SASKEN

Blockchain Technology: Concepts

Whitepaper

Introduction

Cryptocurrency, the digital currency system that enables global monetary transactions between two parties without the need for a trusted third party financial institution, has gained tremendous momentum over the last few years. Bitcoin, the first cryptocurrency, came into existence in January 2009. Its inventor, Satoshi Nakamoto (an anonymous person or a group) published a whitepaper prior to this in October, 2008. Since then, numerous cryptocurrencies have come into existence. More recently, bitcoin has gained mainstream attention. Under the hood, the technological innovation is the blockchain, also called as distributed ledger technology that is seen as revolutionary foundational technology having a tremendous potential across different verticals.

Author:
Girish BVS, Senior Solutions Architect, Technology Group,
Sasken Technologies Limited

Table of Content

Cryptocurrency

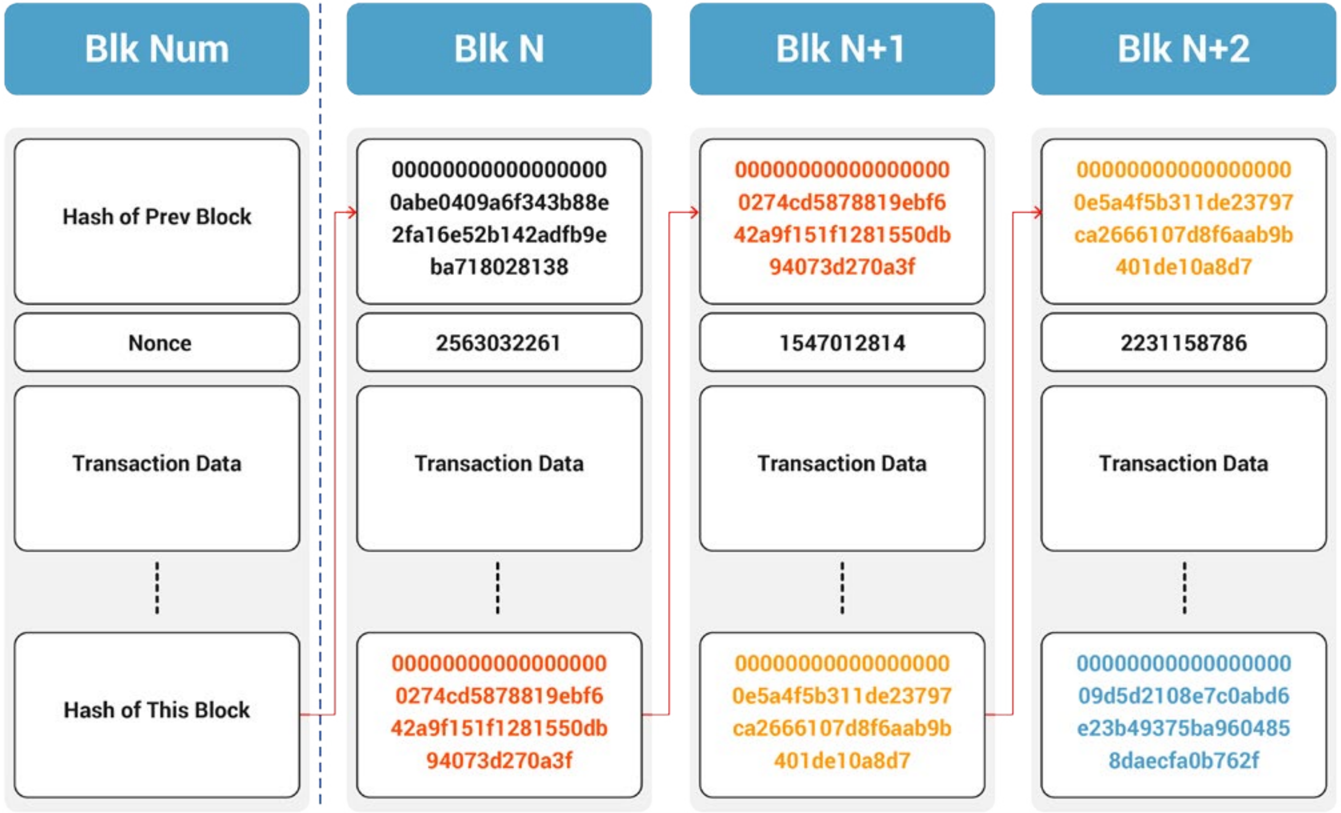
In the cashless fiat currency system, transactions between parties involve third party financial institutions, typically one or more banks that take care of:

- Verifying availability of funds
- Preventing double spends, that is, ensuring the same funds are not spent more than once, by updating ledgers.

In the digital currency system, availability or proof of possession of funds can be verified by using digital signatures. However, the problem of double spending increases since a digital asset or a token can be replicated easily. The solution to this lies in Blockchain.

Blockchain

Blockchain is a decentralized and distributed ledger, where, blocks containing a set of transactions are chained together by cryptographic hash. Transactions originating from a node are validated by participating nodes and a set of transactions are added into a block by a “mining” node. Any mining node with sufficient compute power that solves a cryptographic puzzle can generate and broadcast a new block containing the set of validated transactions.



Blk Num	Blk N	Blk N+1	Blk N+2
Hash of Prev Block	0000000000000000 0abe0409a6f343b88e 2fa16e52b142adfb9e ba718028138	0000000000000000 0274cd5878819ebf6 42a9f151f1281550db 94073d270a3f	0000000000000000 0e5a4f5b311de23797 ca2666107d8f6aab9b 401de10a8d7
Nonce	2563032261	1547012814	2231158786
Transaction Data	Transaction Data	Transaction Data	Transaction Data
⋮	⋮	⋮	⋮
Hash of This Block	0000000000000000 0274cd5878819ebf6 42a9f151f1281550db 94073d270a3f	0000000000000000 0e5a4f5b311de23797 ca2666107d8f6aab9b 401de10a8d7	0000000000000000 09d5d2108e7c0abd6 e23b49375ba960485 8daecfa0b762f

Figure 1: A Typical Blockchain

Block Hash = SHA2562(Hash of Prev Block|| Nonce||Tx Data Hash||Time||ver||Target value)

Target value is the difficulty level set by that network that requires the hash to be less than or equal to this value. The current Bitcoin difficulty target translates to 18 leading zero nibbles.

Participating node receives, validates and stores the new block. There is no master copy. Each block includes the hash of the previous block in the current block, forming a chain of blocks, the blockchain. If the previous block content is modified, the hash of previous block changes, hence the hash of the current block changes and so on. This makes any change easily detectable.

Peer-to-Peer Network

Blockchain uses peer-to-peer (P2P) network overlay on the Internet (Figure 2). Each node communicates with a set of neighbor nodes, each of which communicates with their neighbor nodes and so on. Any node can join and leave the network at will. The transactions and blocks are broadcast on the P2P network and each receiving node forwards it to other neighbor nodes.

Nodes that store a copy of complete blockchain are Full Nodes. SPV (simple payment verification) nodes verify payment using only block headers. Mining nodes generate blocks.

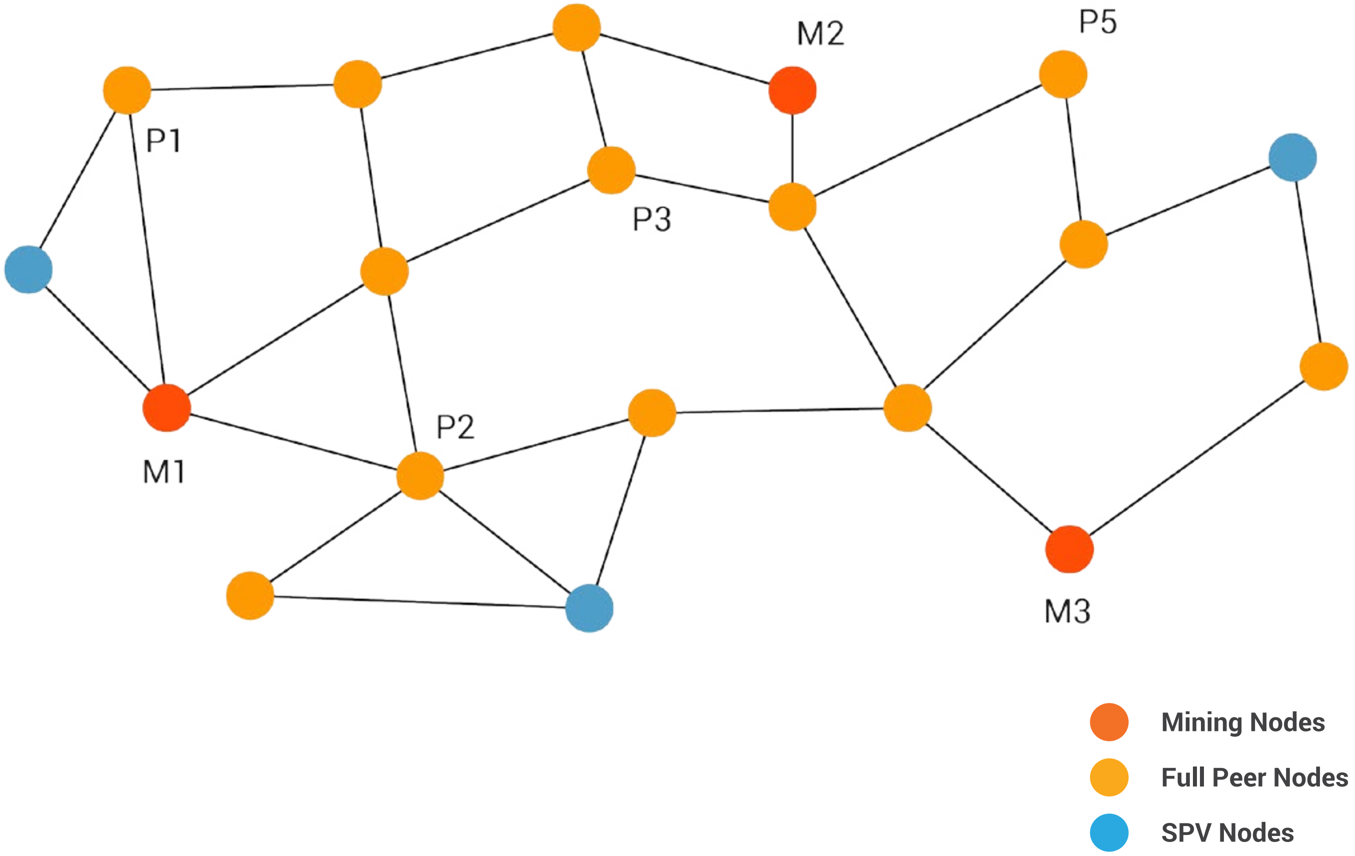


Figure 2: Blockchain Peer-to-Peer Network

Building the Blockchain

There are three important aspects to be addressed in a Blockchain design.

1. Timestamping:
When the transactions are chronologically ordered and a single history is agreed by majority of nodes, the double spending problem can be solved by always considering the first transaction from the sender as valid for the same funds. Timestamping is achieved by collecting the pending transactions into a block and calculating the block hash. It can be proved that the transaction existed at the time of the block creation since it is hashed into the block. Granularity of this is time to generate a new block which is ~10 minutes in Bitcoin.

2. Consensus:
New blocks are created & broadcast by mining nodes, each not being identical and arrive in different order at different nodes. It becomes a necessity for all the nodes to agree on a single version of block, thereby a consensus that is needed. A distributed consensus (in a trust-less environment) must decide on which block out of several variants generated by multiple nodes would be added to the blockchain.

3. Data Security & Integrity:
A malicious node cannot create fake transactions since private keys are used to sign the transaction. However, it can generate its own double spend transactions, one paying to a vendor and another paying back itself. While transaction ordering takes care to include only the first transaction, if the malicious node is able to generate blocks easily and deterministically, it can create new block with the transaction paying back itself. When this block is accepted by other nodes, the malicious transaction gets through.

Proof-of-work

Proof-of-work (PoW), also called as Mining is used to achieve consensus and ensure data security & integrity on the sequence of transactions which can only be changed by redoing the proof-of-work. PoW introduces difficulty in block generation. It involves finding a "nonce" value such that when the block contents are hashed, the hash begins with a certain number of leading zero bits. The only way it can be done is trial and error and the work required to find this nonce value increases exponentially to the number of zero bits required. The correctness of the nonce value can however, be verified by a single hash execution by peer nodes. Nodes that engage in the race to find the nonce are called Mining nodes (see Figure 2).

The longest chain will have the maximum proof-of-work and hence nodes will accept the longest chain as valid. It also implies that the longest chain was formed from the largest pool of computation power. To tamper with a transaction on a blockchain, PoW must be redone for all the subsequent blocks starting with the block in which the transaction is present and then catch-up and outpace the existing chain and form the longest chain. As long as more than 50% of computational power is controlled by honest nodes, the blockchain is immune to attackers.

Types of Blockchain

Depending on how the nodes in the network join and the restrictions placed on the roles, a blockchain can be permission-less or permissioned.

Permission-less blockchain is also a public blockchain. Any node can join and leave at any point in time by merely running the node software. Transactions can be sent by signing the transaction with the private key that can be verified by peer nodes. Bitcoin and Ethereum blockchains are examples of public permission-less blockchain.

Permissioned blockchains are at a consortium or private level (within an organization). Here, the nodes need to be authenticated before joining the network and information needs to be contained within.

There can be restrictions on the nodes that can validate and approve the transactions. There could be various implementations, but to be called a blockchain rather than a distributed database, it should conform to the decentralized notion with a distributed consensus.

Permissioned blockchains are at a consortium or private level (within an organization).

Blockchain Flavors and Other Uses

Blockchain is gaining popularity and has potential use-cases across many verticals, spread across Finance, Healthcare, Supply chain, Internet of Things (IoT), Legal, Government, Notary service, Crowd funding to name a few.

Apart from Bitcoin blockchain, there are various open-source blockchain implementations such as Ethereum and Hyperledger (with 5 flavors) that are coming up, with contributions and backing by industry big-wigs such as Intel, IBM, Accenture, Cisco, American Express, J.P. Morgan to name a few. The permissioned blockchain have more efficient consensus algorithms such as proof-of-elapsed-time (PoET), proof-of-authority (PoA), practical byzantine fault tolerance (PBFT).

These blockchains also support smart contracts with Turing complete language, making it more suitable to develop applications across industry verticals.

> There are various open-source blockchain implementations such as Ethereum and Hyperledger (with 5 flavors)

Smart Contracts

Blockchain based smart contracts are computer codes that implements contract clauses between parties and deployed on the blockchain. Based on the conditions/ events, it executes and enforces the contract fully or partially as per the coded contract, automatically.

An example use-case would be to have a smart contract for goods purchase which must be delivered on time. There can be conditions on full payment, payment with penalty deducted, no payment etc. This can be coded and deployed on the blockchain. The events can be triggered with IoT devices and sent to the blockchain.

Suppose there was a delay in the shipment arriving at the buyer's address, with the arrival event and time automatically sent by IoT device to the blockchain, the contract automatically makes a payment with penalty deducted to the seller.

Conclusion

The invention of blockchain by Satoshi Nakamoto utilized existing technologies and combined it in a novel method. While we have to wait and watch how the cryptocurrencies' future will unfold, the underlying blockchain technology provides a foundation for innovation in different verticals and use-cases with far-reaching effects. It is likely to become disruptive that has enormous potential for next level of automation, integration and service availability across many different verticals bringing in speed, efficiency and transparency.

References

[1] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008

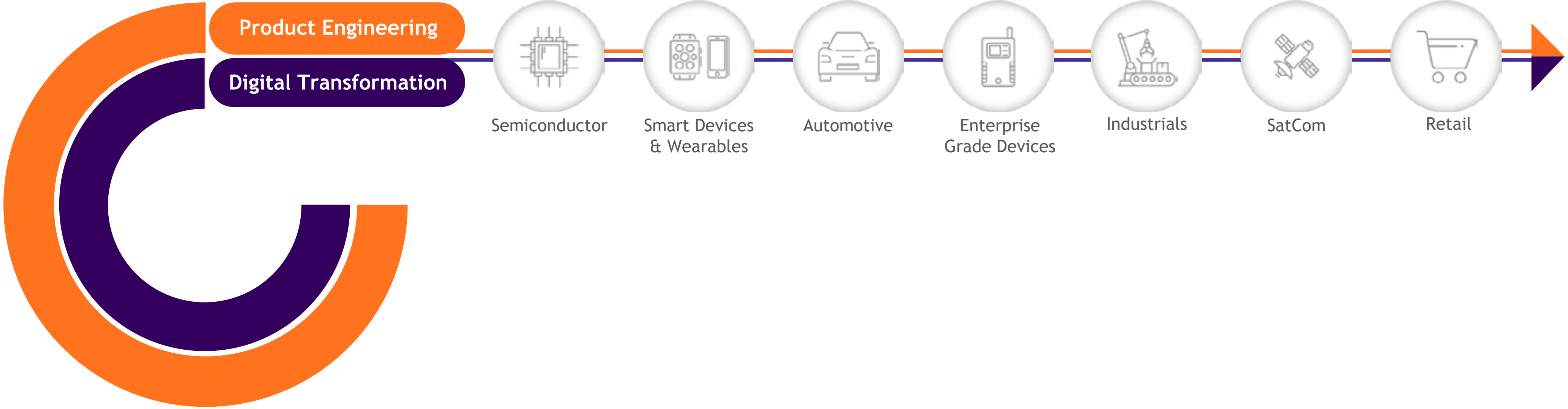
[2] “Developer Documentation”, https://bitcoin.org/en/developer-documentation

[3] “Introduction to Smart Contracts”, http://solidity.readthedocs.io/en/develop/introduction-to-smart-contracts.html

[4] “Bitcoin Developer Reference”, https://github.com/minium/Bitcoin-Spec/blob/master/Bitcoin.pdf

About Sasken

Sasken is a specialist in Product Engineering and Digital Transformation providing concept-to-market, chip-to-cognition R&D services to global leaders in Semiconductor, Automotive, Industrials, Smart Devices & Wearables, Enterprise Grade Devices, Satcom, and Retail industries. With over 27 years in Product Engineering and Digital Transformation and 70 patents, Sasken has transformed the businesses of over a 100 Fortune 500 companies, powering over a billion devices through its services and IP.



SASKEN

Blockchain Technology: Concepts

marketing@sasken.com | www.sasken.com

USA | UK | FINLAND | GERMANY | JAPAN | INDIA | CHINA

May 2018