Blockchain White Paper

One For All (OFA)

December 2023

Introduction

One For All (OFA) startedit process in year 2023 to understand how blockchain works, to learn how it is being used.

This white paper represents OFA findings. .

Blockchain Overview

Conceptual Description

Blockchain, or ***distributed ledger*** technology, is a database that is consensually shared, replicated, and synchronized.

To better understand the technical aspects of a blockchain, it is helpful to explain the concept through an example. When an individual deposits a sum of money into a banking institution, the individual trusts that the sum will be there until they decide to exchange it for goods or services. The individual trusts the bank will have an accurate record of the transaction, such as the amount, depositor, date, and time of the deposit. More broadly, society relies on central repositories, such as banks or governments, to collect, maintain, and protect the recorded actions of individuals or institutions.

Blockchain differs from centralized repositories in that it decentralizes the source of trust. An individual deposits funds into a digital wallet and the value is captured on the blockchain. If this individual purchases a digital song, the transaction is captured in the blockchain along with the change in fund level in the digital account. The bank is not required as a trusted third party. The trustworthy record is recorded in the blockchain shared by all the parties on the network.

Technical Description

The replication and storage of transactional data by each party, or node, on a blockchain network is known as a distributed ledger. Conflicts, or inaccuracies within the database, are automatically resolved with predefined ledger rules. The fundamental characteristics of the distributed ledger include:

- Operation with peer-to-peer networks,
- Decentralized transaction record keeping,
- Consensus or trust-based transactions, and
- Tamper resistance.

Blockchains, while similar to databases, are not used for general data storage, but rather hold information about transactions (see Figure 1). Sometimes the blockchain will contain the transactions themselves or may include the proof a transaction is valid**.**

Blockchain Parts

Blockchains contain three core parts:

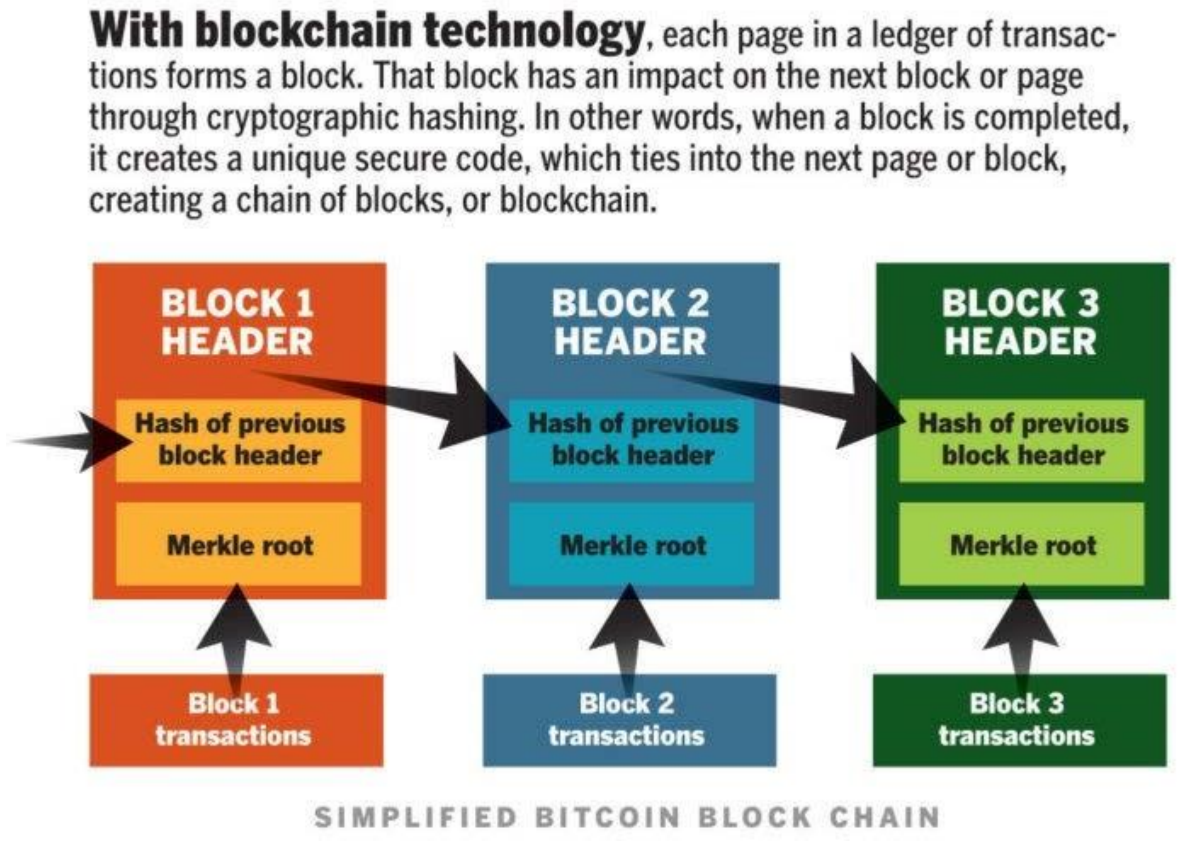
- **Block**: A list of recorded transactions over a period of time. Transactions can represent virtually any type of activity from registering a land deed to a single purchase. Any rules relating to the block itself are established when the network is first created. For example, the maximum number of transactions in a block or the size of each block can be limited.

- **Chain**: When the block reaches its maximum size of transactions, it is chained or linked to the preceding block through a ***hash*** as described in the section below. The hash value of one block is inserted into the next block. This makes a link between the new block and the previous block. Repeating a hash function on an unaltered block of data will always generate the same fixed-length value. If a block of data is altered, the resulting hash output will be different. A user can then see the hashes are different and will know the original block has been altered and may no longer be trustworthy. (See Figure 2)

- **Network**: The network is made up of nodes each containing a complete record of all transactions on a blockchain. No centralized "official" copy exists and no node is "trusted" more than another. The data integrity is maintained by the blockchain being replicated on all of the nodes.

  Think of a node as a cluster of servers running a blockchain. Node operators are incentivized to operate a node by receiving rewards for their efforts. For example, with cryptocurrencies, nodes compete to solve crypto-puzzles. The first node completing the puzzle has its solution verified by other nodes. Once the solution is verified, the node completing the puzzle adds the next block to the blockchain and is also rewarded with cryptocurrency for its effort. This process is called mining, with the resources involved called miners. Nodes are found across the globe and are challenging to operate. For example, the infrastructure of one cryptocurrency is supported by approximately 5000 nodes. Incentivized miners are required for cryptocurrency platforms, but are not necessarily part of other blockchain uses.

Behind the scenes, each blockchain has its own rules or algorithms governing how nodes validate transactions intended for entry into the blockchain. These rules are called a ***consensus mechanism*** and are established when the blockchain is created. By embedding a consensus mechanism, blockchains create a way for parties who do not know if they can trust each other to agree an entry should be added to the blockchain. This addresses the so-called ***Byzantine Generals Problem***. Each blockchain has its own consensus mechanism depending on the type of transaction it is capturing. Some consensus mechanism are known as “proof of work”, “proof of space” or “proof of stake”. The mechanisms facilitate authenticity, or the immutability of transaction records.



With blockchain technology, each page in a ledger of transactions forms a block. That block has an impact on the next block or page through cryptographic hashing. In other words, when a block is completed, it creates a unique secure code, which ties into the next page or block, creating a chain of blocks, or blockchain.

Figure 1. Pursel, Bart. (2018, January 28). Blockchain is Here to Stay. Retrieved from http://sites.psu.edu/ist110pursel/2018/01/28/blockchain-is-here-to-stay/

What is a Hash

A ***hash*** is an algorithm that takes a variable string of data and generates a fixed length value. The data about the transactions must be small so the validity of the transaction can be quickly calculated and distributed to other nodes. Large amounts of data are often stored "***off chain***" with pointers or hashes of the data stored within the blockchain. Traditionally, ledgers were used to record transactions of property or goods: only the transaction was captured in the ledger with the real property being handled separately.

For example, a Secure Hash Algorithm generating a 256-bit signature (***SHA-256***) generates different hash values for slight variations in the spelling of the words "National Archives".

Variable Text String Entry Value	**Hash Value**
National Archives	6429799b9af2d91cbf915cb0290f3a50281193a977b3457d63e4541cc5788c5b
National Archives *(an extra space)*	d926fe7e72d09b249701dbcde2dad0ccb9b4bb653e053e461a67bbb951dcae0b
Nati0nal Archives	5f2d570fc940d5f8de89310db43f789fdd99f51e89c021e1a50acb7a6fe2cf83

Figure 2. Xorbin (2018). Retrieved from https://www.xorbin.com/tools/sha256-hash-calculator

Oftentimes, to save space, multiple hash values can be brought together and hashed again, creating a single hash value or Merkle root that represents multiple hashes. This technology is called a ***Merkle tree***.

NARA began hashing electronic records when the Electronic Records Archives (ERA) was deployed in 2008. NARA has been using the SHA-256 algorithm to prove file ***fixity*** when electronic records are ingested into ERA. The files are automatically hashed and this hash can be used to verify the authenticity of a file. The hash is stored in log files and the processing archivist has access to this information, usually through reports. In the future, it might be feasible to store this information in a blockchain.

Blockchain Types

There are three types of blockchains:

> ***Public***: Large distributed blockchains are available for anyone to participate in and are generally open-sourced with the code maintained by a broad community. For example, Bitcoin, one of the most commonly known blockchain networks, is a public blockchain.
>
> ***Permissioned***: Large distributed blockchain network with established roles that individuals can fill when using the blockchain. For example, a group of banks may share sensitive cash reserve information with each other through the blockchain.

Private: Oftentimes a smaller blockchain is tightly controlled and is established between trusted entities that wish to share sensitive information. For example, an organization could use an internal blockchain to certify documents for its own use.

Blockchain network participants utilize public and private keys to digitally sign and make secure transactions within the system.

Public Key Infrastructure (PKI) mathematically pairs two long numbers or keys together that are not identical. This is called asymmetric cryptography. Both keys can be used to encrypt and decrypt messages. One key can be shared publicly, known as the public key and one is held privately known as the private key. For example, anyone using the public key can send and encrypt a message, but only the individual with the private key can decrypt and read the message. Within the blockchain context, a user can sign a transaction with their private key and anyone can verify the signer by using the corresponding public key. NARA has issued guidance on PKI.

Blockchain Platforms

Blockchain is made up of a collection of underlying technologies that can be bound together in multiple ways. This allows blockchains to be configured in multiple ways to serve different purposes. Our review of various blockchain platforms identified four different approaches represented by the options outlined below.

1. **Bitcoin**: Bitcoin is a ***cryptocurrency*** with a related open-source platform. Bitcoin's blockchain is primarily designed to support the exchange of cryptocurrency without an intermediary third party. Bitcoin assumes no trust between parties and requires numerous decentralized nodes to ensure the blockchain has not been corrupted by malicious actors.

2. **Ripple**: Much like Bitcoin, Ripple is based on an open-source protocol that uses blockchain to exchange value. Ripple has an established user-base of regional and global banks that need to transact international payments in real-time. Ripple also allows the trade of goods, property, and items of value.

3. **Ethereum**: Whereas the two platforms above are primarily focused on their own currency trade, Ethereum launched in July 2015 with the goal of providing a fully functioning programming language to allow users to build full applications with an integrated blockchain. Ethereum is a crowd-funded and open-source programming language. Users of Ethereum can program executable ***smart contracts*** and ***decentralized applications*** using the blockchain.

4. **Hyperledger**: The Hyperledger project focuses on developing an open source and collaborative approach to distributed ledgers. By developing standards and an overall framework for blockchains, Hyperledger has gained support from organizations including

Cisco, American Express, and IBM. Some library and information science schools are incorporating Hyperledger into their curriculum. Hyperledger has stated they will never build a cryptocurrency.

Blockchain Smart Contracts

A smart contract is a contract that has been translated into the software language of the blockchain, stored on the blockchain, and can be autonomously executed by a triggering event. Put differently, a smart contract is a series of if/then statements programmed and saved on the blockchain. Once the requirements of the smart contract are met, the contract will automatically be executed and the resulting action will be stored and shared across the blockchain. For example, a songwriter can sell a digital song at a certain price in an online music app. This agreement could be programmed into Ethereum as a smart contract. The smart contract will automatically distribute payment to the songwriter when a fan buys the digital song and capture the transaction in the blockchain.

During the development of blockchain platforms, system developers have the ability to program smart contracts that will render transactional data, or records, ***cryptographically inaccessible***. This means the records are not deleted from blockchain, but are cryptographically redacted to block the data from general view. It is not clear yet if cryptographically inaccessible data means will be permanently inaccessible and therefore could be considered "removed" from a complete record.

From a records management perspective, features like cryptographically inaccessible data indicates that records retention and disposition was not included as part the original intention of blockchain developers. The use of these smart contracts could potentially address record access, retention, disposition, and litigation hold requirements, depending how the blockchain rules, roles, and features are developed.