CYBERSECURITY
RESEARCH LAB

CRL 101 Series

Blockchain Technology

By Ryan Kennedy & Dr. Atefeh Mashatan

Introduction

Blockchain technology, the buzz word that has been in the ears of academics, managers and everyday people for years. Indeed, blockchain technology is an emerging and disruptive innovation yet, few have a tangible understanding of what it is, what can it do, and what challenges it may bring. Since its inception in 2008 (Nakamoto, 2008), the blockchain market has been slow to grow, valued at 1.2 billion in 2018. However, recent estimates project the market to be worth 23.3 billion by 2023 (Business Wire, 2018). With such a high projected growth rate, for the near future, now is the time to begin understanding the technology; especially with blockchain's positive potential for individuals, organizations and society. For those ready to understand blockchain, this short paper will shed some light into this popular, but poorly understood technology.

Defined & Explained

Blockchain Technology can be visualized as several existing technological components coming together to create a new form of distributed database. In its basic form, a blockchain is a tamper evident and resistant, append only, distributed leger composed of ordered blocks, consisting of digitally signed transactions (Yaga et al., 2018). Blockchains are implemented in a distributed, public or private network, without a central repository and usually without a central authority (Yaga et al., 2018).

With a blockchain, transactions can take several forms, such as exchanges of financial value, code representing smart contracts, and/or a record of a digitized asset (Makhdoom et al., 2019; Wang et al., 2019). Digital signatures are used to conduct transactions, whereby public keys are used to create wallet addresses and private keys are used to authorize/spend transactions (Narayanan et al., 2016). Specifically, to transfer value, the owner digitally signs the hash of a previous transaction (holding the value one wants to transfer) and the public key of the next owner (Nakamoto, 2008). Transactions are publicly broadcast to the network to be collected, validated, and formed into blocks.

Once validation and consensus are performed on blocks within the network, they are time stamped, added to the ledger (chain), and cryptographically linked to the predecessor block (Li et al. 2019; Zamani et al., 2018). The nature of validation and consensus depends on the specifics of the blockchain solution architecture. For example, the consensus mechanism for the Bitcoin

blockchain is known as the proof-of-work (PoW) mechanism, but several other variations have been developed such as the Proof-of-Stake (PoS) model (Yaga et al., 2018). Regardless of the mechanism, mining-nodes within the network perform the consensus.

Having blocks cryptographically linked together ensures transactions within a block are tamper evident. This is due to the properties of the hash function used to chain blocks together. If a single transaction, within a block is changed, the result of the hash function used to chain blocks together will change and be evident to the network (Narayanan et al., 2016). In other words, the ledger is append only. To change the history of the ledger, an attacker must solve the PoW consensus mechanism (assuming the attack is on the Bitcoin blockchain) faster than all other network participants combined; an extremely difficult task to do (Narayanan et al., 2016). When a block is added to the ledger, all nodes within the network update their copies of the blockchain which ensures a single version of the truth (Zamani et al., 2018).

Several different types of blockchains exist and at their basic level, differ based on the network permissions (Yaga et al., 2018). A public blockchain, for example, is permissionless. It is open to anyone without needing permission from an authority. Anyone can download the software (which is usually open source) and read and write transactions to the blockchain. A private blockchain is permissioned. Users need authorization to gain access to the network, their identities are known, and read/write permissions can be restricted. A third type is the hybrid blockchain, which is an amalgamation between public and private (Yaga et al., 2018).

Benefits

Blockchain technology is poised to benefit individuals, organizations and society. The benefits of blockchain technology are numerous and frequently depend on both the type of blockchain and use case making it difficult to discuss each in depth. However, in general blockchain technology allows for; disintermediation of 3rd parties, transaction non-repudiation, tamper evident data, automation capabilities, streamlined processes, increased efficiency, reduced costs and increased trust (Hughes et al., 2019). Blockchains also allow for data provenance, direct transactions in a trust-less network, instant tracking and tracing of assets, and a robust security model (Lacity, 2018). Blockchain technology also has indirect benefits. For example, imagine using a blockchain within the pharmaceutical industry, whereby organizations can provide data provenance on all drugs, ensuing their validity and safety. The use of blockchain technology in this case could serve to directly aid the pharmaceutical organizations but would also indirectly help increase public health. This is just one use case. With blockchain developments in finance, healthcare, governance, education, transportation, supply chain/logistics, energy, and more (Shen and Pena-Mora, 2018; Casino et al., 2019), one can only imagine the positive impacts to come.

History

Although many of the core ideas behind blockchain technology had existed before its conception, they were first combined in 2008 in a paper titled *Bitcoin: A Peer to Peer electronic cash system* (Nakamoto, 2008) written by the infamous Satoshi Nakamoto (A pseudonym, as the original author is unknown). In the paper, Nakamoto describes the Bitcoin cryptocurrency blockchain network, the first of its kind. This phase of blockchain's development has frequently been coined blockchain 1.0 and the focus is largely on transactions and cryptocurrencies (Angelis and Ribeiro da Silva, 2019). Bitcoin inspired others to consider the technology and over the next several years many Blockchains were developed, each providing a slightly different function. Blockchain 2.0 extends version 1.0 to include privacy considerations, smart contracts, and asset tokenization (Angelis and Ribeiro da Silva, 2019). One of the most notable developments of blockchain 2.0 is described in Buterin's seminal work titled; *A Next-Generation Smart Contract and Decentralized Application Platform* (Buterin, 2018). Buterin describes a new blockchain called Ethereum and how it is both different and better than Bitcoin. Ethereum has a built in Turing-complete programming language which allows users to write applications and smart contracts (Buterin, 2018). This is a significant improvement from Bitcoin, which only allows for peer to peer transactions and has a limited scripting language. Blockchain 3.0 was characterized by the introduction of decentralized applications (dApps). A dApp is an application with its back-end code operating on a decentralized peer-to-peer network which greatly extends the possibilities when using blockchain technology (Angelis and Ribeiro da Silva, 2019). Buterin (2018) describes three categories of applications that can operate on top of Ethereum; Financial applications (powerful ways to use money), semi-financial applications (money is involved but the applications also include a non-monetary side) and non-financial. Some examples include, token systems (tokens representing an asset), identity systems, reputation systems, decentralized file storage, insurance, gambling and/or prediction markets (Buterin, 2018). Blockchain 4.0 is about integration with industry and other technology such as the Internet of Things (IoT) and Artificial Intelligence (AI). It is about making blockchain usable for real business solutions.

An Important Distinction

Blockchain technology is not a synonym for cryptocurrency. They are not the same thing but are related. Blockchain technology can be viewed as a higher level of abstraction than cryptocurrency. In other words, cryptocurrency is just one tool or function of blockchain technology, depending on how it is viewed. For example, with the Bitcoin blockchain, Bitcoins serve as an incentive structure to reward miners for performing consensus and a means of transferring value (Nakamoto 2018; Narayanan et al., 2016). In Ethereum, cryptocurrency also provides an incentive to mine and a means of transferring value. Ether, the cryptocurrency for Ethereum is comparable to the gasoline one puts in a car. In fact, Ether, the cryptocurrency for Ethereum is referred to as gas but instead of powering a car, it powers smart contracts. The specific

nature of the relationship of Ether or gas to smart contracts is that, based on the amount of calculations a smart contract completes, a certain amount of gas is required (Buterin, 2018). In other blockchains, cryptocurrencies are simply used to digitally tokenize tangible assets and some blockchains do not have a cryptocurrency at all.

Challenges

As great as blockchain technology is, it is not without its challenges. The challenges can be divided into technical challenges and business. Technical challenges for blockchain surround the technology itself and include; scalability (throughput and latency), consensus (PoW is not energy efficient and allows for selfish mining), key management difficulty and risky, network updates or modifications (causing forks in the chain), the immutability (mistakes with smart contracts), security (51% attacks), privacy (no confidentiality), interoperability (blockchain to blockchain and blockchain to legacy technology), cost, complexity and usability.

On the other hand, the business challenges are framed around the difficulties to implement blockchain technology into an organization and include; the immaturity/novelty, governance establishment, regulation and standardization (the lack of and compliance with existing regulation and standardization), lack of knowledge and skills, legacy infrastructure (people, process and technology) re-engineering, change management, fear of the unknown/ of change, and changing the current organizational mindsets (collaborate with competitors or shared intellectual property).

Here at the Ryerson Cybersecurity Research Lab (CRL), blockchain technology adoption is an active stream of research. We have developed a Blockchain Adoption Framework, and actively research the challenges and drivers of blockchain adoption to develop methods to reduce barriers and foster widespread organizational adoption.

July 15, 2019
CRL 101 Series

References

Angelis, J. and Ribeiro da Silva, E. (2019), "Blockchain adoption: a value driver perspective", *Business horizons*, Vol. 62 No. 3, pp. 307-314.

Buterin, V. (2018), "A next-generation smart contract and decentralized application platform", available at: https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf.

Business Wire. (2018), "The global market for blockchain (2018-2023): projected to expand at a CAGR of 80.2% - ResearchAndMarkets.com", available at: https://www.businesswire.com/news/home/20181210005600/en/Global-Market-Blockchain-2018-2023-Projected-Expand-CAGR (accessed 2 July 2019).

Casino, F., Dasaklis, T. K. and Patsakis, C. (2019), "A systematic literature review of blockchain-based applications: Current status, classification and open issues", *Telematics and Informatics*, Vol. 36, pp. 55-81.

Hughes, L., Dwivedi, Y. K., Misra, S. K., Rana, N. P., Raghavan, V. and Akella, V. (2019), "Blockchain research, practice and policy: applications, benefits, limitations, emerging research themes and research agenda", *International Journal of Information Management*, Vol. 49, pp. 114-129.

Lacity, M. (2018), "Addressing key challenges to making enterprise blockchain applications a reality", *MIS Quarterly Executive*, Vol. 17 No. 3, pp. 201-222.

Li, J., Greenwood, D. and Kassem, M. (2019), "Blockchain in the built environment and construction industry: a systematic review, conceptual models and practical use cases", *Automation in Construction*, Vol. 102, pp. 288-307.

Makhdoom, I., Abolhasan, M., Abbas, H. and Ni, W. (2019), "Blockchain's adoption in IoT: the challenges, and a way forward", *Journal of Network and Computer Applications*, Vol. 125, pp. 251-279.

Nakamoto, S. (2008), "Bitcoin: A peer-to-peer electronic cash system", available at: https://nakamotoinstitute.org/bitcoin/ (accessed 29 June 2019).

Narayanan, A., Bonneau, J., Felten, E., Miller, A. and Goldfeder, S. (2016), *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*, Princeton University Press, Princeton, NJ.

Shen, C. and Pena-Mora, F. (2018), "Blockchain for cities-A systematic literature review", *IEEE Access*, Vol. 6, pp. 76787-76819.

Wang, Y., Wang, J., Singgih, M. and Rit, M. (2019a), "Making sense of blockchain technology: how will it transform supply chains?", International Journal of Production Economics, Vol. 211, pp. 221-236.

Yaga, D., Mell, P., Roby, N. and Scarfone, K. (2018), "Blockchain technology overview", available at: https://doi.org/10.6028/NIST.IR.8202 (accessed 30 June 2019).

Zamani, E., He, Y. and Phillips, M. (2018), "On the security risks of the blockchain", *Journal of Computer Information Systems*, pp. 1-12.