Blockchain for Decentralized Transactions with Distributed Consensus

Dr. Nish Sonwalkar (ScD, MIT~~), Founder~~), Founder, Power2Peer Inc.

Contributing Editors: Mamta Sonwalkar and Michael Mahoney

There is a lot of buzz right now about blockchain being the next generation of software platform design. The internet, with its HTTP (hypertext transfer protocol), is itself a highly decentralized system, but one ultimately controlled by domain name servers through the identification of a node. The domain URL identifies a node on the internet as the location for a transfer of information bits on the information highway. Your internet address (URL) is translated by the DNS and the information packets find their way to your internet location. This is termed as the first generation of internet. However, for conducting financial transactions or for that matter any transaction of goods, money or things, you need a third-party verification system or trusted authority. This third-party validation process makes internet business vulnerable to hackers, who intrude into trusted systems and steal the digital identity of users. Recent hacks to one credit authorization company compromised millions of accounts. Hence, prevention of theft of the digital identity has become a major challenge.

Satoshi Nakamori came up with a famous scheme for digital currency, Bitcoin (BTC), that can be created and operated on a blockchain framework. A blockchain is a shared, encrypted, "distributed ledger" that is maintained by a network of computers with no central authority. The platform is transparent, immutable, traceable and secure.

The blockchain framework allows transactions without involvement of trusted third party for verification of the transaction. Now the innovation of the blockchain technology lies in the decentralization of transactions by creating a distributed consensus, where honest nodes can safeguard against any tampering of the transactions. In the blockchain, there is a linked list of blocks that are connected via hash pointers. The hash pointers are cryptographic hash functions that are unique identifiers for a block, which includes data as part of the cryptographic message. At the center of the block chain technology is NOT encryption but the consensus between honest nodes on all transactions (see Figure 1).

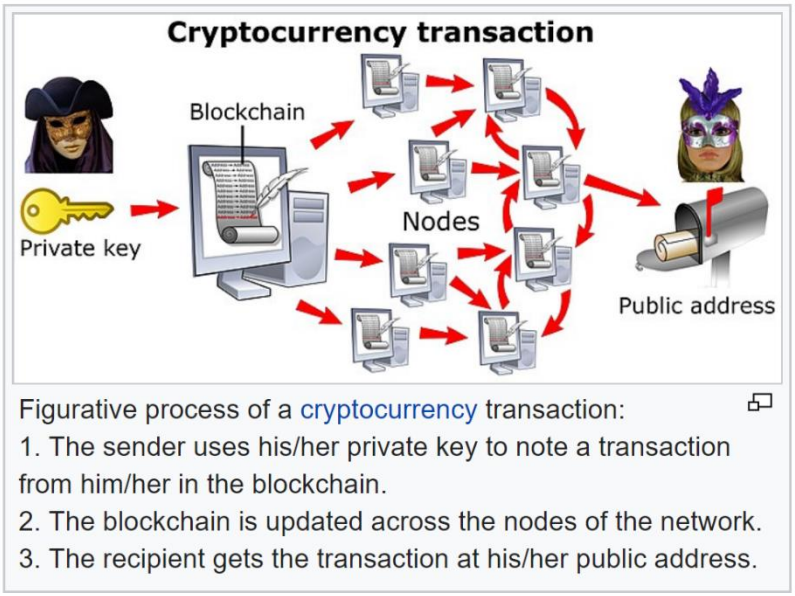


Figure 1: Schematic diagram of blockchain transactions (source Wikipedia)

In this section, we will describe how Bitcoin achieves distributed consensus to protect all Bitcoin-based transactions from hackers. The first step is to create a public and private key in the form of cryptographic hash to identify a participant on the Bitcoin blockchain. One can obtain such an identity pair by creating a digital wallet. All participants in this network will have a hash identity address which is

their public key. Any two entities now can create a transaction of say 10 Bitcoins between them which is termed as peer-to-peer transaction. When this transaction takes place by transferring 10 bitcoins from one hash pointer to another hash pointer, it is broadcast to all nodes; the transaction is completed and documented on the blockchain node.

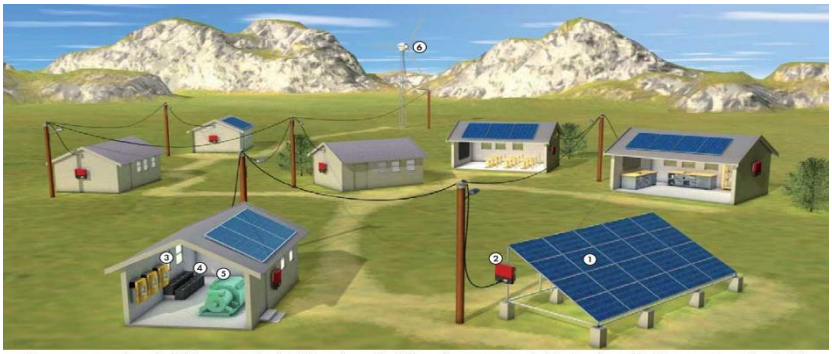
The distributed consensus protocol indicates that if there is a transaction between two entities it must be recorded on all nodes and all nodes must agree on the validity of the transaction. A transaction is accepted if at least six nodes agree and then it goes to a ledger as a new block which has a hash and the transaction data. If the transaction is not confirmed by at least six nodes it is not accepted in consensus chain, then it becomes an orphan node and discarded.

The blockchain transactions are confirmed by the miner nodes. The miner nodes are created by high performance computers whose operators compete to create new blocks by finding new transactions, and get paid by Bitcoin for creating new blocks as well as through transaction fees.

The transaction is protected by the 256-bit hash with a unique random number (nonce). In the Bitcoin blockchain the proof of work is created by miners solving the hash puzzle, which requires extensive compute power to find a unique random number (e.g. a large prime number) a previous hash and a ledger of transactions.

There is large community of miners who create the mining nodes. Bitcoin blockchain has a substantial number of mining nodes which makes it a very active blockchain, which in turn means that the decentralized transactions become hack proof, immutable, and transparent through distributed consensus between the blockchain nodes. Other cryptocurrencies, such as Ethereum, are called altcoin and have their own ways of achieving distributed consensus for the substantial number of distributed transactions. Each of these new cryptocurrencies have miner blockchain nodes confirming all transactions, which are rewarded by generating new coins and transaction revenue.

The blockchain framework thus is adding security, traceability and immutability of transaction to the internet, which makes highly decentralized systems possible. The most common application of the blockchain framework is for financial transactions. The smart contracts that do not require third party validations threaten to disrupt the financial industry by enabling peer-to-peer transactions without banks providing third party validations. The blockchain will bring efficiency to every level of financial business. A survey conducted by Cognizant to 1520 financial industry leaders indicate that 91% believe blockchain technology is critical for their future operations and 48% believe that blockchain technology will fundamentally change the fintech industry.



Components: 1. PV array, 2. IoT Device, 3. Microinverters, 4. Batteries, 5. Generator, 6. Grid

Figure 2The blockchain enabled solar microgrids

Another important example of blockchain technology is in the peer to peer transaction of electrical power generated form clean energy sources.

Solar panels can now integrate within a decentralized blockchain network, where the generated electrical power in kWhr can be transacted peer to peer without any central party validation. The local economy can then use either dollars or a cryptocurrency to buy and sell power generated by individual solar nanogrid owners, creating a city-wide solar power distribution system. Power2Peer is using this central idea of distributed consensus with the Ethereum blockchain platform to create a decentralized solar power distribution network for peer-to-peer trading (see Figure 2)

Contact: Nish Sonwalkar (nish@alum.mit.edu), Founder, Power2Peer.com

Further Reading:

1. Financial Services Building Blockchain One Block at a Time, Cognizant Report (June 2017)

https://www.cognizant.com/whitepapers/financial-services-building-blockchain-one-block-at-a-time-codex2742.pdf

2. Mike Orcutt (2017) "How Blockchain Could Give Us Smarter Energy Grid." MIT Technology Review

https://www.technologyreview.com/s/609077/how-blockchain-could-give-us-a-smarter-energy-grid/