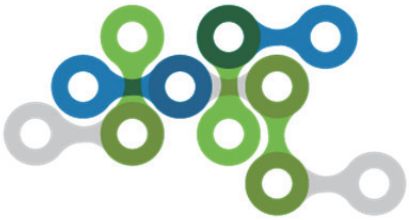
OneBeacon
TECHNOLOGY INSURANCE

A Member of OneBeacon Insurance Group®



Blockchain Technology

Bitcoin & Ethereum, Part 1

Author: Tushar Nandwana, Information Technology Risk Control

Published: October 2018

Note to our Readers

This paper is part 1 of 2 we have authored on the topic of blockchain. Part 1 delves into more detail on the technology of a blockchain and how it operates. The intended audience includes those interested in a deeper understanding of blockchain technology, particularly the technology that is the foundation of the Bitcoin and Ethereum cryptocurrencies which are the most notable applications of blockchain technology.

For information on Bitcoin currency, OneBeacon published a whitepaper on this topic in 2014.

Part 2 is less technical and reviews business applications of blockchain technology, and discusses its prospects for revolutionizing certain transactional processes for commercial and personal purposes.

Executive Summary

There are varying opinions regarding Bitcoin and cryptocurrencies and whether they will eventually replace fiat currency and bring on a new world order. Bitcoin's value reached nearly $22,000 in December 2017 driven primarily by speculation. However, since that time it has been undergoing a correction and as of October 4, 2018 is priced at $6,640. Cryptocurrencies may be experiencing growing pains but are certain to be a factor in how we pay for things in the future.

What is more important is the underlying technology of Bitcoin – the blockchain – which is a truly remarkable and highly disruptive technology. At its core, Bitcoin is simply a useful application of a blockchain platform. As noted by Kris Bennett at Blockchain Training Alliance, "bitcoin is to the blockchain what email is to the internet."[1] Bitcoin is one of the first consumer-grade applications of a blockchain. The blockchain is in its infancy but within 15-20 years, it may become as ubiquitous and indispensable as the internet.

What is a Blockchain?

Our discussion will be focused on the blockchain technology underlying Bitcoin and Ethereum as these are currently the most well-known and widespread applications of a blockchain. Part 2 of this whitepaper discusses other blockchain platforms that share some of the traits found in the Bitcoin blockchain, but also have key differences that make them more relevant for business usage.

A blockchain or distributed ledger technology (DLT) is cryptography-based, distributed, electronic ledger technology that is decentralized. It is "a structure for storing data in which groups of valid transactions, called blocks, form a chronological chain, with each block cryptographically linked to the previous one."[2] It records transactions in a decentralized way and enables a trusted ledger amongst trustless participants.

As it is decentralized, there is no central authority (like a bank or government) overseeing the process. It enables various parties to trust and agree on the state of the ledger system even where

the parties may have limited or no established trust in one another. This mechanism gives the system the functionality of a trusted, centralized, authority without the need for such control. Since the blocks form a chronological chain, there is visibility to the history of a transaction. Lastly, the use of cryptography to link these blocks makes the ledger immutable. Together, this makes the history of the transactions in the ledger immutable, unchangeable, transparent and trustworthy.

How does it Work?

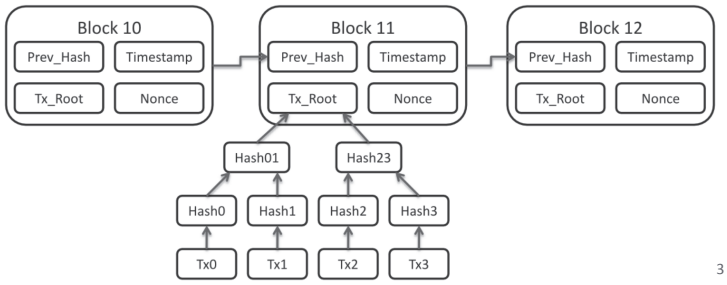
The key features of the Bitcoin/Ethereum blockchain or DLT include:

- Ledger – This is an electronic or digital system to record transaction data. For example - Alice pays Bob a bitcoin to purchase a product. A bitcoin is debited from Alice's account and credited to Bob's account in the ledger. Payments are made using digital wallets and signatures. The nodes (see below) that are mining the blocks will verify the transaction. They will check to see if Alice actually has sufficient funds in her wallet before processing the transaction. It is a triple-entry accounting system in that the ledger keeps a record of the transaction's debit and credit, and provides a link or chain to prior transactions for historical record and transparency.
- Decentralized – There is no centralized authority or arbiter overseeing the ledger. Control of the ledger is distributed amongst the different parties/computers on the network (also known as nodes) using this ledger. The level of control amongst the nodes may vary depending on the blockchain platform. For Ethereum and Bitcoin, all of the nodes have equal control. A node is generally a miner/computers/participant on the network; more information on nodes is provided here.
- Distributed – The ledger database is distributed, meaning that it is present on the computers of all parties or nodes in that network. Any change made to one ledger is automatically synchronized in the ledgers of the other nodes. This prevents one party from making unauthorized changes to the transactions (e.g. deleting or changing a payment) without alerting the other nodes. It also provides redundancy, as there is no single point of failure; there is no single centralized node that houses all of the ledger data. For example, Bitcoin and Ethereum average about 10,000 and 16,000 nodes, respectively.
- Cryptography or Hash Function – The use of a hashing algorithm to secure the payment transaction data into blocks and then chaining or linking these blocks to the prior block is one of the most important features of a blockchain.
    - Hashing algorithms used by the major blockchain platforms include SHA 256 for Bitcoin and KECCAK-256 for Ethereum.
    - Hashing converts an input string of alphanumeric characters or "message" (data from a transaction block) into a unique and hopefully one-of-a-kind fixed-length output of alphanumeric characters called a "digest."
        - For example - the SHA 256 algorithm generates a 64-character, hexadecimal digest. If converted to a decimal based number, it would be 74 digits long.
    - These hash algorithms are one-way functions, meaning that one cannot recover the input data (message) by putting the digest through another hashing function; there is no way to reverse engineer the process.
    - Examples of hashed digests for the message "Hello1" and "Hello2" are noted below. As you can see, changing one value in the initial message generates a new and unique digest. This prevents someone from determining the input message simply by inspecting other digests. It is also evidence of how the uniqueness of these digests prevents "collisions." A collision is when two different input messages have the same digest – which would be disastrous.
        - Hello1 - 948EDBE7EDE5AA7423476AE29DCD7D61E7711A071AEA0D83698377EFFA896525
        - Hello 2 - BE98C2510E417405647FACB89399582FC499C3DE4452B3014857F92E6BAAD9A9
    - In Bitcoin and Ethereum, transactions (A paying B) are packaged together using a hashing function to form a block (see diagram). A transaction contains information on which coins

to spend, and the recipient and payer identities, as defined by their wallets' digital signatures. Each transaction (denoted as Tx0, 1, 2, 3…) is hashed (Hash 0, Hash 1), then these are hashed again (Hash 01, 23, 45, …) until all of the transactions form a hashed Tx_Root or Merkle Root.

This is then combined with the block hash from the prior block, a time stamp, the transaction list, a number of other logistical data, and most importantly a nonce (see Proof of Work below). It is then hashed again to form the final block. By doing this, all of the blocks from block zero to the current block are linked or chained, thereby forming a blockchain. Although not shown in the diagram below, the transaction data is also appended to the block and is available for review when needed.

Any change made by any of the nodes to any of the transactions within a prior block revises the hash value (digest) of all of the following blocks. This would alert the other nodes that a change has been made. This step and the proof of work process results in the chain being immutable to changes and preserves the history of the transactions. For a Bitcoin blockchain, one can trace back every bitcoin to the date and time it was created – whether that happened yesterday or in January 2009 when Bitcoin was initiated.



3

- Consensus or Consensus Protocol – A software-encoded protocol by which nodes or participants on the network review and agree on the state of transactions and ultimately, the block itself.
- Proof of Work (PoW) – This is the consensus protocol used in Bitcoin, Ethereum and a number of other cryptocurrency blockchains.

To confirm a block onto the chain requires the nodes to solve a cryptographic puzzle, which requires extensive computing power and is therefore an expensive proposition. The PoW process deters attempts by nodes or users to commit fraud such as changing transactions in prior blocks. Changing prior nodes is costly from a computing power perspective as you would have to redo all of the PoW; the further back you go, the more computing resources it would require, thereby increasing the costs exponentially. This makes it highly unprofitable to pursue and this is an excellent deterrent to fraud.

A node that solves this puzzle correctly receives a reward of X number of bitcoins (12.5 coins at this time) or ether (currency in Ethereum platform) and/or a transaction fee (other blockchain platforms). This is the concept of mining and the nodes that are trying to solve the puzzle are called miners.

The Cryptographic Puzzle

So what is this cryptographic puzzle?

- The challenge is essentially finding a nonce – a unique number that satisfies the requirements of the blockchain platform. For Bitcoin blockchain, the process is as follows:
  - Requires that the node/miner guess an initial nonce or number and hash it with the block.

- The hashed digest is checked against a target value developed by the Bitcoin blockchain software.
- If the hash is greater than the target value, then the node increments the nonce, redoes the hash and compares again.
- This continues until a nonce value is found that generates a hash which is less than or equal to the target value.
- There could be a significantly large number of nonce values that can satisfy this requirement. However, the overall set of numbers that the node can consider as a nonce is exponentially larger, so it is really becomes a matter of being lucky when solving this puzzle. The more computing power a node can dedicate, the more likely they are to solve the puzzle.

- Once the correct nonce is determined, the node informs all of the other nodes on the network. The algorithm allows them to very quickly check and confirm or deny whether the nonce is correct. If correct and there is consensus with at least 51% or more of the nodes, then the block is confirmed and added to the chain. This process occurs every ten minutes as required by the Bitcoin platform.
- The target value is known to all nodes on the network as it is generated by the Bitcoin blockchain platform. The current target value is - 0000000000000000000275a1f0000000000000000000000000000000000000000000[4] and it is adjusted by the Bitcoin blockchain platform every 2016 blocks, or about 2 weeks depending on how quickly or slowly the nodes are solving the puzzle.
- If the nodes solve the puzzle very quickly, the platform increases the difficulty in solving the puzzle.

A concern with PoW consensus is that over time, it becomes quite expensive to solve. There is an exponential increase in computing power and financial cost, and it may become impractical for enterprise/business to use a blockchain requiring PoW consensus.

A more practical approach for enterprise/business application is to use Proof of Stake (PoS) or other consensus protocols. These are discussed in Part 2 of this white paper.

The Ethereum blockchain currently uses a PoW consensus but due to the computing and related energy costs involved, they are considering a move to a PoS consensus sometime in 2018.

Types and kinds of Blockchain platforms

Blockchain platforms can be public or private and the ledger types can be permissioned or permissionless. There isn't a single qualified definition of this but loosely we have the following:

- Public or Private – Determines who can read or write data to the ledger.
  - A public blockchain is completely open and anyone can join, participate, read or write into the network.
  - For a private blockchain, participants are authenticated and validated by the owner/operator of the blockchain network before they can perform any activities on the blockchain.
- Permissioned or Permissionless – Indicates whether all users/nodes on the blockchain are equal or not; it clarifies who can validate a block and who cannot. It also indicates whether the users are known or anonymous. Anonymous users have a digital ID but no other indication of who they truly are.

Bitcoin and Ethereum are public and permissionless blockchains that are open to all and everyone can contribute (read, write and audit). This means that everyone can also view all of the

transactions that occur on the blockchain due to its inherent transparency. That being the case, the Bitcoin blockchain is clearly not used for any enterprise or business application. It lacks a scripting language for smart contracts and its transaction confirmation rate is extremely slow for business applications.

Ethereum blockchain has capability for enterprise uses but these applications could be limited due to the transparency of all of the transactions.

Conclusion

The purpose of this paper was to provide the reader with a glimpse of how the blockchain technology works – specifically how cryptographic elements are used to create an immutable, distributed ledger that operates in a decentralized environment and enables trust amongst trustless participants. With this understanding, the reader should be better able to understand Part 2 of this whitepaper which focuses on blockchain platforms that are geared towards enterprise/business and ultimately consumer applications.

Contact Us

To learn more about how OneBeacon Technology Insurance can help you manage online and other technology risks, please contact Dan Bauman, SVP of Risk Control for OneBeacon Technology Insurance at dbauman@onebeacontech.com or 262.623.6558.

References

[1] Richardson, Melissa; Bennett, Kris. (November 25, 2017). "Ethereum vs. Hyperledger." Blockchain Training Alliance and training video on YouTube. Accessed June 2018 https://blockchaintrainingalliance.com/blogs/news/ethereum-vs-hyperledger

[2](April 23, 2018). "A glossary of blockchain jargon." MIT Technology Review. Accessed June 2018. https://www.technologyreview.com/s/610885/a-glossary-of-blockchain-jargon/

[3]"Can someone explain how the Bitcoin blockchain works?" Blog. Accessed June 2018. https://bitcoin.stackexchange.com/questions/12427/can-someone-explain-how-the-bitcoin-blockchain-works

[4] Learn me a Bitcoin. Accessed June 2018. http://learnmeabitcoin.com/glossary/target