ISSN: 2200-1872(Print), 2200-1883(Online)
Australian Journal of Wireless Technologies, Mobility and Security

Exploratory Analysis of Block Chain Security Vulnerabilities

Pavan Manjunath [1], Dr. Pritam Gajkumar Shah [2], Saurabh Mishra[3], Harish Sudarsanan[4]
[1]Ph.D. Scholar in Computer Science, Jain University, Bangalore
[2]Department of Computer Science, Jain University, Bangalore
[3]Dr.A.P.J.Abdul Kalam Technical University Uttar Pradesh, Lucknow
[4]Musaliar College of Engineering And Technology, Kerala

Abstract: Distributed ledger technology or block chain, is a progressing future domain, and accepting its constraint and boundaries will be serious to employing it into the Internet of Things or in any other technologies. Obviously, the security and trust and privacy issues will pitch in as well as other constrains. The Distributed ledger technology has drawn major attraction of the next-generation financial technology due to its security, and also it's extensively used in the design of smart cities and other areas of business or industry throughout the world. In this paper, we will first discuss on block chain domain and its process and then focuses on possibilities of block chain security analysis threat occurrence and in the area of public domain where it's attracting more and more hackers' threats. This paper provides helpful guidance and reference for future research works.

Keywords: Block Chain; Analytics for Smart Contracts; Cloud Technology; Security; Vulnerabilities

INTRODUCTION

The block chain has evolved one of the best domain in the cryptography in this era, but there are certain open issues in the form of security and other issues which need to be resolved first for block chain domain to go extremely outside the hype and influence their bursting potential [1]. First and foremost, we should understand the working of the block chain works, the block chain is a decentralized transaction, and it's developed first for cryptocurrency or virtual currency [2]. Block chain, can also be called as the circulated database which maintains millions of growing blocks which holds the transactions of the users. Each block contains the timestamp and link information which points out for the preceding block [3], and it's based on the hashing techniques, it's acting as stepping stone or base for the platforms for banking sectors, executing smart contracts and for the trading of the virtual currencies [4].

On the other side, Block chain will allow more responsive values, faster product development, customer friendly, and faster integration with the latest technology such as the IoT (internet of things), AI (artificial intelligence), Cloud technology [5].

Let us take the first example of block chain technology used in the cryptocurrency exchange, when one user sends a virtual currencies over the Block chain; they will be sending them in the form of a hashed version that is known as "Public Key". There is one more key which is hidden that is known as the "Private Key". This Private Key is used to originate the Public Key. The only user can know their own Private Key, but at any cost, the Private Key should not be shared in the public network, and if it's shared, then the cryptocurrencies will be stolen, once it's stolen it's very difficult to trace back [6].

The second example will explain a short description of how block chain is implemented in cloud technology. All users in distributed cloud storage are inter-connected over a two or more network [7]. The block chain domain allows secure, scalable, and easy access to the resources or services [8].

Currently, in the market, there are few companies such as MaidSafe, Filecoin, Storj and Siacoin work on decentralized cloud platforms [9].

The final example will explain an over view of block chains for the Internet of Things, it simplifies the sharing of services and resources [10], by utilizing the block chain domain in IoT (Internet of Things) solutions can assist trust less messaging between IoT (Internet of Things) devices in an IoT (Internet of Things) network. The block chain will treat message conversations between smart devices similar to the concepts used in financial transactions in a cryptocurrency network. The other advantage of block chain is the capacity to keep up a duly decentralized, securely trusted ledger of all transactions occurring in a network [11].

However, there is a challenge in the block chain in the form security point of view it's been noticed that current block chain has a possibility of a 51% attack.

DIFFERENT TYPES OF BLOCKCHAIN

Block chain domain can be evenly divided into three different Types, each one is explained below.

Public block chain: It's completely decentralized, and everyone can read, send transactions to and share in "agreement process" and as its public the number of users will be millions [12].

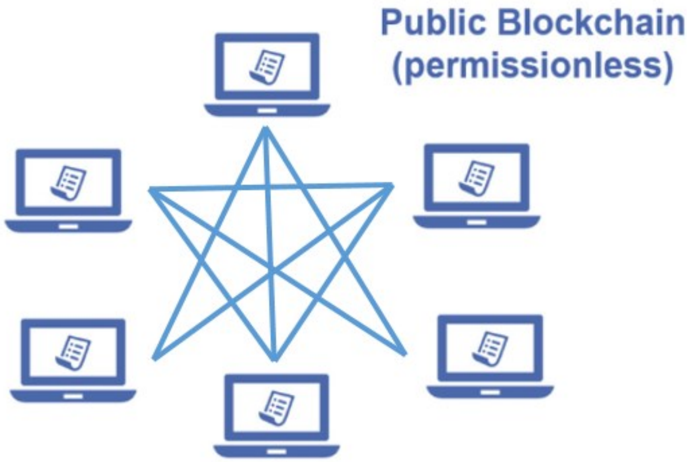


Figure 1: Public Block chain Domain.

Private block chain: The access is for members only, who can be the co-founder, and the number of users can be few thousands [13]. The participants are trusted and known, for example, sub-entities companies or business partners [14].

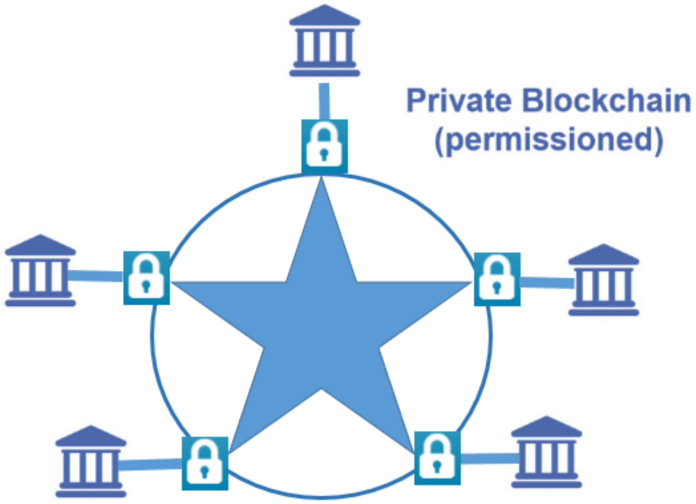


Figure 2: Private Block chain Domain.

Consortium Block chain or Federated Block chains: As the name is Cleary indicated that is controlled by a group or consortium of members [15]. It provides faster or higher scalability and provides transaction privacy, for example, there are a group of 30 financial institutions, each group of which operates a node and of which 20 must sign every block for the block to be authorized [16], as it shows in figure 3 [17].

BLOCKCHAIN PLATFORMS

A couple of block chain platforms or distributed ledger systems are explained below.

[1] **BigChainDB:** It is decentralization and immutability and its hashed-together chain of blocks, it supports public and private network, and it's an open source database system [18].

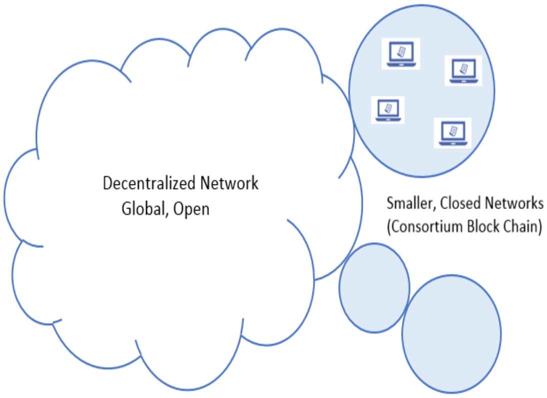


Figure 3: Consortium Block chain Domain.

[2] **Chain Core:** It's an open source and runs on the Chain protocol the process of the network is administered by the set of group. It supports smart contracts, and transaction privacy [18].

[3] **Corda:** It's an open source, and pluggable consensus, it allows other external databases to be connected and also allows bulk imports [18, 19].

[4] **Credits:** It's not a public block chain, and it's a framework for building DLT (Distributed Ledger Technology) based application [18, 20].

[5] **Domus Tower Block chain:** The Domus Tower Block chain prove that block chain is proficient in recording at a high rate of transactions in a scalable fashion. Data storage is bounded in a MerkleDAG (Merkle directional acyclic graph), and nodes on this graph are termed as "blocks" [21]

[6] **Ethereum:** Is a decentralized application, very useful for decentralized applications and speedy development time [22], it allows anyone to write a smart contract. And it creates a tradeable digital token that can be used as currency [23].

[7] **HydraChain:** It is an extension of Ethereum, and it is used for creating Permissioned Distributed Ledgers for Private and group chains and its open source [24].

[8] **Hyperledger Fabric:** It consists of one or more networks, each of them managing different Transactions, Assets, and Agreements between the different set of member nodes and it is a distributed ledger solution, it's based on modular architecture providing flexibility and scalability. It is considered to support pluggable implementations of different components [25].

[9] **Multichain:** It's multi-asset financial transactions based on bitcoin's block chain, and open-source block chain platform [26].

[10] **Openchain:** It's based on the Smart contract modules, and open source distributed ledger system for delivering and handling digital assets. The Tokens on Openchain can be attached to Bitcoin, making it a sidechain [27].

[11] **Stellar:** Stellar is a platform that connects payments systems, banks, users and Integrate to move money faster, constantly, and at no price [28].

[12] **xQuorum:** It used the smart contract platform based on Ethereum and open source distributed ledger. The privatize transaction blocks and confine their transfer without breaking the block chain and, it will allow your data is only routed to its intended receiver and no other receiver [29].

BLOCK CHAIN VULNERABILITIES

The most of the financial institute's and other institutes and government institutes throughout the world started using the distributed ledger technology (DSLT), but the security must be treated at the heights priority, and there are certain block chain security and vulnerabilities which needs to be addressed as sooner rather than the later point of time. Few security issues are mentioned in the below points [30].

[1] **Lack of Standards and Regulation:** The decentralized block chain has not a central expert, or any central organization can make a decision [31].

[2] **Criminal Risks:** It is due to the peer-to-peer environment, the cryptocurrencies are the most favored choice of criminals and target the business financial transaction. For example, in the defunct Silk Route web the drugs and other criminal activities were are executed using Bitcoins [32].

[3] **Mining malware and Endpoint:** The Hoaxers have also been recognized to take over unsuspicious endpoint computer systems and use them to mine or create new crypto currency [33].

[4] **Mobile wallet Theft:** The mobile wallet apps get easily infected if there is no proper security is provided, in the recent months, hoaxers have written particular phishing traps to enter into mobile wallet [33].

ANALYSIS OF BLOCK CHAIN SMART-CONTRACTS

First, we should understand the working process of SMART-CONTRACTS, it's also called as self-executing contracts or digital contracts. The self-executing contracts assistance the user to exchange anything of value in a clear way that does not depend on mediators. It is a very extraordinary tool which unlimited use case is possible.

The smart contract is the set of computer programing code that is saved and replicated on a network of computers systems that run and secure the block chain. Based on the details in the code, a smart contract is automatically performed when conditions are met between both, a code in a smart contract is basically an "if, then" condition statement, for Example: if conditions in the contract are encountered, then an event detailed in the contract is triggered [34].

The below-mentioned figure explains the smart contract for example for the automobile case car leasing business network,

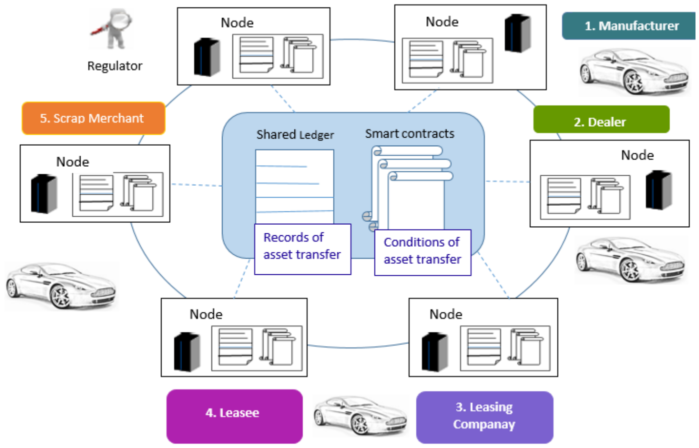


Figure 4: Car Leasing Business network with Smart Contracts.

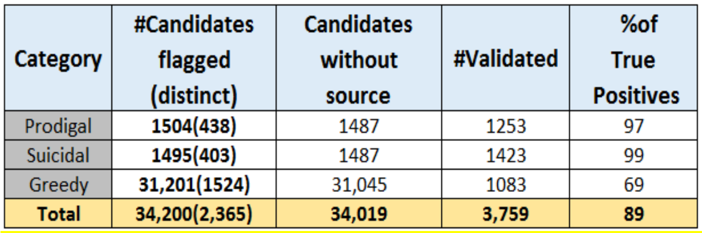
In the figure [35], the Smart contracts business requirements are encoded in the transaction database and executed with transaction [35], the contracts can be inserted with other data, such as bills statements, make the block chain technology ideally suited across a different area of the automotive environment [36].

The analysis of 2 million contracts deployed and live on the mainnet, and the question arises how many of these can be "hacked". As per the research group from the National University of Singapore, University College London and Yale under the guidance of Prateek Saxena, Aquinas Hobor and Ilya

Sergey attempted to find smart contract vulnerabilities at scale and this group developed the tool named MAIAN which used to discover and confirm vulnerabilities in a smart contract in a matter of under 10 seconds [37].

The analytics is done based on three types of vulnerabilities that the MAIAN tool was trying to find out, first is Greedy in this the contract should have been locked in a way that no user can take away funds from the contract, second is Suicidal, It was possible to execute the SUICIDE operation such that no more communication with the contract was possible and third analysis was based on Prodigal, contracts that would give away Ether to any random address and the MAIAN tool truly found the Parity exploit as shown in Figure 5 [37].

The result finding using MAIAN tool analysis of nearly 1 million contracts produced the following results:



Category	#Candidates flagged (distinct)	Candidates without source	#Validated	%of True Positives
Prodigal	**1504(438)**	1487	1253	97
Suicidal	**1495(403)**	1487	1423	99
Greedy	**31,201(1524)**	31,045	1083	69
Total	**34,200(2,365)**	**34,019**	**3,759**	**89**

Figure 5: Final results using depth of 3 invocations and at block 4,499,451 [37].

CONCLUSION

There is no uncertainty that block chain is a burning issue in recent centuries, there are some issues from security and vulnerabilities which needs to be addressed and also attracting more and more organizations are interested in implement it and to take befits to the fullest and other interesting part is that recent analysis concludes that it’s been found that current block chain has a possibility of a 51% attack, but as block chain domain is growing day by day and most of the security issues will be resolved as year progress.

REFERENCES

[1] H.Halpin and M. Piekarska,"Introduction to Security and Privacy on the Blockchain," 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Paris, 2017, pp. 1-3.doi 10.1109/EuroSPW.2017.434

[2] PLoS One. 2016; 11(10): e0163477. Published online 2016 Oct 3.doi:10.1371/journal.pone.0163477. [Online].Available:https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5047482/

[3] S. Singh and N. Singh, "Blockchain: Future of financial and cyber security," 2016 2nd International Conference on Contemporary Computing and Informatics (IC3I), Noida, 2016, pp. 463-467.doi: 10.1109/IC3I.2016.7918009

[4] M. D. Pierro, "What Is the Blockchain?," in Computing in Science & Engineering, vol. 19, no. 5, pp. 92-95, 2017. doi: 10.1109/MCSE.2017.3421554

[5] DDT. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels and B. Amaba, "Blockchain technology innovations," 2017 IEEE Technology & Engineering Management Conference (TEMSCON), Santa Clara, CA, 2017, pp. 137-141.

[6] WeTrustLeonDFollow, Product Marketing @ WeTrust, Jan 29, 2017· [Online].Available:https://blog.wetrust.io/why-do-i-need-a-public-and-private-key-on-the-blockchain-c2ea74a69e76

[7] Allonin, Friday 23, June 2017 Naveen Joshi, [Online].Available:https://www.allerin.com/blog/distributed-cloud-storage-with-blockchain-technology

[8] IntroducingiEx.ec:Blockchain-based Distributed Cloud Computing,Gilles FedakFollow, Aug 26, 2016. [Online].Available:https://medium.com/iex-ec/introducing-iex-ec-blockchain-based-cloud-computing-47dab8122b74

[9] Blockchain technology for cloud storage: This looks like the future,Angela Karl, February 8, 2018. [Online].Available:http://techgenix.com/blockchain-technology-for-cloud-storage/

[10] KONSTANTINOS CHRISTIDIS, (Graduate Student Member, IEEE), AND MICHAEL DEVETSIKIOTIS, (Fellow, IEEE), Received April 23, 2016, accepted May 8, 2016, date of publication May 10, 2016, date of current version June 3, 2016.

[11] IoT and Blockchain Convergence: Benefits and Challenges, Ahmed Banafa, January 10, 2017. [Online].Available:https://iot.ieee.org/newsletter/january-2017/iot-and-blockchain-convergence-benefits-and-challenges.html

[12] State of Bitcoin and Blockchain Q3 2015, Published on Oct 14, 2015, Slide 68, [Online].Available:https://www.slideshare.net/CoinDesk/v3-state-of-bitcoin-and-blockchain-q3-2015

[13] Financial William MougayarFollow,Author, The Business Blockchain (Wiley, 2016) Investor Analyst Speaker Startup Managemen 3x entrepreneur HP,Cognizant. Blockchain theorist & strategist. Nov 7, 2016. [Online].Available:https://medium.com/@wmougayar/understanding-semi-private-blockchain-applications-6bbe91fc3596

[14] Introduction to bitcoin & blockchain for financial services, Diana Biggs, Digital Innovation in Financial Services, Published on Nov 9,2015, Slide 27, [Online].Available:https://www.slideshare.net/DianaBiggs/introduction-to-bitcoin-blockchain-for-financial-services

[15] Do you know there are different types of Blockchain, geek4geek42, in blockchain, [Online].Available:https://steemkr.com/blockchain/@geek4geek/do-you-know-there-are-different-types-of-blockchain

[16] BlockchainHub, Blockchains & Distributed Ledger Technologies, [Online].Available:https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/

[17] Trust Machine: Global & Federated Blockchains, Muneeb Ali,Co-founder Blockstack, bringing decentralized computing to the masses, Princeton PhD.Nov 2, 2015 [Online].Available:https://medium.com/@muneeb/trust-machine-global-and-federated-8b9dc6dab7ec

[18] 17 blockchain platforms a brief introduction, Rohas NagpalFollow,Apr 12, 2017. [Online].Available:https://medium.com/blockchain-blog/17-blockchain-platforms-a-brief-introduction-e07273185a0b

[19] Corda, Blockchain for business,

[Online].Available: https://www.corda.net/

[20] Docs, FAQ, Is Credits a distributed ledger or blockchain? [Online].Available:https://credits.readthedocs.io/en/latest/faq.html#is-credits-a-distributed-ledger-or-blockchain

[21] Domus Tower Blockchain (DRAFT),March 28,2016,Rhett Creighton1, Domus Tower Inc. San Francisco CA, USA,Patent Pending,everett@domustower.com, [Online].Available:http://domustower.com/domus-tower-blockchain-latest.pdf

[22] Ethereum, Blockchain APP, [Online].Available: https://ethereum.org/

[23] A Next-Generation Smart Contract and Decentralized Application Platform,White Paper,James Ray,130 revisions, [Online].Available:https://github.com/ethereum/wiki/wiki/White-Paper

[24] HydraChain/hydrachain, [Online].Available:https://github.com/HydraChain/hydrachain

[25] Hyperledger/fabric, [Online].Available:https://github.com/hyperledger/fabric

[26] MultiChain Private Blockchain—White Paper,Dr Gideon Greenspan, Founder and CEO, Coin Sciences Ltd, [Online].Available:[Online].Available:https://www.multichain.com/download/MultiChain-White-Paper.pdf

[27] MultiChain Private Blockchain — White Paper, Dr Gideon Greenspan, Founder and CEO, Coin Sciences Ltd, [Online].Available: https://www.openchain.org/

[28] Stellar | Move Money Across Borders Quickly, Reliably,And For Fractions of a Penny, [Online].Available: https://www.stellar.org/

[29] J.P.Morgan,Solutions,Quorum, [Online].Available:https://www.jpmorgan.com/country/US/EN/Quorum

[30] Ignite Outsourcing,Publications,5 Blockchain Security Risks and How to ReduceThem, [Online].Available:https://igniteoutsourcing.com/publications/blockchain-security-vulnerabilities-risks/

[31] Fundamental challenges with public blockchains, Preethi KasireddyFollow, Blockchain Engineer,11 Dec 2017, [Online].Available:https://medium.com/@preethikasireddy/fundamental-challenges-with-public-blockchains-253c800e9428

[32] Blockchain—Benefits & Risks,Shawn PangFollow,Oct 29 2017, [Online].Available:https://medium.com/@pangshawn/blockchain-benefits-risks-bbd9f17aed6f

[33] Blockchain Exploits and Mining Attacks on the Rise as Cryptocurrency Prices Skyrocket,January 8, 2018|By David Strom, [Online].Available:https://securityintelligence.com/blockchain-exploits-and-mining-attacks-on-the-rise-as-cryptocurrency-prices-skyrocket/

[34] Crypto for Beginners 5-Smart Contracts, [Online].Available: https://pirl.io/blog/crypto-beginners-5-smart-contracts/

[35] A Distributed Business Network: The Difference with Blockchain, [Online].Available: https://www.altoros.com/blog/the-difference-with-blockchain/

[36] Ignite Outsourcing,Publications,10 Applications for Blockchain in Connected Car Automotive, Lyudmyla Novosilska by Lyudmyla Novosilska, [Online].Available:https://igniteoutsourcing.com/publications/blockchain-automotive-industry/

[37] Jeffrey TongFollow,Mar 3, Finding Smart Contracts Vulnerabilities at Scale, [Online].Available:https://medium.com/@trigun0x2/finding-smart-contracts-vulnerabilities-at-scale-72196d16afbc