

Asia-Pacific Research Exchange Business Model Investment Series

Blockchain – the underlying technology of cryptocurrency

Kenneth Kwong, CFA

Abstract

2022 was a terrible year for crypto. However, one should never deny the potential of blockchain technology. The technology is currently being used in both public and private sectors. In this article, we will explore its characteristics and business adoption.

Keywords: Blockchain, crypto, DEFI,

One should never deny the potential of blockchain, the underlying technology of cryptocurrency. A blockchain is a distributed database that is used to record data. The technology has several characteristics:

1. **Immutable** – A blockchain is a permanent network that is irreversible. A “block” - data structure within the blockchain database - records some or all of the most recent transactions that are yet to be validated by the network. Subsequently, the block is closed after the data validation, and a new block is created for new transaction data. Different blockchain networks take different amounts of time to reach finality, a state whereby the transaction on the blockchain cannot be reversed.
2. **Distributed and Decentralised** – The ledger is maintained by nodes, which hold copies of the ledger and participate in the validation process. The network is governed by nodes instead of any centralised governing authorities.
3. **Consensus** – The consensus mechanism is how the network of nodes reaches an agreement on the state of a blockchain. The most common ones are the Proof of Work and Proof of Stake. Consensus mechanism aims to solve the Byzantine Generals problem - a game theory problem describing a situation whereby participants have difficulty coming to a consensus when they do not know who to trust due to the absence of a trusted central party.
4. **Secured** - Blockchain utilises cryptography to sign transactions and data. Blocks are “hashed” cryptographically as each block contains its unique hash and the hash of the previous block. Modifying the data in one block results in a change of its own hash and as a result the hash of the connecting blocks in the blockchain. As of now, undermining consensus mechanisms of the prevailing blockchains is mathematically difficult.

There are different types of blockchains.

Public blockchain - a public blockchain network, such as Bitcoin and Ethereum, is permissionless. Most DeFi protocols are built on Ethereum due to its smart contract feature and decentralized nature. Meanwhile, some enterprises do not use public blockchain, concerning the limited privacy of transactions.

Private blockchain – a private blockchain network, such as Hyperledger Fabric, is usually governed by a single organisation. The central party decides who can execute a consensus protocol and maintain the shared ledger.

Consortium blockchain – a consortium blockchain network is governed by a group of organizations rather than one central organization. Multiple

organizations can share the responsibilities of maintaining a blockchain. These pre-selected organizations determine who may submit the transactions or access the data. Hence, consortium blockchains are more decentralized and secure.

In a utopian world, a blockchain should consist of all three elements:

1. Security (being more secure with more nodes and hence greater difficulty for a hack)
2. Decentralization (shifting control from one central entity to decentralised participants)
3. Scalability (growing the network while maintaining the same processing power e.g. transactions per second).

However, the world is not perfect. Blockchain Trilemma refers to the difficulty in blockchain development, that one can only focus on two out of the three elements. Scalability and decentralization are often held back by security, meanwhile security tends to be compromised by any shifts on a network that offer scalability. To address this problem, “Layer 2” blockchains - secondary blockchains integrated on top of an existing “Layer 1” blockchain - like sharding, rollups, side-chains and state channels reduce demand for block space of “Layer 1” by transferring transactions to the “Layer 2”, enabling faster transactions, reducing monetary expenses and expanding the underlying blockchain’s application.

Governments are researching, testing and distributing blockchain technology for their Central Bank Digital Currency (CBDC), the digital form of a country’s fiat currency that is controlled by the issuing authorities. For example, together with Bank for International Settlements Innovation Hub (BISIH) Hong Kong Centre, the Hong Kong Monetary Authority (HKMA) launched a pilot CBDC “Project mBridge” to expedite cross-border payments. Additionally, Bahamas launched the Sand Dollar; Sweden’s Riksbank launched the e-krona; China’s PBOC launched the e-CNY; and the Federal Reserve issued a discussion paper examining the pros and cons of a potential U.S. CBDC.

On the other hand, financial institutions are integrating blockchain into their banking businesses. Facilitated by the Monetary Authority of Singapore’s (MAS) Project Guardian, JPMorgan has successfully executed its first-ever cross-border transaction using decentralized finance (modified version of AAVE) on Polygon. Furthermore, Goldman Sachs trades bonds and debt

securities for clients on blockchain networks, reducing settlement times and lowering costs for issuers, investors and regulators. Banks are building their own blockchain-based trading platforms, aiming to cut down each trade's processing time and to free up capital. "Deposit tokens," considered as blockchain-based "cash equivalents," is also being widely discussed as they are similarly to traditional deposits held by licensed financial institutions, except they exist and operate on-chain. Ripple, an enterprise blockchain services provider, has been building out blockchain-based solutions for banks to use for clearance and settlement since 2016. Meanwhile, Society for Worldwide Interbank Financial Telecommunications (SWIFT), the world's leading provider of secure financial messaging services has tapped into Symbiont's enterprise blockchain to improve operational efficiency. Corporate action data from SWIFT messages will be uploaded to the blockchain, enabling institutional partners to share crucial information and ensure accuracy.

Eyeballs are on the business opportunities of tokenising real-world assets with blockchain technology. Assets, such as properties, bonds and art, can be tokenised, tracked and traded on a blockchain network. As a result, individual investors could transact fractions of assets with easier access, faster settlement time, higher liquidity, no minimum investment threshold and no redemption period restriction.

In fact, blockchain technology is being used to solve climate change as tokenisation covers green bonds, solar panels, and carbon credit as well. In healthcare, the technology is already being used to encrypt patient medical data. In supply chain management, blockchains tokenise a variety of data across the value chain, from trade data such as purchase orders and inventory units to Internet of Things (IoT) data generated from smart sensors and RFID tags, resulting in higher traceability, visibility, and accuracy throughout the supply chain. In art and gaming, NFTs provide a blockchain-based record of ownership of digital assets — which can range from images and songs to in-game weapons and digital identities. Web3 gaming models typically involve a play-to-earn (P2E) component facilitated by NFTs and tokens, that players can transact their digital assets in marketplaces or swap them on DeFi exchanges.

Using the Polygon blockchain, Value of Values (VoV) - a blockchain-based art project curated by Ann Mak, conceived by French artist Maurice Benayoun and produced by the Osage Art Foundation registered brain waves as NFTs. The project aims to discover human perception toward values through EEG (Electroencephalography, and biofeedback). Exhibition visitors create – straight from their brain waves – a three-dimensional shape to abstract

concepts, like MONEY, LOVE, and HEALTH. The resulting shapes are then registered as NFTs, which can be stored in crypto wallets and transacted in the marketplace. As of time of writing, 77,200 VoV NFTs have been created. Interestingly, in HK, values like “Money” and “Space” rank higher than “Happiness” and “Intelligence”.

The 14th Factory, a digital-physical art show curated by Hong Kong artist Simon Birch, adopts blockchain technology to facilitate the ticketing mechanism as ticket buyers will receive NFTs upon ticket purchase. The show will be hosted across 4 cities globally, offering participants satisfying in-real-life (IRL) experiences. The NFT tickets will be a form of digital art linked to another physical art.

Blockchain technology will be mature, stable, and common for public use. Similar to the adoption of the Internet, we will know that blockchain technology has achieved its success when it becomes part of our lives.

Reference

<https://ethereum.org/en/developers/docs/consensus-mechanisms/>

<https://www.ledger.com/academy/what-is-the-blockchain-trilemma>

<https://www.hkma.gov.hk/eng/news-and-media/press-releases/2022/10/20221026-3/>

<https://www.imf.org/en/News/Articles/2022/02/09/sp020922-the-future-of-money-gearing-up-for-central-bank-digital-currency>

<https://www.federalreserve.gov/central-bank-digital-currency.htm>

<https://blockworks.co/news/deposit-tokens-stablecoins-defi-jpmorgan>

<https://www.v-o-v.io/>

<https://the14thfactory.com/>

About the Author

Kenneth Kwong, CFA, is a member of Web 3 Committee at CFA Society Hong Kong. He had experience in traditional banking and finance, covered institutional clients in the digital asset space and studied cryptography in Peking University.

