OneBeacon
TECHNOLOGY INSURANCE

A Member of OneBeacon Insurance Group®

Blockchain Technology and its Future, Part 2

Author: Tushar Nandwana, Information Technology Risk Control

Published: October 2018

Note to our Readers

This paper is part 2 of 2 on the topic of blockchain. Part 1 provides technical insight on the blockchain technology that is the foundation of the Bitcoin and Ethereum cryptocurrencies, one of the most recognizable applications of blockchain technology.

Part 2 is less technical as it reviews different types of blockchain platforms, business applications using this technology and how it may soon revolutionize certain enterprise and consumer transactional processes.

Executive Summary

Globally, spending on blockchain applications is projected to increase from $945M in 2017 to $2.1B in 2018 as more projects move from proof-of-concept to deployment, with 40% of the spending in 2018 occurring in the U.S.[1] By 2024, forecasts indicate that the blockchain market could be worth up to $60.7B worldwide.[2] "Many see the technology's rise as a vital new phase in the internet economy – one that is, arguably, even more transformative than the first…(and) this movement challenges the whole idea of a for-profit middlemen altogether."[3]

What is a Blockchain?

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."[4] 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. Alternatively, 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, and trustworthy. The level and who has visibility into the transactions could vary depending on the blockchain platform.

Consensus Protocol

Consensus protocol is 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. Part 1 of this whitepaper discussed that the Bitcoin platform uses a Proof of Work (PoW) consensus protocol and provides detail on how it works.

A concern with PoW consensus is that over time, it becomes quite expensive to solve as there is an exponential increase in computing power and cost. This makes it impractical for businesses or

enterprises to use blockchain platforms that use PoW consensus protocol. A more practical approach is to use Proof of Stake or other protocols to ensure consensus in the network.

- Proof of Stake (PoS) – This is the consensus protocol for Hyperledger Fabric and a number of other blockchain platforms. Ethereum currently uses PoW but there is an effort to switch this to PoS due to computing and cost concerns noted above. This should occur in 2018.

  PoS is a "consensus protocol in which, instead of mining, nodes can validate and make changes to the blockchain on the basis of their existing economic state."[5] Instead of miners, we have validators – nodes that validate the transactions in a deterministic fashion and complete the blockchain. These nodes stake an amount of their capital, asset or cryptocurrency if they want to process a block. If they are successful at solving the puzzle, they are rewarded with a like amount. If not, they do not lose anything. However, if they are committing fraud or attempting to fraudulently validating a transaction, the other participants in the network can strip them of their stake resulting in a loss for the node; this acts as a deterrent against fraud.

  PoS rewards the validators through transaction fees paid for by the users of the block undergoing verification and inclusion into the blockchain.

  Depending on the blockchain platform, consensus could range from 100% of the nodes having to sign-off, to a majority, or to a group of nodes that is randomly selected by the platform.

- Other – There are a number of other consensus protocols such as Delegated Byzantine Fault Tolerant (DBFT), Practical Byzantine Fault Tolerant (PBFT), Proof of Elapsed Time, Proof of Authority and others. These alternatives are quite complicated and outside of the scope of this discussion.

Types of Blockchain platforms

Blockchain platforms can be public or private and the ledger types can be permissioned or permissionless. A single qualified definition does not exist, 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 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 public or 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 visibility into the transaction. On the other hand, another blockchain platform called Hyperledger Fabric is private, permissioned and visibility is limited to permissioned nodes/participants in the network.

Private and permissioned blockchain platforms are partially decentralized as there could be a one or a number of entities on the network that have more control than others. These platforms could be favored for business applications.

The Future of Blockchain

The Bitcoin blockchain is not suitable for corporate use since it lacks scripting language for smart contracts and tends to have extremely slow transaction confirmation rate; it takes ten minutes for a transaction to clear (for a block to be added to the blockchain).

Business Enterprise Blockchain platforms

Therefore, for enterprise usage, there is a need for blockchain platforms that process transactions quickly and have scripting language so that smart contracts or chaincode (see below) can be developed for different business applications. Business-friendly platforms include Ethereum, Hyperledger Fabric, R3 Corda, Quorum, Ripple and others. These have their pros and cons as outlined below:

	Ethereum	Hyperledger Fabric & Flavors	R3 Corda	Quorum	Ripple
Industry Focus	Various industries	Various industries	Financial Services	Various industries	Financial services
Governance	Ethereum Enterprise Alliance	Linux Foundation	R3 Consortium	Ethereum and JP Morgan	Ripple Labs
Ledger Type	Permission-less	Permissioned	Permissioned	Permissioned	Permissioned
Public or Private	Public	Private	Private	Private	Public
Consensus Algorithm	PoW but changing to PoS	Pluggable Framework*	Pluggable Framework*	Majority voting	Probabilistic voting
Currency	Ether	None	None	None	Ripple (XRP)
Smart Contract	Yes	Yes	Yes	Yes	No

* NOTE – Pluggable framework means that the each group using Hyperledger Fabric or R3 Corda is able to plug in or use different consensus protocols as needed by their application. Since these are private, the users of these platforms have this flexibility and can use a protocol that best suits their needs and purpose.

- Ethereum – Launched in July 2015, it is able to process transactions within approximately 15 seconds and has scripting language to create smart contracts. However, since it is public and open, any smart contracts that operate on this platform would not be private; they would be fully viewable by all participants. For example, all transactions that have occurred in Ethereum since inception can be found here. It may work for some businesses but it may not be best option for commercial enterprises that want to maintain private transactions.

- Hyperledger – This was launched in December 2015 and is governed by the Linux Foundation. It is an umbrella project of open-source blockchains. It has scripting language to create and enable smart contracts/chaincode. It includes a variety of flavors supported by different companies for specific applications. For example:
  - Hyperledger Fabric – Developed by IBM for use in business applications. This appears to be the leading flavor of Hyperledger due to its enterprise focus.
  - Sawtooth – Developed by Intel for use with IoT (internet of things).
  - Iroha – Developed by Soramitsu for use in the mobile space.
  - Others – Burrow, Indy and others.

  In the Hyperledger Fabric platform, nodes or participants are defined with specific permission levels on the network and are known as endorser, peer and orderer; this defines the level of control a node has in the network. By varying the permission levels for the nodes, it improves the performance of the platform.

It allows for the use of various consensus protocols to suit the user group's requirements and needs.

A major benefit of Hyperledger Fabric is that it processes transactions faster than Ethereum. In addition, since it is private, there are fewer expenses and no transaction fees. It will likely be the platform of choice for business applications in the future.

- R3 Corda – This also launched in 2015 and is open-source and designed specifically for banking, but can be used in supply chain, healthcare, trade finance and by government entities. The R3 Consortium consists of large, global banks.
- Quorum – It is an Ethereum-based platform but developed further by JP Morgan for use in a variety of industries.
- Ripple – This was launched in 2012. It does not have smart contract capability but is used by financial institutions and others for cross-border payments.

Blockchain Applications

Due to the immutable and reliable nature of a blockchain, it can be used in business processes that require an attestation or confirmation about the history of a product or service. Because of its full to partial decentralized nature, it can be a disruptive force in business processes that traditionally have centralized or middleman oversight.

Specifically, it can radically change the financial services sector "which can span across payments, capital markets, trade services, investment and wealth management, securities and commodities exchanges, (and) it could reduce financial services infrastructure cost between U.S. $15 billion and $20 billion per annum by 2022."[6] Some applications include:

- Smart contracts or Chaincode – This is simply code that acts to do something when certain conditions are met. It defines rules and processes that get invoked when certain activities occur. For example - automatically conduct a specific transaction once there is confirmation that payment has been made.
- Payment and Micropayments – This is the ability to send monetary funds to another party without using a bank, thereby reducing fees and speeding up the transaction. American Express and Spain's Banco Santander are using Ripple to allow users to send non-card payments to the UK.[7]
- Streamlining Business Processes – Certain auditing processes can be eliminated as all relevant parties have the correct information with a historical record. This could decrease manual processing and duplication with "70% potential cost savings on central finance reporting."[8]
- Banking, financial post-trade and settlement activities – These could be redesigned and become less onerous with blockchain technology resulting in "50% potential cost savings…"[9] On a cost basis of $30 billion, blockchain technology could result in $10 billion in annual cost savings.[10]
- Insurance sector – It may be used in product development and claims handling. A start-up called InsureETH developed a flight insurance policy using the Ethereum blockchain. It pays the policyholder a set amount in case their flight is cancelled or delayed by a certain time. This is accomplished using smart contracts that rely on verified flight data sources. In another application, information on claims payment can aid in reducing fraud as multiple claims for the same event would be rejected by the network, enabling insurers to identify suspicious behavior as the blockchain would have historical data.[11]
- Enterprise Supply Chain Management – It can be used to confirm the authenticity or provenance of the supply from all suppliers that provide any component of a product – from birth to death. This can be used to prevent fraud and counterfeiting, as well as improve recordkeeping and recall process. Examples include pharmaceutical, electronic components, organic foods and so on.
- Medical clinical trials – Clinical trial data can be added to a private blockchain and due to its timestamp and immutable nature, it can ensure the safety, integrity and authenticity of the

trial data and informed consent data for relevant parties.[12] Furthermore, data duplication can be minimized when sharing with regulatory bodies (e.g. FDA, other) or others.

- IoT devices – Cisco along with 17 other companies launched the IoT Alliance in September 2017, which includes the development of a proprietary blockchain protocol for IoT devices[13] to develop trust, and validate and authenticate IoT devices connected to a network.
- High-end Retail – It can be used to ensure products (e.g. diamonds, fine wine) are not counterfeit as the blockchain can attest to the item's integrity as it moves from supplier, to manufacturer, to distributor and finally, to the customer.
- Streamlining real estate transactions – Blockchain can eliminate the need for a title search company as the history of the property is fully known to all relevant parties, or it can expedite a purchase transaction by reducing duplication of data.
- Other potential uses – Digital rights management, healthcare, auction/online marketplaces, aerospace, data storage in the cloud, voting systems and voting records, government systems, digital betting and video gaming, any industry with a supply chain (e.g., construction, etc.), national defense and others.

Issues & Problems

As with any emerging protocol, there are a number of issues with blockchain technology at this time:

- Most blockchain platforms were released within the past two to three years so it is continually changing and expanding. Applications are being researched and tested and will require time before being production-ready. There is a lot of hype as practitioners appreciate that not all processes need to be "blockchained." There will be failures and a growth curve before success becomes the norm.
- New platforms may not be fully tested and may have technical issues or "bugs" that undermine the platform. Think of the Dao hack in 2016 that resulted in a theft of $150 million in ether.
- The technology is complex and many may not understand how to use it appropriately.
- Transaction processing rates may not be fast enough for many platforms and there is concern with scaling – or the ability to process more transactions quickly. This may slow down adoption rates.
- Smart contracts are code-based and could have software bugs that cause the contracts to fail or become corrupted.

Conclusion

Blockchain technology holds a lot of promise, but as with any disruptive technology, there will be a number of false starts and failures – some of which may be significant. This is part of the learning phase and there will be growing pains before the technology becomes resilient and ubiquitous. Just think of how the internet has evolved over time. The initial excitement is there but not all processes or applications need to be "blockchained."

It may take 10 or even 15 years before this technology becomes an indispensable part of our lives – similar to how the internet or smartphones are today. Good adoption of the technology will take time. There will be considerable growth in this sector as new firms enter the marketplace to develop blockchain applications and provide services to companies. It will also be disruptive and may change or even eliminate many aspects of today's business processes and those that offer middlemen types of services. The next few years will definitely be quite interesting as we engage with blockchain and become increasingly linked to its practical usefulness.

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] Ghosal, Anirban. (January 25, 2018). "New IDC spending guide sees worldwide blockchain spending growth to $9.7 billion in 2021." Accessed June 2018 https://www.idc.com/getdoc.jsp?containerId=prUS43526618, https://www.vccircle.com/global-spending-on-blockchain-solutions-to-reach-2-1-bn-in-2018-idc-report/

[2] (February 14, 2018). "Blockchain market size is anticipated to reach USD 60.7 billion by 2024." Market Reports Center. Accessed June 2018. https://globenewswire.com/news-release/2018/02/14/1347823/0/en/Blockchain-Market-Size-is-anticipated-to-reach-USD-60-7-billion-by-2024.html

[3] Vigna, Paul and Casey, Michael. (May/June 2018). "In blockchain we trust." MIT Technology Review. Page 10. Accessed June 2018

[4] (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/

[5] ibid 4

[6] Gregorio, Max Di. (February 2017). "Blockchain: a new tool to cut costs." Pricewaterhouse Coopers. Accessed June 2018. https://www.pwc.com/m1/en/media-centre/articles/blockchain-new-tool-to-cut-costs.html

[7] Williams, Sean. (January 10, 2018). "The Basics of Blockchain Technology, Explained in Plain English." Motley Fool. Accessed June 2018. https://www.fool.com/investing/2018/01/10/the-basics-of-blockchain-technology-explained-in-p.aspx

[8] (2017). "Banking on Blockchain – A value analysis for investment banks." Accenture Consulting. Page 5. Access June 2018. https://www.accenture.com/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Consulting/Accenture-Banking-on-Blockchain.pdf

[9] ibid 8, Page 5

[10] ibid 8, Page 6

[11] ibid 6

[12] Benchoufi, Mehdi; Procher, Raphael; Ravaud, Philippe. (February 1, 2018). "Blockchain protocols in clinical trials: Transparency and traceability of consent." F1000 Research. Accessed June 2018. https://f1000researchdata.s3.amazonaws.com/manuscripts/15062/87d9b2cd-ca90-411c-ba90-fb252c21abbe_10531_-_Mehdi_Benchoufi_V5.pdf?doi=10.12688/f1000research.10531.5

[13] Freeman, Mary. (September 21, 2017). "Blockchain in retail: Cisco launches new IoT alliance." Accessed June 2018. https://blogs.cisco.com/retail/blockchain-in-retail-cisco-iot-alliance