Blockchain for Cybersecurity - Standards & Implications

– Vinod Kumar Mishra
Blockchain Consultant with Upgrad
https://orcid.org/0000-0002-8416-9158 vkumar201415@gmail.com

Article History
Paper Nomenclature:
Experiential Research Papers (ERP)
Paper Code: CYBNMV1N5OCT2019ERP1
Submission Online: 08-Oct-2019
Manuscript Acknowledged: 09-Oct-2019
Originality Check: 12-Oct-2019
Originality Test Ratio: 4%
Peer Reviewers Comment: 15-Oct-2019
Blind Reviewers Remarks 17-Oct-2019
Author Revert: 20-Oct-2019
Camera-Ready-Copy: 25-Oct-2019
Editorial Board Citation: 28-Oct-2019
Published Online First: 31-Oct-2019

Cybercrime is estimated to cost most than $500 to individuals and businesses. The CEO and chairman of IBM, Ginni Rometty said in an occasion "cybercrime, by definition, is the greatest threat to every profession, every industry, every company in the world."

Blockchain technology is seen as a promising emerging technology to benefit the cyber security domain. Blockchain technology is made up of different components working together in a distributed decentralized network. The technology ensures 'trust' into the completely untrusted network with unknown parties.

Keywords : Cybercrime | Blockchain System | Protocols

Introduction

The Blockchain based cyber security is different from standard cyber security in the following ways:

	Blockchain Security	Standard Cyber Security
1.Architecture	The basic architecture is decentralized and distributed among untrusted set of computers (nodes)	The general design has centralized computers/ servers under the control of security team of the company.
2. Properties	The properties are Integrity and availability.	The attributes are Confidentiality and integrity.
3. Security	Security in blockchain is based on the fact that multiple copies of the same data exist on various systems at the same time (world state). Also, the data is secure since it is cryptographically linked with a timestamp of older records/transactions.	All the computers/servers along with the restricted user roles are under the control of the organisation. So the priority is to prevent unauthorized access to the attackers from outside the network. While many organisations are making the shift to cloud-based environments, they still have a high degree of control over the security and configuration of their rented systems.
4. Denial of Service attack	In blockchain, a denial-of-service attack involves submitting more transactions to the blockchain than it can handle. The block size is fixed for most of the blockchain projects with a defined time period for creation of new blocks which is replicated in the peer to peer network. The attacker can, therefore, exceed the defined maximum capacity rendering the blockchain system unusable.	The denial of service attacks targets the centralised server of the company to prevent users from using its services. This attack is performed by creating more and more connection requests that the server is capable of supporting.

5. End Point security	The end points in Blockchain based systems are the peer nodes which may be completely homogenous. A homogeneous network is a network in which a error in one system may exists in all the systems in the network.	The end points in traditional systems are under the control of the organisation and a higher chance of heterogeneity exists. A heterogeneous system is a system where multiple ways of vulnerability may exist into the network.
8. Code Vulnerabilities	The business logic can be programmed in form of smart contracts in the blockchain based system. But any flaw in the smart contract or the underlying logic in the decentralized network may have adverse consequences. The only hack which have occurred in the bitcoin network till date took place due to integer overflow vulnerability in the Bitcoin protocol. The attacker on the bitcoin network was able to assign himself more bitcoins than it ever existed into the network. The Bitcoin network reacted by hard forking the Bitcoin network to ensure that the integrity and the worth of Bitcoin is maintained. So, any node or person in the blockchain based network needs to understand the risks in a distributed decentralized system.	The business logic is programmed by the organisation itself and any vulnerability can only exist from the code which the organisation owns.
9. Intentional Misuse	Intentional misuse of the system can take place only if the miners or nodes control more than 51% of the computational power in the network. This implies in systems where POW consensus protocol is used.	Attacks by the employees of the organisation such as database administrator is possible.
10. Data Protection	The data is protected by strong cryptographic algorithms in the distributed decentralized network to provide integrity and availability.	The data exists in multiple applications and are controlled by the authorized entities of the organization who aims to provide confidentiality, integrity, and availability.

Impact of Blockchain in different industries

Blockchain technology is been explored and adopted by the leading organizations in multiple industries to resolve cybersecurity issues such as:

Finance:

The banking and the fintech sectors are early adopters of Blockchain technology with the maximum number of use cases being explored in the domain. A report from the US Office of the Comptroller of the Currency (OCC) had suggested that most of the phishing attacks target the employees and the risk can be minimized by using multi layered decentralized security layer.

The largest financial institution of US i.e. JP Morgan had already developed a Blockchain based platform called Quorum for enterprise-based use cases. It provided a $150 million dept to the National Bank of Canada which is tracked and managed by the Blockchain system.

Santander group which is the 16th largest banking institution in the world has implemented "One Pay FX" which is a solution already used in countries like Poland, Spain and UK to transfer money between the accounts of Santander in South America and Europe. It is also creating pilots to explore the use of Blockchain technology in shareholder voting.

Barclays has filed a patent to store the KYC of its customers on Blockchain based systems. It is also implementing Blockchain to enhance the security in fund transfer.

Government:

The Government of almost all major countries in the world has been exploring Blockchain technology and its impact in improving governance and citizen services. Some of the most widely explored use cases are vehicle registration, citizen identity and land registration.

The Australian government has prioritized to use Blockchain technology to improve the cybersecurity into the network. It is also using DLT to digitalize and store its documents securely.

The state of Colorado in US has implemented Blockchain technology to improve the encryption and protect its vital network. The state was facing an attack with the intensity of six to eight million per day on the existing network. It is planning to pass more bills in enhancing the cyber security of the government network.

Malta which is a small European island country is implementing Blockchain based cyber security measures to protect its documents. It is emerging as a innovation hub for the technology.

Healthcare:

Healthcare industry is also prone to cyber attacks and with the emergence of new devices operating on the network the necessity for more security of the network is immense. It is believed that the healthcare network experiences malware attacks and phishing emails twice than any other industry. The healthcare industry has very critical records of the individuals including the health records which is used by the cyber criminals to demand money and blackmail in the dark market.

Philip Healthcare which is a research unit of Philip Research firm is using Blockchain technology to secure all the data which is collected by its Artificial Intelligence based system which is operational in multiple hospitals. It is used to discover and analyse the entire aspects of the healthcare system.

Hashed Health which is a US based consortium of leading health companies had created a working group to improve the health record and the payment system for all hospitals across US.

Military and Defence:

According to a report from Accenture more than 86% of defence companies plan to integrate Blockchain for cyber security in the next 3 years. The defence-based companies are using the decentralized encryption-based techniques to improve security and enhance privacy.

The technological development unit of US Army which is the Defense Advanced Research Projects Agency (DARPA) is exploring blockchain technology for secure data transfer and encryption of the records. It is creating messaging system created on Blockchain technology to securely message information without the risks of hackers.

The Chinese military is also said to be exploring Blockchain technology to securely store the records in tamperproof ledgers.

A defence-based contractor in US i.e. Lockheed Martin is developing Blockchain based protocol to protect every step of weapon development and its security.

Supply chain:

The Global supply chain-based organizations is exploring the use of Blockchain technology to improve the security and enhance trust into the entire process. Organizations like Walmart are piloting Blockchain technology is China and US to track the products from farm to the end consumers.

Blockchain is being explored in the supply chain of Diamonds, wine, fashion products, agricultural products and oil.

Cyber security protocols in permissioned Blockchain

Most of the implementations using Blockchain focuses on permissioned blockchain system. A permissioned blockchain based system is a network where the actors participating in the decentralized are known and the authority to create blocks is restricted to few users. The immense adoption and implementation of blockchain technology in major industries needs to consider the use of standard protocols. There are many standards which are still under development.

The following features of Blockchain technology are inherently favourable for cybersecurity:

- Distributed Architecture: The distributed architecture of the decentralized blockchain network prevents cyber attacks targeted at centralized databases. Blockchain technology ensures that there is no single point of failure in the network and data is replicated in all peers. The risks of attacks like ransomware is also minimized in the distributed system.

- Consensus verifications: The consensus mechanism in the blockchain based system ensures that the data stored in all blocks into the network is verified. The integrity of all the past data into the system is also ensured by the compulsive validation of each block into the ledger.

- Encryption: The permissioned blockchain system has multi layered encryption into the access rights and smart contracts of the system. Multiple encryption techniques is used at different levels into the system along with asymmetric cryptography based identities.

International Organization for Standardization (ISO) standards:

The International Organization for Standardization (ISO) is already drafting the standard for blockchain technology. The working committee is setting up the standard for Blockchain, Distributed Ledger Technology (DLT) and smart contract and is expected to be released in around 18 months.

The permissioned Blockchain based system will be interoperable for multiple cloud providers and blockchain platforms. The ISO/IEC 17788 standard provides the ability of two or more systems or applications to exchange information and use the information which is exchanged. The cloud interoperability is governed by the ISO/IEC 19941 standard. ISO/IEC 19941 provides the ability of one cloud service customer (CSC) to interact with the information with other cloud service providers (CSPs).

The sub standards under ISO/TC 307 standard for Blockchain and distributed ledger technologies which is under development is as follows:

- ISO/CD TR 3242 is ISO standard for Use cases related to Blockchain and DLT.
- ISO/DIS 22739 is developed for use of terminologies in Blockchain.
- ISO/CD TR 23244 focuses on the privacy and personally identifiable information and the considerations for its protection.
- ISO/CD TR 23245 is the standard for Blockchain based security risks and its threat and vulnerabilities.
- ISO/NP TR 23246 is based on the identity management based on Distributed ledger technology and Blockchain.
- ISO/WD TS 23258 is prepared for the taxonomy in DLT.
- ISO/AWI TS 23259 focuses on the legality of the smart contracts in the DLT based systems.
- ISO/CD TR 23576 is based on the security management of the digital asset into the Blockchain based network.
- ISO/NP TS 23635 standard is for the guidelines of governance in the DLT/ Blockchain based decentralized network.

National Institute of Standards and Technology (NIST)

The National Institute of Standards and Technology (NIST) had published a report (Report 8202) with the overview and components of Blockchain. The NIST framework which is voluntary for organizations to understand the cyber security risks for Critical Infrastructure Cybersecurity should be considered while designing permissioned blockchain based systems. Many companies in multiple domains considers the framework for designing critical IT systems.

The five goals of the framework are identified, protect, detect, respond and recover. The unique properties of permissioned blockchain based system is aligned with the properties such as access control, risk assessment, data security and response planning. Most of the fundamentals of the framework are inherent in the permissioned blockchain.

The hashing algorithm recommended by NIST for use of DSA and ESDCA in the internet x.509 certificates. The algorithms identifiers are SHA224, SHA256, SHA384, SHA512. The certificate authorities in the permissioned blockchain system should use these hashing algorithms on generating certificates. The Digital Signature Algorithm which is a federal standard for digital signature should be preferred. The Elliptic curve Digital signature algorithm (ECDSA) is used in most of the blockchain platforms. The bit size of public key believed to be needed for ECDSA is about twice the size of the security level in bits in DSA. For example at a security level of 80 bits (*meaning an attacker requires maximum of about 2^80 operations to find the private key*) the size of an ECDSA public key would be 160bits, whereas the size of DSA public key is 1024 bits. The signature size is however the same in both the cases.

The Software development lifecycle principles outlined in ISO/IEC 27034-1:2011 should be followed in the development. The SDLC and security-by-design principles in ISO/IEC 27034 incorporate security controls, referred to as "application security controls," into all aspects of the software and into all aspects of the design-to production phases.

Conclusion:

Many leading industries is exploring the use of Blockchain technology to enhance the cyber security of their applications. The standards which are mostly under development will certainly help in a common secure framework for all the implementations. The technology is also under continuous development and experimentations. There are many permissioned Blockchain based platforms which promises to solve the issue with the technological components within it.

References:

https://builtin.com/blockchain/blockchain-cybersecurity-uses

https://www.iso.org/committee/6266604/x/catalogue/p/0/u/1/w/0/d/0

https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf

https://www.microsoft.com/en-us/cybersecurity/content-hub/advancing-blockchain-cybersecurity

https://www.forbes.com/sites/andrewarnold/2019/01/30/4-promising-use-cases-of-blockchain-in-cybersecurity/

Vinod Kumar Mishra Vinod Kumar Mishra has above 3 years experience as a Freelancer Consultant in Blockchain and Cyber Security. He is presently working as Blockchain Consultant with Upgrad. His qualifications include B. Tech in Computer Science and Engineering (C.S.E) and Bachelor of Laws (L.L.B). He has completed multiple certifications in Blockchain including 'Introduction to Digital Currencies' from the University of Nicosia, 'Blockchain for Business' certified Professional from The Linux Foundation, 'IBM Blockchain Foundation Developer', Smart Contract and DAPPs from The University at Buffalo and The State University of New York. He has also completed multiple certifications in Cyber Security including Certified Ethical Hacker (CEH) from EC Council and Asian School of Cyber Laws.

vkumar201415@gmail.com
https://www.linkedin.com/in/vinodkumarmishra

Annexure I

Submission Date	Submission Id	Word Count	Character Count
12-Oct-2019	D64611217 (urkund)	2666	15818

Urkund Analysis Result

Analysed Document: 1.1 ERP-1 Blockchain for Cybersecurity - VK Mishra.docx (D61611217)
Submitted: 12/22/2019 2:09:00 PM
Submitted By: scholastic.seed@gmail.com
Significance: 4 %

Sources included in the report:

K391325_C008.pdf (D54316799)
https://www.microsoft.com/en-us/cybersecurity/content-hub/advancing-blockchain-cybersecurity
https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d41.pdf
https://builtin.com/blockchain/blockchain-cybersecurity-uses

Instances where selected sources appear: 5

Note: Cybernomics runs an Urkund plagiarism tool for the originality check of an article before publication. Urkund is developed by Prio Infocenter AB based in Stockholm, Sweden.

Reviewers Comment

Review 1:- This study presents an in-depth analysis of the market along with the current & future trends to elucidate imminent investment Pockets.

Review 2:- A blockchain's integrity depends on its network governance model and the methods it uses to validate transactions.

Review 3:- Blockchain technology may be able to help solve difficult general Cybersecurity problems that require reliable distributed data and records.

Editorial Excerpt

Initially at the time of submission, this paper had 4% of plagiarism which is accepted percentage for the publication. The finding related to this manuscript "**Blockchain for Cybersecurity - Standards & implications**" Blockchain is a powerful innovation that is poised to bring substantial positive change to the financial services industry as well as many other industries. Despite such promise, blockchain, like any emerging financial services technology, Blockchains also provide participants with enhanced transparency, making it much more difficult to corrupt blockchains through malware or manipulative actions. And blockchains may contain multiple layers of security – both at the network level and installed at the level of each individual participant. Hence the article is earmarked and finalized to be published under category of "**Experiential Research Papers (ERP)**".

Scholastic Seed Inc.
www.scholasticseed.in

Citation

Vinod Kumar Mishra
"Blockchain for Cybersecurity - Standards & Implications"
Volume-1, Issue-5, Oct 2019. (www.cybernomics.in)

Frequency: Monthly, Published: 2019
Conflict of Interest: Author of a Paper had no conflict neither financially nor academically.