public blockchain to process transactions and record share ownership, is now supported on the Polygon blockchain. Powered by blockchain, mutual funds can be traded 24/7/365 with instant trade settlement and execution.

It is also important to remember that this is an early-stage technology, as the internet was in the early 1990s. When, however, the infrastructure matures and it becomes more user friendly, there is clear economic value to be generated by decentralisation, enabled via cryptoassets and DLT. There is also the potential for significant returns, especially if this is based on a disciplined, risk controlled and diversified investment approach that blends the range of opportunities with the different strategies available to explore them.

Crypto Jargon Glossary

#

51% Attack

A situation where a single party, or a coordinating group of parties, has over 50% of decision-making power on a crypto Network, enough to unilaterally determine which Transactions are approved and which are not. This situation violates the basic principle of how decentralised Networks are secured, in that no single party controls a large proportion of the Network to be able to abuse their power. In decentralised Networks, there is no central authority to control things, and so a 51% attack is a major security concern for all other users. This is because this can lead to data integrity issues, such as Double-Spend Attacks.

A

Address

In crypto, the term Address refers to a form of Public Key through which one can receive Cryptoassets. Therefore, it can be thought of as a bank account routing number for Cryptoassets. It may also refer to the location of a Smart Contract in some Networks.

Airdrop

A way to distribute newly created Cryptoassets as a donation to the Wallets of users on a crypto Network, according to predetermined rules. For example, users of the Ethereum Network might get Tokens Airdropped into their Ethereum Wallets, for a new game launching on the Network. Airdrops are usually a marketing technique used to increase awareness and popularity of the project or Token.

Altcoin

Typically refers to an alternative Cryptocurrency to bitcoin (BTC).

B

Bitcoin (Network)

The first decentralised and distributed crypto Network, invented in 2008 by pseudonymous creator Satoshi Nakamoto. It is software which provides a decentralised and distributed Internet Network using Blockchain technology and is an adjacent Internet network to the World Wide Web. Transaction data on the Network is stored on a public Ledger that is distributed across a Network of thousands of Nodes globally. The Network is secured by Miners, ensuring that assets on the Network are transferable, without the need for a central intermediary to coordinate and manage who owns what.

bitcoin ("BTC")

The namesake native Cryptocurrency of the Bitcoin Network. The Network is designed to issue, maintain and transfer units of bitcoin, the cryptocurrency between and on behalf of parties.

Blockchain

The most common type of Distributed Ledger Technology used by many crypto Networks. Data on such a Network is stored within discrete Blocks, which are then cryptographically linked together, forming an auditable chain of Blocks, hence the name Blockchain.

Block

A single unit of a Blockchain in which data is stored. Blocks are produced by Validators and are targeted to be produced at regular time intervals e.g. every 10

	minutes for the Bitcoin Network. Blocks have a capped capacity in terms of the amount of data each can hold.
Block Height	The number of a given Block within its Blockchain, counting from the Genesis Block. For a Block which is the 100th Block in a Blockchain, its Block Height is 100. As time in Blockchain is measured by Blocks, the Block Height, in a sense, captures the age of that Block.
Block Reward	The Cryptocurrency which a Validator receives for creating a new Block. This payment serves as a way to incentivise parties to become Validators, and to invest the required resources to do so e.g. electricity and hardware. Block Rewards include Transaction Fees paid by Network users and newly minted issuance known as the Block Subsidy.
Block Time	The time that it takes to generate a new Block on a Blockchain. For Bitcoin, this is targeted to 10 minutes. In other crypto Networks, it can be less.
Block Subsidy	The newly minted issuance of Cryptocurrency which a Validator credits to themselves within blocks they publish. Other Nodes will verify that the Block Subsidy meets the rules of the Protocol before accepting it.

C

Central Bank Digital Currency ("CBDC")	A form of digital currency, similar to the digital bank accounts and digital money transfers carried out by commercial banks, except that the bank accounts and money are held directly with the central bank. The central bank issues a digital form of its currency units and provides the electronic storage and payment systems for this money. It is possible for commercial banks and payment services to be either bypassed or integrated. Many Central Banks have ongoing research projects while a minority, including the People's Bank of China have already launched early production versions.
Coin	Refers to a crypto Network's unit of account, but the term is also often used informally to refer to the Network itself. This excludes other forms of Cryptoassets such as Tokens, which do not have their own native Network. For example, Ether, which is the native Cryptocurrency of the Ethereum Network and is core to its functionality, is a Coin. Tether, which also sits on the Ethereum Network, is not native to it, but was added to it at a later date by a third party, is not a Coin, but a Token.
Cold Wallet	A type of crypto Wallet which stores its Private Keys offline, away from the Internet. Offline, Private Keys cannot be accessed remotely through a cyberattack and so cannot be used by an attacker to control Cryptoassets which belong to the Wallet. Cold Wallets are considered the safest way to store Private Keys. Typically, Cold Wallets are in the form of specialised personal hardware devices, similar to a USB memory stick, but can even just be a piece of paper with a Private Key printed on it.
Cryptoasset	Broader term used for Cryptocurrencies, as well as other kinds of Digital Assets that exist on Distributed Ledgers. All these assets rely on cryptographic technology for their cyber security, hence the name Cryptoasset. There is a wide spectrum of different Cryptoassets, differing in their functionality and use, from a means of payment to concert tickets to digital securities.

Cryptoeconomics	A branch of economics that studies the incentives of parties using Cryptoassets in decentralised Peer-to-Peer crypto Networks. With no central authority to control things and enforce the rules, crypto Networks have to rely instead on incentivising participants to act in socially beneficial ways, to enable the ecosystem to operate as intended. Most specifically, it attempts to alleviate the need for trust by making malicious behaviour more costly than the benefits of it.
Cryptocurrency	A decentralised, digital currency relying on cryptographic technology for cyber security, operating on a Distributed Ledger, with no central authority. Such a currency can operate without the need of an intermediary like a bank or government. A Cryptocurrency can carry monetary value when there is trust and usefulness in the distributed Network on which it exists. A Cryptocurrency is also known as a Coin. The most popular Cryptocurrency is bitcoin. Others include Ether, bitcoin cash and Dogecoin.
Cryptography	The field of mathematics concerned with data Encryption. Cryptography empowers not only cryptocurrencies but also many commonly used technologies on the Internet which facilitate private communication and message authentication over the public Internet. This technology allows for the storage or transfer of data in ways that are hard for an external party to decipher and manipulate, keeping it secret, authentic and tamper evident, making unauthorised changes visible. This technology is used to secure most data online, from online banking to e-commerce.
Cyberattack	An unauthorised action via the Internet to harm computer services or steal information. This could include the guessing of passwords to take a computer and install surveillance software; steal corporate secrets; or Private Keys to crypto asset holdings.

D

Decentralised Application ("DApp")	A software program operating on top of a decentralised Network such as Ethereum, typically utilising Smart Contracts. These are typically designed in a way that does not require human interaction and thus can operate autonomously. Unlike traditional applications that operate on a single server, DApps run simultaneously on many copies of the Distributed Ledger. Therefore, no single entity has control over them and they cannot be stopped or censored.
Decentralised Autonomous Organisation ("DAO")	A set of decentralised Smart Contracts creating a virtual organisation, governed by its "shareholders" in a decentralised manner. DAOs are typically not a legal entity. Instead of having company shares, DAOs typically feature a Governance Token. Token holders can vote on how to manage the DAO, similar to the way in which shareholders do so for companies (for example, approving financial budget proposals).
Decentralised Finance ("DeFi")	Types of Decentralised Applications providing financial services. This can include decentralised exchanges or decentralised borrowing and lending platforms. This allows for permissionless and potentially more efficient and cost-effective alternatives to traditional financial services, making them available to companies and people all over the world.
Digital Asset	Usually used interchangeably with the term 51% Attack, but traditionally used to describe anything which is purely digital and has long-term monetary value similar

	real world assets. All digital assets are ultimately just digital data, whether data in a traditional form (for example, a list of useful contacts, or something like a website address or digital art).
Digital Currency	See Cryptocurrency.
Digital Signature	A process that utilises Cryptography to authenticate messages linked to Public Keys by means of unforgeable proof of control of Private Keys. This proof of control of the Private Keys is deemed to be a proof of ownership of the corresponding crypto Address. In crypto, Digital Signatures are typically used to sign and authorise Transactions associated with the given Address.
Distributed Ledger Technology ("DLT")	Unlike traditional electronic databases, Distributed Ledgers have a distributed web like structure, where many independent parties have their own independent copy of the database. These parties then come to consensus on the state of the Distributed Ledger, i.e. what data should and should not be included in the database and in what sequence. This database largely consists of financial transactions and so agreeing on the state of the database, determines the "bank balances" of everyone on the Network. DLT is often used interchangeably with Blockchain as Blockchain is the most common form of DLT.
Double-Spend Attack	A situation where a Cryptoasset is spent more than once, e.g. the same bitcoin is sent to two recipients. In traditional banking, banks and regulators prevent people from spending the same electronic money twice. Bitcoin was the first system that solved this problem without the need of a central intermediary to enforce the rules, who would traditionally prevent people from trying to Double Spend.

E

Ethereum	The second largest Cryptoasset Network by market capitalisation. It is the major platform for Smart Contracts and Decentralised Applications. Ethereum is an open and Permissionless Network, so anyone can join and run a Validating Node.
ether ("ETH")	The native Cryptocurrency used on the Ethereum Network. The Network is designed to issue, maintain and transfer units of ether the Cryptocurrency between and on behalf of parties.
Encryption	Techniques used to communications between parties private from the general public and eavesdroppers. Communications across the Internet, including crypto Transactions, are in the public domain, so any information which is for the intended recipient(s) only must use encryption to keep it private.
Crypto Exchange	A marketplace where buyers meet sellers and engage in the trading of Cryptoassets. Crypto Exchanges can be thought of as the stock exchanges of the Cryptoassets world, though they differ from traditional stock exchanges in various ways, for example, people can directly open accounts with crypto exchanges, instead of needing to trading via a broker.

F

Finality — The degree to which a Transaction is considered irreversible and final, with high Finality indicating a low chance of reversal. With Bitcoin, it is conventional to consider Transactions as final after six Blocks have been Mined on top of them.

Fork — Either a split of a Cryptoasset Network into different competing Networks, or a change of a Network's Protocol. There are two classes of Fork: Hard Fork and Soft Fork. One of the most known examples of a Fork was the creation of Bitcoin Cash in 2017, which now competes against Bitcoin.

Fourth Industrial Revolution — See Industrial Revolution 4.0.

G

Genesis Block — The first Block in a Blockchain, back to which all other Blocks ultimately link. The Genesis Block of Bitcoin was created on January 3 of 2009.

Governance Token — Protocols and Decentralised Applications may issue a Token to their service providers, users and contributors, to help manage and govern the project. Such Tokens may be considered, or even referred to as equity tokens, given the decision-making rights they hold. Governance Tokens may or may not have associated cash flows, such as those from fees collected from consumers. Decentralised Autonomous Organisations are typically managed using Governance Tokens where token holders vote on proposed, such as changes to the software.

H

Halving — The point in time at which the rate of supply growth of a Cryptocurrency halves. With Bitcoin, Miners are rewarded with a fixed amount of newly minted bitcoins and this fixed amount halves every 210,000 blocks or approximately every four years. The last Bitcoin Halving occurred in May 2020, when the Block Subsidy was halved from 12.5 to 6.25 BTC per block. Note that not all crypto Protocols have Halving events.

Hard Fork — Implementation of an expanded set of Network Protocol rules that are not retroactively compatible with the previous version of the Protocol. In this case, Nodes that do not implement the new rules will not be able to communicate with Nodes that do implement it and thus a split in the Network happens. One of the most known examples of a Network split via Hard Fork was the creation of Bitcoin Cash in 2017, which now competes against Bitcoin.

Hash — The output of a Hash Function.

Hash Function — A mathematical function that turns an arbitrary amount of input data into output data of a fixed length. A *cryptographically secure* Hash Function will have apparently randomised output distribution and have outputs that are sufficiently large for it to be very unlikely that any two distinct inputs will yield the same output. Therefore, a Hash of data can be considered as a unique fingerprint of that data. It is also not possible to recompute the input on the basis of only knowing the output. Its properties make verification of data fast and easy. It is a key technology not only in crypto, but also the Internet in general.

Hashrate

The number of Hashes produced per second by either a given piece of computer equipment, a Mining Farm, a Mining Pool, or over an entire Network. It measures the speed at which solutions to the Mining puzzle are being tested.

Hardware Wallet

A purpose built Wallet device, which is a form of Cold Wallet because it stores Private Keys offline and it is therefore secure against Cyberattacks. Hardware wallets can look like USB memory sticks but are much more secure. The main goal of Hardware Wallets is the secure generation and management of Private Keys that are used to sign Transactions.

Hot Wallet

A Wallet which stores Private Keys on a device which is connected to the Internet and therefore can be compromised through a Cyberattack. Crypto Exchanges typically keep a portion of funds in a Hot Wallet to facilitate fast withdrawals for customers. Smart phone based Wallets are typically Hot Wallets. Hot Wallets are typically considered less secure than Cold Wallets, when Cold Wallet best practices are followed.

I

Industrial Revolution 4.0

Industrial Revolution 4.0, or the data revolution, is a suite of technologies which use and integrate data to improve efficiency and outcomes in the production of goods and provision of services. These technologies center around cyber physical systems, digital scarcity, automated decision making and digital networks. Industrial Revolution 4.0 technologies include the Internet of Things, Artificial Intelligence, big data and Distributed Ledger Technology, as well as many other technologies.

Initial Coin Offering ("ICO")

A primary public sale of a new Cryptoasset, used to raise funds for the development of a particular, associated project as well as other business activities and constitutes the initial distribution of the Cryptoasset to the market. The idea behind ICOs is similar to Initial Public Offerings, but ICOs are unregulated and do not always have an exchange on which to trade the associated Cryptoasset.

Initial Exchange Offering ("IEO")

A modification of ICOs, where projects raise money via an exchange that supervises and aims to establish transparency of process. This also ensures that there is a trading venue for the associated Cryptoasset.

Internet

The global collection of computer Networks which communicate by using the Internet protocol suite commonly referred to as TCP/IP. This is the base software on which everything from Amazon to emails to video calls depends. Note that while the terms "Web" and "Internet" are commonly used interchangeably, they are in fact different things.

Interoperability

The ability of Protocols to understand each other. In the context of DLT, for example, one Transaction on Ledger A may trigger another Transaction on Ledger B. The third generation platforms like Cosmos, Avalanche or Polkadot focus on interoperable Blockchains that ensure seamless cross-Network communication.

J

Joy Of Missing Out ("JOMO")

Acronym used by the crypto community. This is the opposite to "Fear Of Missing Out".

K

Key

In the context of crypto, Keys are primarily Private Keys, but also their associated Public Keys, which are used to sign outgoing Transactions and receive incoming Transactions, respectively. While Public Keys (and their associated Addresses) can be shared with anyone as a form of personal identifier (akin to a bank account routing number), Private Keys must be kept secret as they are the sole means of signing (approving) outgoing Transactions.

L

Ledger

In accounting terms, Ledgers are used to record financial transactions and account balances. In DLT, Ledgers are decentralised and maintained by Nodes.

Light Client

A type of Wallet that does not download and verify the full Distributed Ledger. These are usually operated on mobile devices and are dependent on third party servers to feed them Transaction data from a Network, instead of being fully independent.

Lightning Network

A Protocol which piggybacks the Bitcoin Network, designed to handle a very large number of Transactions with close to instant Finality and with much lower fees than on the Bitcoin Network, itself. This Network is not designed for larger value Transactions, but for a high volume of small and quick Transactions.

M

Mainnet

The “real-money” version of a crypto Network. Typically, the Mainnet is preceded by a Testnet, where new features are tested. While Networks have usually only one Mainnet, they can have multiple Testnets.

Miner

A participant in a Proof-of-Work crypto Network who undertakes Mining.

Mining

The process of Validating Transactions by adding them to Distributed Ledgers which employ Proof-of-Work, such as Bitcoin. Mining is a service to the Network for arbitrating between competing Transactions which would otherwise be equally valid, whether they are fraudulent Double Spends or honest Transactions vying for priority of confirmation. As a service, it is funded directly by Transaction Fees (i.e. tips or inducements to approve a Transaction quickly) and Block Subsidy. Mining is intentionally resource-intensive (in terms of electricity and capital) to undertake, in order to align the interests of the Miners with the currency holders and users.

Miners can be considered the ‘(de)central bank’ of a crypto Network who are collectively responsible for final settlement. The process is, however, called Mining as a metaphor drawn from the slow and costly process of extracting traditional commodities.

Mining Farm

A professional Mining operation which consists of specialised industrial buildings or containers to house large quantities of dedicated Mining equipment.

Mining Pool

Created by Miners to allow them to pool computing power, for which they then share Block Rewards amongst themselves. This results in more predictable and frequent

cashflows for each of the Miners, and is therefore the usually preferred option for small Miners.

Multi-signature

A type of Smart Contract construction which requires multiple parties to approve new Transactions. Such Transactions enable better governance and control over Cryptoassets held by companies and are typically used by corporate custodians and institutional investors.

N

Network

In relation to crypto, a Network is a collection of Nodes, or independent computers that store a copy of the Distributed Ledger, connected via the Internet. Typically, these Networks are permissionless, so anyone can join and be part of the Network by simply downloading and installing a piece of software. The Network collectively fulfils the function of "authority" that oversees and enforces the rules of the Network, instead of having a central authority enforcing its rules.

Node

A basic unit of a Distributed Ledger Network. A Node is a software package which includes the Protocol and usually also Wallet functionality, being run on an Internet connected device. It verifies and maintains its own independent copy of the Ledger. Depending on the Network, a Network can consist of hundreds, thousands or virtually unlimited numbers of individual Nodes.

Non-Fungible Token ("NFT")

A Token which is unique, like the Mona Lisa by Leonardo da Vinci is unique among objects. There is no other painting like it in existence and that is partly what makes it valuable. Similarly, an NFT stores some form of metadata that makes it a unique entry on a Distributed Ledger and that is what makes it valuable. NFTs are popular in applications that deal with computer game items or digital art.

In other words, NFTs are digital (hence "Token") certificates of ownership stored on a Distributed Ledger. They are exclusive and not interchangeable with other Tokens (hence "non-fungible"). A key application is likely to be in the field of intellectual property.

O

On-chain

A term used to describe events, Transactions and records facilitated by the Distributed Ledger Protocol, for example when a bitcoin Transaction is saved on the Bitcoin Ledger. When something is saved on the Bitcoin Ledger, it is saved on the Bitcoin Blockchain. This is described as being 'saved on-chain'.

Off-chain

A term used to describe anything which is not On-chain. For example, the Lightning Network, software built on top of the Bitcoin Network, is considered to be 'off-chain'.

P

Paper Wallet

A type of Cold Wallet that stores Private Keys offline and therefore is more secure from Cyberattacks than online Wallets. This is simply the Private Key code printed out on a piece of paper, which is in turn stored in a safe location, such as a personal safe.

Peer-to-Peer ("P2P")	A type of network that consists of computers connected to each other directly, without a central server and with no hierarchy. Crypto Networks are typically Peer-to-Peer networks and so are message passing or file-sharing systems.
Permissioned Ledger	This term is typically used to describe a jointly controlled and maintained Ledger, with a controlled user base and small number of semi-trusted Validators, all identified. This allows for greater control and customisation. It does not require a Cryptocurrency. Permissioned Ledgers are typically deployed between companies for enterprise use cases of DLT.
Permissionless ("Public") Ledger	A type of Ledger that allows anyone to run a Network Node and verify their own copy of the Ledger and compete as a Validator. Permissionless Ledgers need a Cryptocurrency that incentivises Validators to enforce the Network rules, as there is no centralised entity to control it. The most famous example of a Permissionless Ledger is Bitcoin.
Private Key	Used to sign (and approve) Transactions, thus allowing its holder to unlock assets locked to a corresponding Public Key, or equivalent, as recorded on a Ledger. Private Keys need to be kept secret and secure. An example of a Private Key, in hexadecimal form, compatible with many Networks including Bitcoin: e9873d79c6d87dc0fb6a5778633389f4453213303da61f20bd67fc233aa33262
Private Ledger	A form of Permissioned Ledger controlled by a single entity.
Proof of Stake ("PoS")	A mechanism used in some Public Ledgers to incentivise the security and integrity of a Network. Unlike Proof-of-Work (PoW), it does not require vast amounts of electricity. Many recently introduced crypto Networks deploy some form of Proof-of-Stake. Unlike PoW systems, in a PoS system Network Validators stake their Coins to align their interests with currency holders and users. This means that the influence in the Network is proportional to the amount of Coins possessed by each entity.
Proof of Work ("PoW")	The mechanism used by Bitcoin and some other Public Ledgers to incentivise the security and integrity of a Network. While it enables immutability and censorship resistance, it is often criticised for using a vast amount of energy. At its core the mechanism requires Miners to perform energy intensive computations to secure integrity of Ledger data.
Protocol	The set of rules to which a crypto Network adheres and the messaging standards by which its Nodes communicate. These rules include the setting out of how a Transaction becomes valid and how the Network is governed.
Public Key	This is derived from a Private Key and acts as an identifier for it. Once a Public Key is converted into Address form, it fulfils a similar function to a bank account number that identifies a receiver. Public Keys (or Addresses) can be shared with anyone in order to receive a payment from them. For the purposes of maintaining privacy in a Public Ledger environment however, users are encouraged to use new Public Keys as often as practical. An example of a Bitcoin compatible Public Key and a resultant Address:

02588D202AFCC1EE4sAB5254C7847EC25B9A135BBDA0F2BC69EE1A714749FD77DC9 -> (*1CC3X2gu58d6wXUWMffpuzN9JAfTUWu4Kj)*.

Public Ledger See .

Q

Quantum Computer A computer which makes use of quantum phenomena such as superposition and entanglement to perform computations. Using these techniques potentially allows computers to become far more powerful than is possible with traditional computer technology. While Quantum Computers do currently exist and work, practical Quantum Computers which are quantum superior have still to be developed. Their potential power, however, could undermine the security of most cryptographic technologies currently used to secure both crypto and the Internet more generally.

Quantum Resistance This refers to Cryptography which will remain secure, to all intents and purposes, from hacking and compromise by Quantum Computers. Cryptography relies on complex mathematical problems which traditional computers cannot solve in any useful time scale e.g. within 10,000 years, but a Quantum Superior Computer will be able to solve these mathematic problems quickly, meaning that most Cryptography used today to secure the Internet will no longer be secure when Quantum Superior Computers exist.

Quantum Superiority / Quantum Superior Computer A Quantum Computer which can perform calculations which are too large and complex for the most powerful non-Quantum Computers to be able to achieve in any useful timescale. A Quantum Superior Computer is able to perform calculations in minutes or hours that would take non-Quantum Computers 10,000 or more years to calculate.

R

Ring Signatures A type of Digital Signature used in some privacy-conscious crypto Networks such as Monero. Here, someone can sign a Transaction without revealing their exact identity (i.e. their exact Public Key) on the Public Ledger. Instead, the public see a “ring” of possible Public Keys, only one of which is the true Public Key.

S

Satoshi The smallest denomination of bitcoin. Each bitcoin is 100,000,000 satoshis. The name is derived from the pseudonymous creator of Bitcoin, Satoshi Nakamoto.

Satoshi Nakamoto The pseudonymous person or a group of people who created Bitcoin and whose real world identity or identities is or are unknown.

Scaling The act of expanding the capacity of a crypto Network to meet demand. Blockchains, for example, can only Validate a limited volume of Transactions per Block and hence a limited number of Transactions per hour, which results in delays and Transaction Fee bidding wars in times of congestion. Scaling may be achieved by expanding the technical limits of a given crypto Network and its Protocol, or by adding additional aggregation and netting systems, which use main Network for the Final net

payments. This is similar to how systems like Visa or SWIFT work in traditional finance.

Security Token

A Token which represents financial assets and complies with existing legal frameworks for financial securities. Examples of financial assets which can be Tokenised include shares in companies, debt instruments and units in an investment fund. Security Tokens are the crypto equivalent of digital securities.

Security Token Offering

The Security Token equivalent to Initial Public Offering of company shares or primary debt issuance.

Smart Contract

In Ethereum and other crypto Networks designed for Decentralised Applications, Smart Contracts are programs saved on a Distributed Ledger available for others to trigger and use by sending Transactions to them. All active Nodes will execute the triggered Smart Contract to verify the results. Smart Contracts may contain arbitrary computer programs. They are particularly well suited however, to financial service applications, such as Digital Asset exchanges or escrow management.

Soft Fork

Implementation of a rules change in the Network Protocol which is compatible with the previous version of the Protocol. Therefore, no split in a Network happens, even if not every Node updates to the new Protocol.

Software Wallet

The most common type of Wallet when it comes to Cryptoassets. It is a software program which acts as a crypto Wallet.

Stablecoin

These are Cryptoassets designed to have a price which closely tracks some reference asset, either by directly linking to it, or by providing a hedging mechanism. This is designed to make its price more stable and make it more useful as a means of payment for everyday transactions. A Stablecoin can be pegged to a currency or basket of currencies, exchange traded commodities, or other Cryptoassets.

Staker

A participant in a Proof-of-Stake crypto Network who undertakes Staking.

Staking

The process of Validating Transactions by adding them to Distributed Ledgers which employ Proof-of-Stake, such as Tezos. Staking is a service to the Network for arbitrating between competing Transactions which would otherwise be equally valid, whether they are fraudulent Double Spends or honest Transactions vying for priority of confirmation. As a service, it is funded directly by Transaction Fees (i.e. tips or inducements to approve a Transaction quickly) and Block Subsidy. Staking is intentionally capital intensive, requiring large amounts of the Protocol's native Cryptocurrency, to align the interests of the Stakers with the currency holders and users. It avoids incurring the external resource costs of Mining.

Stakers can be considered the '(de)central bank' of a crypto Network who are collectively responsible for Final settlement. The process is called Staking to highlight the Stakers having put something of value at risk to provide the Finality service.

T

Tether

Tether is the most popular Stablecoin currently in use. It is used primarily to trade other Cryptoassets on Crypto Exchanges, since Tether markets are generally the most liquid. It is pegged to the value of the US Dollar.

Testnet

The test version of a crypto Network, where developers can freely experiment in a test environment before deploying systems or upgrades to the "real-money" Mainnet. Testnets are also used as pre-productions versions of a Mainnet prior to its launch. Networks may have multiple Testnets.

Token

A Cryptoasset which can be created by anyone on top of an existing crypto Network such as Ethereum. Thesedo not, therefore, require their own Ledger like a Coin does. Decentralised Applications commonly issue their own token to incentivise engagement by service providers or customers. Common types include Utility Tokens, Security Tokens and Stablecoins.

Tokenise

To represent any asset as a Token. Tokenisation is the process of issuing Tokens onto a crypto Network and may refer to various use cases such as the separation of ownership rights from the practicalities of custody of tangible assets (for example, with gold bullion) where one Token may be redeemable with the issuing custodian for one bar of gold. Equity rights to a company may be issued in Token form directly without the need for a traditional registrar or paper documents; this would be the direct Tokenisation of a company's ownership structure.

Tokenomics

A branch of Cryptoeconomics that studies the economic design of Tokens within a particular ecosystem of a Decentralised Application. In the absence of a central authority to manage the ecosystem, the design of a successful Token needs to align incentives of the software developers, any service providers and the service users or Token holders. It should also contain a value accrual mechanism for the Token.

Transaction

Any record of data made into a Distributed Ledger. Typically, Transactions contain data related to the change of ownership of Cryptoassets, i.e., a payment or transfer.

Transaction Fee

Tips or inducements paid to Validators within a crypto Network to incentivise them to process a Transaction. Like traditional tips, they are determined by the sender of a Transaction. The higher the fee, the more motivated Validators will be to add the Transaction to the Distributed Ledger quickly. Fees are only payable in the native Cryptocurrency of the Distributed Ledger.

U

Utility Token

Used to digitally access (or reward for providing) an application or service within a crypto Network. Coupons, gift vouchers and loyalty points are straightforward use cases for Utility Tokens.

V

Validator

A Node in a Network that Validates Transactions. Miners and Stakers are classified as Validators. There are many conditions within a Protocol's rules which Transactions must meet to be valid (for example not spending more Coins than are available) and it is the responsibility of the Transaction sender and their Wallet to adhere to these rules, otherwise, all Nodes will reject the Transaction in a process referred to as verification. It is the role of a Validator to apply one Final arbitrating

approval to an otherwise almost valid Transaction and that approval is to say that this Transaction can be relied upon not to be replaced, especially by Double-Spends.

Virtual Asset — See Digital Asset.

W

Wallet — A device and/or software used to manage a person or entity's Cryptoassets, similar in some ways to an online bank account. Wallets are designed to generate, store and manage safely the Private Keys which control all Cryptoassets in that Wallet. One must open one's Wallet to pay in crypto, analogous to opening a traditional Wallet to pay by cash or card.

Wallets also communicate with Nodes, which collect information from the Distributed Ledger upon request. This ability allows Wallets to determine crypto balances, draft, sign and send new transactions accurately and monitor the status of existing transactions and Smart Contracts. See Hardware Wallet and Software Wallet for more information.

Web 3.0 — The term used to describe various transformative technologies and software which look to reshape the way the Web currently works and how it is used. This is a growing movement to re-design cyberspace and replace today's tech giants with decentralised Networks.

Whitepaper — A proposal document prepared by a project team which provides the key information prospective users, investors and developers would like to know about the project. It typically provides an overview of the overall vision, Cryptocurrency use and cryptoeconomic design, technical information and a project roadmap.

World Wide Web / WWW / Web — A global information system which functions via the Internet using the hypertext transfer protocol (HTTP), hypertext makeup language (HTML) and uniform resource locators (URLs), such as https://www.aaro.capital. The Web is separate from but dependent upon the Internet. The Web includes all Web pages from Amazon to Facebook to internet banking. Note that while the terms "Web" and "Internet" are commonly used interchangeably, they are in fact different things.

X

XBT — XBT is an alternative abbreviation for bitcoin the Cryptocurrency, instead of the more commonly used BTC abbreviation.

Y

Yellowpaper — A Yellowpaper is a research document which provides more in-depth and technical analysis than a Whitepaper. This paper is typically written for the technical and developer community as opposed to non-specialist investors.

Z

Zero-Knowledge Proofs ("ZKPs")	Cryptographic technology that allows statements to be proven simply to be true or false, without revealing any other information or data. For example, a program can verify a user is at least 18 years old, by that person revealing only a proof of that fact, but does not reveal their actual age or birthday i.e. it is a proof with zero other knowledge. This technology is explored and experimented with in multiple crypto Networks, mainly for privacy purposes, but also for Scaling throughput and accessibility of crypto Networks.

Aaro Capital

Contact Information:

Investor Relations
investor.relations@aaro.capital

aaro.capital