Hyperledger Sawtooth for Application Developers

Module 2: Blockchain Basics

MODULE 2: Blockchain Basics

This module introduces you to general blockchain concepts, such as a distributed ledger, transactions, blocks, and consensus.

Contents

- What is a blockchain?
- What is a transaction?
- How does a blockchain work?
- Cryptographic security
- Blockchain permissions
- Consensus
- When not to use a blockchain

What is a Blockchain?

A *blockchain* is an append-only database of transactions that is distributed to all participants in a blockchain network. There is no owner, administrator, or centralized data storage. Participants do not necessarily belong to the same enterprise or organization.

Another term for blockchain is *distributed ledger*, because the database can be thought of an electronic ledger of transactions (state changes) to the data. This distributed ledger is:

- **Shared**: Each participant has a copy of the database that is demonstrably identical to all other copies in the blockchain network.
- **Auditable**: The blockchain provides an *immutable* (unalterable) history of all transactions that uses block hashes to detect and prevent attempts to alter the history.
- **Secure**: All changes are performed by transactions that are signed by known participants. Cryptographic and signing mechanisms provide additional security for the transactions on the blockchain.

These features work together with a consensus mechanism to provide "adversarial trust" among all participants in a blockchain network.

★ For more information, see Wikipedia's definition of blockchain.

What is a Transaction?

A *transaction* is a change to the shared state of the blockchain database. For example:

- Transferring an asset, such as spending cryptocurrency or earning frequent-flyer points
- Changing an item's location when tracking provenance on a supply chain
- Updating personal data, such as patient information in an electronic medical record

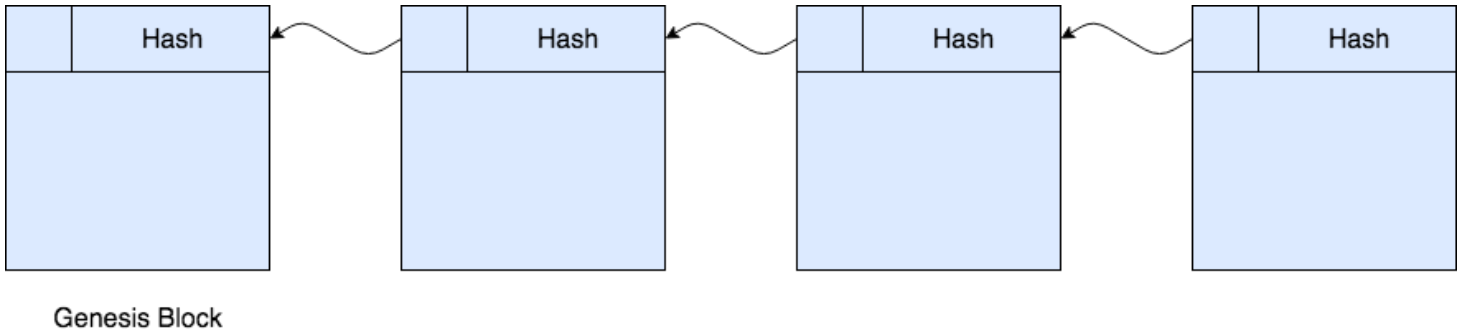
Transactions are gathered into *blocks*, with one or more transactions per block.

How Does a Blockchain Work?

You can think of a blockchain a series of *state changes*, or log of transactions, that affect the state of the data on a shared distributed ledger. Each block on the blockchain contains transaction data and a header with a timestamp, signer, and hash value.

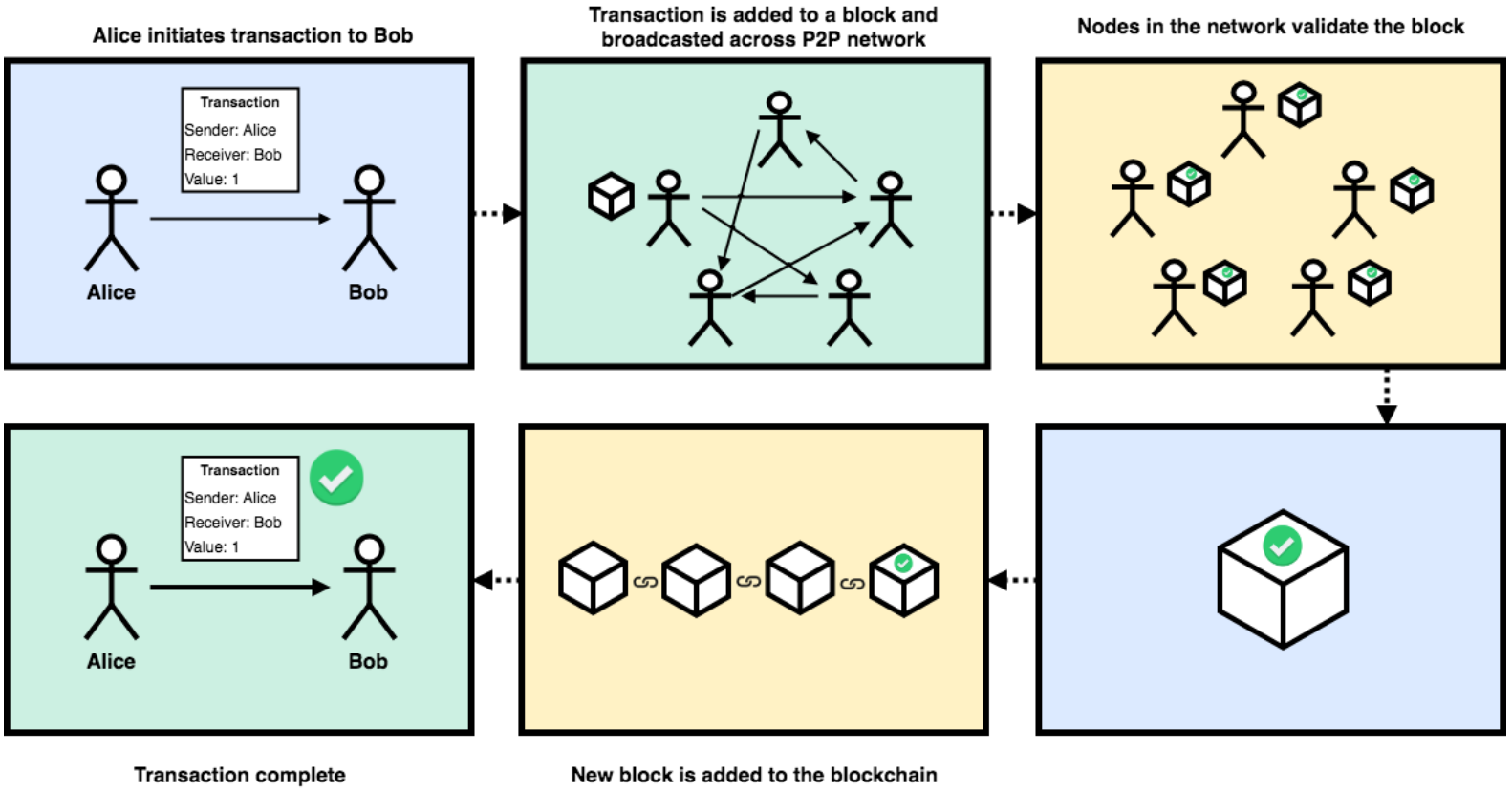
The *hash value* is a cryptographic signature or digital fingerprint that uniquely identifies the data in that block, as well as the block's position in the blockchain. Each block's hash includes the hash value of the previous block, which makes it very difficult for a malicious actor to change a previous block. Importantly, the hash algorithm takes an input string of any length and produces fixed-length output. Common blockchain hash algorithms include RIPEMD and SHA-2, (such as SHA256 and SHA512).

A blockchain starts with a genesis block. Depending on the blockchain platform, the first block could be empty (except for its hash value) or contain initial settings for the blockchain.



Blockchain Workflow

This picture shows the general workflow for adding new data (a transaction) to the blockchain.



Cryptographic Security

Blockchains commonly use *public key cryptography* to identify legitimate participants and to make sure that malicious users or systems cannot insert bad data or modify the blockchain history.

Public key cryptography uses a pair of keys, a public key and a private key, to identify participants and sign transactions. The public key is available on the network and the private key is kept secret. Together, the two keys provide a secure digital signature that identifies the source of each transaction.

Many blockchain platforms use the Elliptic Curve Digital Signature Algorithm (ECDSA) for public-private keys. Sawtooth uses the ECDSA standard algorithm with secp256k1 curve for signing.

For more information, see:

- https://www.blockchain-council.org/blockchain/how-does-blockchain-use-public-key-cryptography/
- https://blog.cloudflare.com/ecdsa-the-digital-signature-algorithm-of-a-better-internet/

Blockchain Permissions

Blockchain networks have the following types of general permissions:

A public blockchain has no restrictions on participation. It allows anyone to join and submit transactions. A signing mechanism, such as public/private keys, identifies each submitter. Ethereum and Bitcoin are examples of public blockchains.

A consortium blockchain is partly private or decentralized. It restricts which nodes can join the network, and can further control which nodes can participate in consensus. However, any participant can submit signed transactions. This network type supports policy-based transaction permissions. For example, Quorum is an Ethereum-powered consortium blockchain that is intended for use by banking and financial industries.

A private blockchain is "permissioned" with access control features. It can have separate controls to restrict who can join, submit transactions, and participate in consensus. This network type supports policy-based transaction permissions. In addition, a private blockchain:

- Specifies the type of transactions that "transactors" can sign
- Restricts "address space access" to a limited set of "transactors"
- Supports policy-based transaction permissioning

Examples of private blockchain platforms include Hyperledger Fabric and Hyperledger Sawtooth.

For more information, see http://au.pcmag.com/amazon-web-services/46389/feature/blockchain-the-invisible-technology-thats-changing-the-world

Consensus

A blockchain network uses *consensus* to determine whether a block is valid and should be added to the blockchain. The consensus algorithm determines how the participants decide and how many participants must agree. Types of consensus include:

- Practical Byzantine Fault Tolerance (PBFT), where participants elect a leader to validate transactions. As long as malicious participants are less than 50% of the network, they are overruled by the other participants.
- Proof of Work (PoW), a lottery-like system where the participant who finishes a computational task first (such as solving a cryptographic puzzle) is chosen to publish a block. Bitcoin uses Proof of Work consensus.
- Proof of Stake (PoS), another lottery-like system that requires a stake (such cryptocurrency or computational power). As each participant votes on whether a block is valid, the vote is weighted by the size of the participant's stake.
- Proof of Elapsed Time (PoET) was introduced in Hyperledger Sawtooth. This type of consensus uses random wait times that are generated from a trusted source. The wait time determines who can propose and publish blocks. The participant with the shortest wait time wins the right to validate the block. PoET consensus improves energy use and resource consumption as compared to PoW or PoS consensus.

For more information, see the PoET 1.0 Specification in the Sawtooth documentation and:

- https://medium.com/@chrshmmmr/consensus-in-blockchain-systems-in-short-691fc7d1fefe
- https://jornfranke.wordpress.com/2017/11/18/blockchain-consensus-algorithms-proof-of-anything/

When Not to Use a Blockchain

Blockchain technology is designed for applications that need a decentralized, distributed database with no central control or owner. Participants can be "mutually distrusting," such as competitors in the same business space.

The traditional approach is a centralized relational database (RDBMS) under the control of a single managing authority. A centralized RDBMS is appropriate for data with a single owner (such as a corporation or government entity) where all contributors are trusted.

Performance is another issue. A blockchain platform is designed for security and decentralization, but not necessarily speed. For example, traditional stock market transactions must occur at a much faster rate than is possible on current blockchain platforms, where each participant must process every transaction.

★ For more information, see https://hackernoon.com/blockchains-versus-traditional-databases-c1a728159f79

Module 2: Summary

This module described the important features of blockchain technology, including blockchain structure, transactions and blocks, cryptographic security (hashing and signing), types of blockchain networks, and consensus.

The next module describes the key concepts of Hyperledger Sawtooth.

Walker Evans, Detail of Mooring Chains, New Bedford, Massachusetts (fragment)
J. Paul Getty Museum
Digital image courtesy of the Getty's Open Content Program.