GUIDE

Cryptocurrency – Background & Blockchains

Last reviewed: January 2022

What is a cryptocurrency

History

Following the global financial crisis in 2008, a white paper authored by the pseudonymous 'Satoshi Nakamoto' appeared on the internet, proposing the creation of a peer-to-peer (**P2P**) electronic cash system built on an underlying platform of distributed ledger technology (**DLT**).[1]

Nakamoto's proposition stemmed from the analysis that "commerce on the internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments."[2] This, Nakamoto argues, results in high transaction costs and permits payments to be reversible at the discretion of the third party intermediary.[3] The promise of DLT is a system where cryptographic proof replaces the need for trust in third parties, effectively cutting out the 'middle man'.

The first public iteration of this technology, known as 'the Blockchain', was launched in 2009, complete with its own electronic payment system, or cryptocurrency, known as 'Bitcoin'. In recent years, this technology has undergone a rapid evolution, with new platforms and cryptocurrencies launched daily.

The Building Blocks of Blockchain

The conceptualisation of an online, decentralised ledger system arose out of post-global financial crisis which resulted in a mistrust in centralised institutions.[4] This has had a profound effect on not only the P2P architecture of the technology itself, but also the system's designed insulation from interference by governments, banks and other intermediaries.

In order to understand cryptocurrencies and the unique risks they pose to investors, it is imperative to understand the underlying characteristics of DLT that make secure P2P value exchange possible.

Distributed Network

The Blockchain is a distributed ledger network. In its simplest form, a distributed ledger (**DL**) is a database, characterised by its shared information nodes in the network. Nodes in the DL system are in effect devices that collectively run the software and together maintain the database records. In this format, the connected nodes share and validate information.

[1] Stoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (White Paper, 9 January 2009) accessed 2 December <https//bitcoin.org/bitcoin.pdf>

[2] Ibid

[3] Ibid

[4] Usman W Chohan, 'Initial Coin Offerings (ICOs): Risks, Regulation and Accountability' (Notes on the 21st Century: University of New South Wales Discussion Paper Series, 2017)

The connected-node structure allows all devices running the DL software to view transactions and participate in the process of transaction verification protocols.[5] This ensures that no single entity has the ability to control the network's data, and removes the need for an intermediary in verification of transaction records.

Open Source Software

Whereas traditional databases are constructed to operate with a central hub acting as a single source of valid information and control, blockchains are traditionally open-source.[6] In practice, this means that any computer that is running a blockchain's software becomes a node in the system, allowing it to share database management responsibilities on a P2P basis.

The open-source database structure allows for any individual with internet access to download the blockchain software for free and participate in the distributed ledger. This format complicates regulators' enforcement actions against individuals, as open-source blockchain users generally cannot be vetted prior to gaining network access or be blocked from the network at a later date.

Transaction Transparency

The end-result of a blockchain's open-source software and distributed network architectures is a transparent ledger of transactions. Every transaction and its associated value are listed on the ledger, and visible to all nodes.

As aptly noted by commentators, 'if the price of centralisation is *trust* (as users need to trust centralised operators with their data), decentralization comes at the price of *transparency* (as everyone's interactions are made visible to all network's nodes)".[7]

Though buyer and seller transact publicly and directly in a DL ecosystem, the transaction's transparency does not extend to the identities of the parties. Rather, transactions are conducted between 30-plus character alphanumeric public keys used as identifiers.[8] Though the blockchain retains an encrypted record of every user's identity on its public ledger, it is ultimately up to users to decide whether to remain anonymous or provide proof of identity to others on the system.[9]

The pseudonymous nature of blockchain technologies is commonly linked with regulatory fears of money laundering and criminal activity, as well as the growth of 'darknet' online marketplaces where illegal goods and services are traded.

Permanent and Immutable History

Each transaction conducted by parties on a blockchain network is timestamped and verified before being recorded on the DL.[10]

The progressively increasing list of records are catalogued and sequenced in 'blocks', each containing a unique cryptographic fingerprint, and verified by consensus algorithm before being broadcast to all other

---

[5] David Mills, Kathy Wang, Brendan Malone, Anja Ravi, Jeff Marqardt, Clinton Chen, Anton Badev, Timothy Brezinski, Linda Fahy, Kimberly Liao, Vanessa Kargenian, Max Ellithorpe, Wendy NG and Maria Baird, 'Distributed Ledger Technology in Payments, Clearing and Settlement' (2016) Finance and Economics Discussion Series 2016-095. Washington: Board of Governors of the Federal Reserve System <https://doi.org/10.17016/FEDS.2016.095> 10

[6] Mills et al, supra note 29, 10; Blockchain networks are generally run as an open source software although closed systems can be created. See Xiwei Xu, Ingo Weber, Mark Staples, Liming Zhu, Jan Bosch, Len Bass, Cesare Pautasso and Paul Rimba, 'A Taxonomy of Blockchain-Based Systems for Architecture Design' (2017 IEEE International Conference on Software Architecture, Gothenburg Sweden, 3 April 2017) < http://design.inf.usi.ch/sites/default/files/biblio/icsa2017-blockchain.pdf>

[7] Primavera De Filippi, 'The interplay between decentralization and privacy: the case of blockchain technologies' (2016) 9 Journal of Peer Production 2

[8] John D Halamka, Andrew Lippman and Ariel Ekblaw, 'The Potential for Blockchain to Transform Electronic Health Records' (2017) Reprint H03I15, Harvard Business Review 1, 4

[9] Judith Lee, Arthur Long, Marcellus McRae, Jeff Steiner and Stephenie Gosnell, 'Bitcoin Basics: a Primer on Virtual Currencies' (2015) 16(1) Business Law International 21, 21

[10] Xiwei Xu, Cesare Pautasso, Liming Zhu, Vincent Gramoli, Alexander Ponomarev, An Binh Tran and Shiping Chen, 'The Blockchain as a Software Connector' (IFIP Conference on Software Architecture (WICSA), Venice Italy, April 2016) 2

nodes on the network.[11] As each block is added to the publicly shared ledger, it forms a chain containing a complete record of all transactions – or a 'blockchain'.

As the public ledger is shared across all nodes in the network, there is no centralised point for hackers or other parties to change or delete the record retroactively without consensus from all nodes. This structure provides certainty for those who use the technology, and ensures transactions are permanent and immutable. Furthermore, the cryptographic fingerprint of blocks and the node consensus algorithms theoretically make a blockchain 'tamperproof'.[12]

The four central aspects of DLT (distributed network, open-source software, transaction transparency and permanent, immutable and secure transaction history) ensure a secure value exchange in a P2P format, removing the necessity of a third party intermediary in these transactions.

However, this poses legal uncertainty for both regulators and developers as traditional legal and regulatory approaches generally focus on the intermediary function. Furthermore, the open-source software and pseudonymity of users challenges regulator's abilities to enforce laws and regulation on blockchain platforms as users could be easily masking their identity and potentially be located anywhere in the world with internet access. In the resulting legal vacuum, regulators face major challenges as they seek to build regulatory frameworks around this developing ecosystem.

Regulation

The autonomous governance framework of DL systems (commonly referred to as 'code is law') effectively hinders the ability of sovereign governments to enforce their own laws and systems on blockchain platforms.[13] Whilst some commentators and crypto-enthusiasts view blockchain ecosystems as the 'wild west'[14], governments and international organisations are eager to bring stability and transparency to the cryptocurrency frontier.[15]

Cryptocurrency regulation is a rapidly evolving field spearheaded by multiple governments and international organisations (sometimes working together, but more often not). As each jurisdiction works to define and build a regulatory framework around cryptocurrencies, investors must weigh up for themselves the risks and benefits of investing in a blockchain ecosystem.

Overarching principles for investment

Without the robust, comprehensive and cohesive regulation found in other, more familiar forms of investment (such as stocks and shares, or property) investors in cryptocurrencies will need to be aware of the inherent risks they assume by opting to invest in blockchain-native assets.

The US Commodity Futures Trade Commission has identified four categories of risk faced by those purchasing cryptocurrency and other crypto-tokens:

- 'Operational risks' arising from the fact some cryptocurrency platforms do not have system safeguards or consumer protection systems in place to protect purchasers of Coins;
- 'Cybersecurity risks' due to hacking vulnerabilities in crypto-wallets (where Coins are held) or situations where platforms opt to co-mingle consumer assets in shared accounts;
- 'Speculative risk' as high volatility and large price swings are a common feature for most Coins; and
- 'Fraud and Manipulation Risk' from Ponzi schemes and other fraudulent attempts "seeking capitalise on the current attention focused on virtual currencies".[16]

---

[11] Mike Orcutt, 'How secure is blockchain really?' (2018) 121(3) MIT Technology Review 40; 45 Giang-Truong Nguyen and Kyungbaek Kim, 'A Survey about Consensus Algorithms Used in Blockchain' (2018) 14(1) Journal of Information Processing Systems 101, 102

[12] In practice cryptographers and hackers have found creative ways to 'cheat the system', see: Orcutt, supra note 11 on eclipse attacks etc.; see also Robinson's notes on 51% attacks, Sybil attacks and hard forks (supra note 13)

[13] Randolph Robinson, 'The New Digital Wild West: Regulating the Explosion of Initial Coin Offerings' (University of Denver Sturm College of Law Legal Research Paper Series, Working Paper No. 18-01)

[14] Mihailis Diamantis, The Light Touch of Caveat Emptor in Crypto's Wild West (April 5, 2020). 104 Iowa L. Rev. Online 113 (2020), U Iowa Legal Studies Research Paper No. 2020-20

[15] Roasario Girasa, Regulation of Cryptocurrencies and Blockchain Technologies: National and International Perspectives (Palgrave MacMillan 2018)

[16] Commodity Futures Trading Commission, 'A CFTC Primer on Virtual Currencies' (cftc.gov, 17 October 2017) <https://www.cftc.gov/sites/default/files/idc/groups/public/documents/file/labcftc_primercurrencies100417.pdf> accessed 14 January 2022

Over the coming series, we will consider in turn each of the four categories of risk, highlight recent events where such perils have materialised, and consider how investors can mitigate the inherent risks of buying and holding cryptocurrencies.

Contacts

A full list of contacts specialising in cryptocurrency can be found here.

This guide is only intended to give a summary and general overview of the subject matter. It is not intended to be comprehensive and does not constitute, and should not be taken to be, legal advice. If you would like legal advice or further information on any issue raised by this guide, please get in touch with one of your usual contacts. You can find out more about us, and access our legal and regulatory notices at mourant.com. © 2022 MOURANT OZANNES ALL RIGHTS RESERVED

2021934/82736755/2