RESEARCH REVIEW JOURNALS
Volume-03
Issue-10
October-2018

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com [UGC Listed Journal]

Security Aspect in the Blockchain

[1]Saurabh Jain; [2]Dr Debasis Patnaik; [3]Dr. R.Gopal & [4]Dr.Vani Kamath

[1]Senior Manager, Cognizant, Mumbai (India)
[2]Head of the Department of Economics, BITS-Pilani, K. K. Birla Goa Campus, Goa (India)
[3]Director, D.Y.Patil Deemed to be University School of Management, Sector 4, CBD Belapur, Navi Mumbai (India)
[4]Dean, D.Y.Patil Deemed to be University School of Management, Sector 4, CBD Belapur, Navi Mumbai (India)

ARTICLE DETAILS

Article History
Published Online: 10 October 2018

Keywords
Blockchain, Technology, Ethereum

ABSTRACT

Blockchain is proven technology for providing immutability for the information which is locked in the blocks. But on last few years, we saw that attackers are highly incentivized to export the bugs, risk factors in the existing block chain

The objective of this paper is understand the risk associate with the conventional centralized technology & try understand how the labeled technology like block chain help us in order to mitigate the risk . But same time it is important estimate and appreciate the respective risk associated with the same in terms of operational challenges, vulnerabilities& prospective attacks etc as Blockchain is in early stage of its adoption & with introduction of decentralized platform for development like 'Ethereum' which is nothing but smart math& software codes . Hence, they eventually carry the respective risks associated with software life cycle.

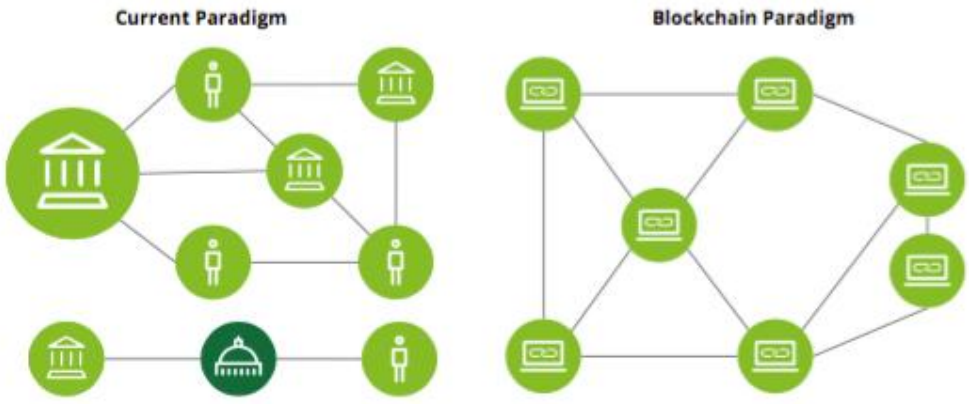
1. Introduction

Block chain technology started with famous use case as BITCoin , which is based on the paper presented by the paper presented by [6], S. Haber, W.S. Stornetta et al called 'How to time-stamp a digital document'. Because of massive popularity of BIT Coins in the recent period of time, people start thinking BITcoin as synonym of Block chain technology which mainly focus on the finance .

But this technology is far ahead, which basically create the trust between the untrusted. It has capabilities to work outside the traditional accounting systems, frameworks & to fulfil its potential in the game of emerging technologies, blockchain technology require further maturity and hardening. we try to understand some important aspect of this technology in terms of computing models like centralized and decentralized approach in current landscape , types of blockchain followed by the threats and limitations associate with this technology.

BIT Coin were introduced in 2008 , as first decentralized crypto current which is basically first use of DST technology . But it was available in the form of a software program which can be downloaded by user to be part of network and "**Inside this program** "details of all transactions are get stored , point here is everything is happening inside the program we can't have that luxury to take out the code outside & use for other application until 2015 when the next version of cryptocurrency got introduced , which is called 'Ether' & it got developed on the world first decentralized platform which is called as 'Ethereum'.

2. Centralized Vs Decentralized ledger technology



Distributed Ledger Technologies (DLT) have received growing attention in recent years as an innovative method of storing and updating data within and between organizations.

In the current paradigm which is also called as centralized coordination system, where every node is connected with the central node of the system , the basic problem with this scenario is if central node get down then entire network get down .

While Traditional infrastructure focuses on confidentiality and integrity, control of all the systems including databases,

network ,security is managed centrally. The key components of these centralized systems are Authentication and authorization but as we know great power comes with great responsibility hence these centralized system constantly gives out the litmus test to prove their worthy against data leaks , hacks , SQL injection , DOS attacks etc. can be possible and happened on regular interval of time .

Blockchain is designed to provide integrity and availability, to get the dose of decentralized business models and business process can be a bit challenging . Because in the reseat past world saw millions of dollars get grounded due to misunderstanding, smart contract errors or by **security mistakes.** In short the game of trust the non trusted is not so easy , till time technology is get evolved fully to accept the incremental growth of operational risks over the upcoming years .

3. Conceptualizing Crypto Hashing in the Block Chain

Now the fundamental question arises from where we get the essence of security in case of decentralized, who we can protect our network from the cyber-attacks . The answer of this question lies in the fundamental principles of block chain

1. Cryptographically deigned hash functions (SHA256)
2. Consensus Protocol where Each node caries the same copy of ledger & periodically communicates with each other to correct themselves on the principal of **51% or not.** Because of this property, attack on block chain becomes practically impossible but still there are some ways ,which we can see in the below mentioned topics .

The core hash function behind the solid immutable blockchain technology is SHA256.

The fundamental properties of the hash function which make it unique is

- It is only one way function, which means that that hash can calculated but be reengineered from the respective text .
- Minute changes will completely change the entire hash code

Example al[1] shows small change in the text leads to complete change of hash function in blockchain

hello world! —
> ed42329d864d140ed766bb5c6d4db5a3cc2c40d4e447c75daf224c801d832fc6

Hello World —
>699733a22af63e4ae4bd674d8d615f254aa1d1818b6db494c7d41bbf6816ecd1

hello world —
> c169407155f99dbe433361cc48e4e1bd29ea42da934d520bb07cd2c2b5fe9972

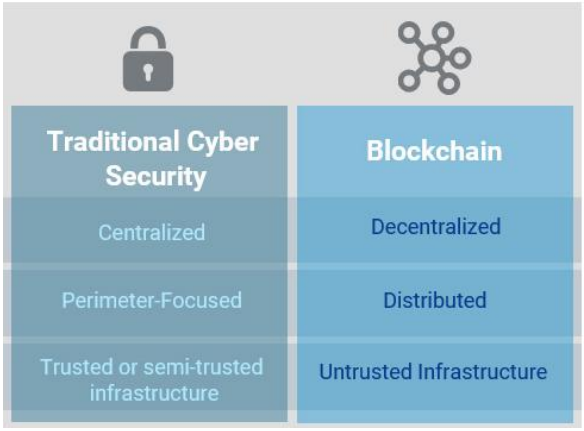
4. Traditional Vs Blockchain

With increasing awareness about the DLT / blockchain technology & availability of respective literature, peoples started evaluating the opportunities and challenges in the existing paradigm vs futuristic blockchain landscape . we also try to compare certain features of existing world with reference to blockchain technology but same time we would like to highlight that this technology is in its initial phase many question still requires satisfactory answers before the enterprise implementation .

As per [15] et al , Salil Gunashekar& RAND corporation , many factors are still answered before mass acceptance of this technology

1. Uncertainty around regulation
2. Multiple non-interoperable implementations and resulting fragmentation
3. Lack of clarity on the terminology and perceived immaturity of the technology
4. Insufficient evidence on business gains and wider economic impact
5. Perceived risks in early adoption and likely disruption to existing industry practices

By taking such inputs we try to compare the existing base with the DLT case .



In the traditional security system, we generally put the trusted data behind the trusted data & systems owned by the company , enterprise or any firm. Anybody inside the perimeter can access the resources. Here authorization and authentication plays a vital role in the traditional enterprise landscape .

Whereas Blockchain But in case of block chain the things are completely different as the concept of blockchain start with ‘Decentralization’ & everything present on the peer-to-peer network. We cannot define a standard perimeter in case of block chain special the same is public in nature .

Another issue with conventional security aspects is they really on in-house or third part solution to safeguard their respective perimeters .Since these codes are coming from multiple parties hence we don’t have any choice but we have to show faith and trust on them

But this is not the condition with the blockchain , as blockchain solutions are written in the smart contracts which calls codes from other smart contacts which may comes from variety of different authors & developers which means that we have to spend lot of time and energy in order to establish the authenticity of respective codes .In other words we have to ensure that we are not inheriting the security vulnerabilities from other smart contracts which are written by unknown , untrusted parties .

Conventional cybersecurity or conventional line of business with centralized approach, systems are running on the secured and trusted hardware , while in case of blockchain all the codes get run on untrusted hardware , untrusted resources which are owned by anyone ,anywhere in the world . **Hence we have to ensure that all the security measures in the blockchain will come from protocol and code layer itself.**

In the conventional system large chunk of data , databases is centralized in nature & security of these elements generally depends on the central systems . .

In case of blockchain , due to presence of multiple nodes

In [4], Shin et al , describe a theoretical concept where forgery of blocks could be possible with **common prefix property and common quality property** . By using these properties, we can estimate the probability which the adversary succeeds to manipulate the blockchain , this can be done at protocol layer This is the requirement only for protocol specification of the backbone protocol. From the system and application viewpoints, we should care about more aspects of security. Even on the protocol security, there are many assumptions in achieving its security goals.

In [5] , LI Yue et al , describe that forged blockchain initiated by introducing a bad node in the blockchain to overcome with rules of consensus protocols or the success probability is define by a mathematical equation

$$P_Z = 1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} * \left(1 - \left(\frac{q}{p}\right)^{z-k}\right), \quad \lambda = Z\frac{q}{p}$$

By calculating the value of Pz , we can understand that with incremental nature of blockchain means adding more and more nodes in blockchain make it immutable as their is need of very large computing power to crack this setup .

Since blockchain is massive decentralized distributed system & we don't have any direct control on the systems so this pillars would be keep in mind before implementing the block chain solutions .

5. Risk factors associate with BlockChain technology

Scalability: Bitcoin block chain will take around 10 mins to clear the transactions ,it's very long time to conform the transactions for the system which is doing max time micro payments from machine to machines transfer where our expectations is like millions and millions of transactions per sec

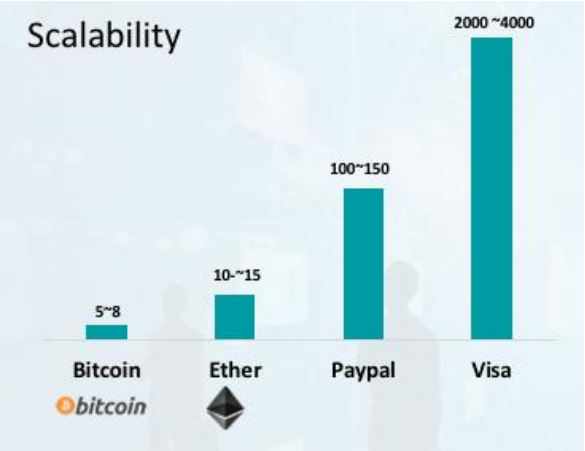
Just to give understanding about the issue, Visa will perform around 2000 transactions / second while Bitcoin all only do 5-6 transactions per second

In [2] , Federico et al , suggest that to increase the block size, which increases the maximum amount of transactions that fit into a block to create off chain *channels* through which users can bypass the network transaction rate cap; to create nested blockchain structures in the form of sidechains (e.g. Plasma) or to split the network in partitions (i.e. shading).

Opposed to blockchain technology where dedicated validators must exist in order to generate and order blocks, a user in Nano must sort his/her own transactions. This approach vastly differs from the way transactions are executed on blockchain systems: transaction ordering is done asynchronously by the account owner being in charge of the ordering. The consequence is that there is no inherent cap in the transaction throughput in the protocol itself. However, peak throughput on a test reached on the main network was 306 Transactions Per Second (TPS) with an average of 105.75 TPS [7]. The limit is currently determined by the quality of consumer grade hardware and network conditions

Suggestions for the same are also present like Segway, Lightning Networks. which is based on the principal, that don't take all the transaction into the blockchain but only start and end. rest intermediary transactions are sorted between the trusted groups

Block chain Bloat in which we can't save the data directly on the blocks, but we have the pointer which is living somewhere in the distributed hash tables in order to fasten the block processing.



6. Operational Issues with Block Chain Technology

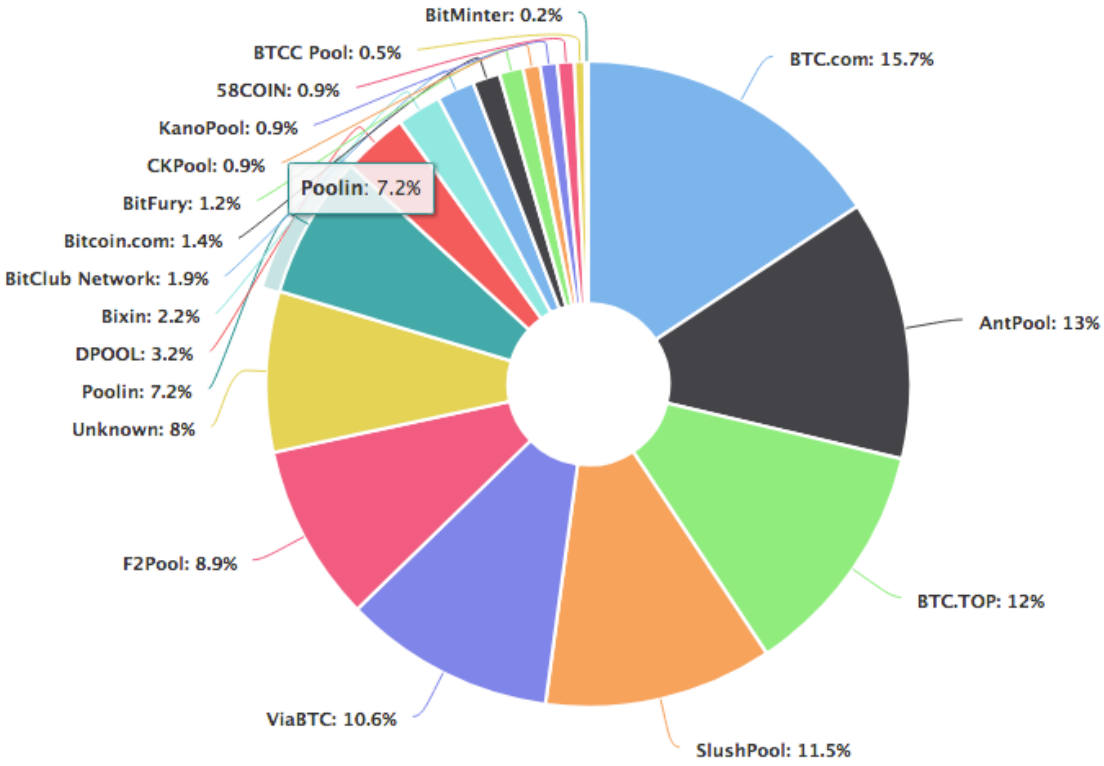
Fees : Fees for the Bit coin transactions is count 0.001 BTC which approx. to 1 dollar while fees charged by Visa is around 2% of the total transaction value now think about the micro payments in the Bot Coin network,anything below 1 dollar become obsolete as the fees of traction is more than the transaction itself.

Lot of Computing Power is require in maintaining the Block chain Network: Major cryptocurrencies are based on the Proof -of-Work protocol. Which basically tris to solve one mathematical problem using random numbers. This requires lot of unconditional power supply which is around 61.4 TWh as calculated by forbes et al [16]. It means that 60% is the mining cost which makes entire process as 'Non Profitable' as we gradually require high computing power to compete within the group .

Centralization of decentralized Cryptocurrency: China is mining 71 % of total cryptocurrency,there are large centralized mining pools in the chin for doing it .**BTC.com, BTC TOP** and **Antpool** is mining 40% of total cryptocurrency, both these pools are controlled by **'Bitmain'** which is largest manufacturer of 'application-specific- circuits' (ASIC) miner. At this level ,Bitmain is dangerously close to reach 51% of Bitcoin hash rate. By attaching these few mining power hubs , one could get easily control on the entire network o blockchain.

This can't be top as due to 'Longest Chain Rule 'more & more blocks are created by this consortium further increase their respective mining power . Which may increase the chances of 51% attack.

In [3] etal , graph shows the mining distribution among the top mining players .Most of them are based out of china again make them centralized in nature.



Associated Risk Factors

Vendor Ecosystem: Is not fully evolved in the market . Development is happening at consortium level, start-ups, university research etc but nobody is completely established in the present landscape.

Disintermediation : Implementation and adaptation of emerging technology is always fascinating but just by grasping few articles and blogs we can't take these flying arrows.

With adoption of total decentralized approach over disinter raise serious threats

Decentralization and distributed network for financial or banking system is always matter of concern , specially interns of securing & protecting 'Golden records' , databases , reconciliations etc

Lack of ledger Interoperability:
Poor Customer Experience:
Wallet and key management:
Poor development experience
Skill scaricato &Cost

7. Security Threats in Blockchain Ecosystem

Creative ways of cheating blockchain

Blockchain works on the concept sharing data between two or more people untrusted people using sophisticated math (Hashing) and some innovative piece of software codes (called hyper ledger)& of course a decentralized peer to peer network .

But fancy maths and tools got filed out when it comes in the contact with humans who are skilled cheaters & famous for making the things messy.

This rule also applies to the so called famous immutable ledger technology called 'Block Chain' which is marketed for the most prominent feature called 'Security'

The basic pillars of this security in the block chain, which make it "Tamper Proof ' are mentioned below

- Hash Cryptography
- Consensus Protocol

Because of that even a small change (even a single , in paragraph) completely changes the entire hash function . But unfortunately these finger prints or hash functions which are irreversible in nature , can also be cracked , this is what claimed by the Connell University's researchers **EminGünSirer of Bloxroute Labs .**As per him a "selfish miner" can gain unfair advantage by fooling other nodes into wasting time on already solved crypto puzzles .

'Eclipse Attack'can be also possible in the existing scenario which basically uses the property of blockchain having constant communication with other nodes .

This generally happens as nodes in the block chain because of consensus protocol communicate with each other in order to compare their respective data and rollback in case of any difference . Data is synchronise based on the fact that what is majority is saying (51% & more nodesstatus) .

But now considera scenario , where an attacker manages a control of single node in the block chain fool other nodes in the network with wrong information so that rest of the network can absorb the wrong info & update themselves because of consensus protocol **(What 51% will say , rest all will do)**

More vulnerability zone exist where the amalgamation of block chain happen with real world , in colloquial language we called it the edge line between the **'Software application and Third party application integration point of contact '.**

Complexity of the hash function is always counted by the no of zero's in the hash function . These has values are generated by the Nonce values which except some random value in order to create blocks . An attack on the random number generator is something that can be brushed under the carpet. Random numbers with insufficient entropy can spell trouble to the entire system due to weak entropy

Some people also claimed that from DOS attack ,even Block chain can not be immune for the same .But I am little sceptical about it as by DOS attack we can shut down the system but hacking of the system is not possible as per my understanding but we never know , world is creative in nature .

Smart Contracts Vulnerabilities :

This term was first coined by the computer scientist '**Nick Szabo**' , in the year 1996 . As per him these contracts can be realised by using the public ledgers. In blockchain technology the realisation of smart contracts happened through decentralised arrangement done between the two or more parties without any intermediary &

Smart Contracts are set of code which are in the executable format (Codes) which is hosted on the blockchain . The most important property about them is , you can't change or updated hem once they get deployed in the system.

Smart contract or rather we can call it smart codes which basically executes or triggered when they meet the respective criteria or benchmark like neural networks which when the specific conditions meet up .

We can understand with the example of home loan , where payment has been disbursed by the bank at every stage of construction , this can easily get bundled in the smart contracts .

But vulnerabilities in these smart contracts will process serious security threats .[8] BY 2017 cryptocurrency market reached to 600 billion plus , managing such a fast wealth with insecure &vulnerable platform results serious losses in past convert the entire blockchain landscape into disneyland for the hackers .

[10] The infamous DAO contract bug [10] led to $60 million US loss. The Parity wallet has suffered from two vulnerabilities [11][12]. The first one has resulted in the loss of $60 million, and the second one has frozen more than $150 million in terms of Ether and several more recent ones have had impact of a similar scale.

With these kind of security issues, Ethereum platform caused huge financial loss in recent time hence there is serious need to study these vulnerabilities which are associated with the smart contracts.

In [13] [14], Prateeket al classified such vulnerabilities into 3 border category like

Vulnerability 1 :prodigalContracts

One which occurred due to glitch in the process flow like contracts often return funds to the owner (when under the attack) , to addresses that have sent Ether to it in past (e.g., in lotteries), or to addresses that exhibit a specific solution (e.g., in bounties). How- ever, when a contract gives away Ether to an arbitrary address— which is not an owner, has never deposited

Vulnerability 2 :SuicidalContracts

This contract is used in the emergency situations when the owner wants to switch off the show because of some hacking, malfunctioning or attack etc . Here the most vulnerable part is, it can execute by any arbitrary account user & execute the suicidal codes which kills the entire blockchain just by invoking couple of functions .

Vulnerability 3 : Greedy Contracts

Here contracts that remain alive and lock Ether indefinitely, allowing it be released under no conditions, as greedy. The wallet contracts could no longer access the library, thus became greedy. This vulnerability resulted in locking of $200M US worth of Ether indefinitely!

Vulnerability 4: **Call to the Unknown**

The Call to the Unknown vulnerability arises from the fallback function in Solidity that may cause harm under certain conditions. The most well known case of a Call to the Unknown vulnerability was when an attacker stole $60M

Vulnerability 6: **Reentrancy Bugs**

The reentrancy vulnerability is consists of the function which allowing an attacker to retransfer money in his account . This loop will continue till time contract is out of the gas .

Vulnerability 7: **Exception Disorder**

Exception Disorder is a vulnerability arising in Solidity based smart contracts under several conditions:

1. When there is a shortage of gas
2. When encountering a call stack limit
3. During the execution of a throw command

Vulnerability 8:Gasless Send

The cause of gasless send vulnerability is the out-of-gas exception. This exception happened at the time of transferring fees via send function and because of system issue called as out-of -gas exception , system pretend that the fees is submitted in the respective account while in actual it is not happened .

To understand further , we take the example of famous game *King of the throne ,* as per the rule who so ever wants to become a king in the game will pay certain amount as fees & some part of this fees will goes to previous king as compensation for disenthronment . Now the owner will designed the smart contract in such a way that no fees will go to previous king but kept with the owner of the game .

Vulnerability 9:Timestamp tampering

For normal operations all the transactions and block creation in the blockchain having respective timestamp . But some malicious miners with mindset of executing fraud or some scam will temper the timestamps using smart contracts . The malicious miner generated a block for his transaction with the modified timestamp that delayed his transaction to be the final one and in this way he won the funds from the smart contract.

Vulnerability 10: Generating Randomness

Many smart contracts specially designed for online lottery , games etc. May have a primary function of generating the random numbers . For generating a random number , some transaction need to be get triggered in the blockchain. Some malicious miner can control this and generate the random number which matches with their numbers and use this technique for his own purposes.

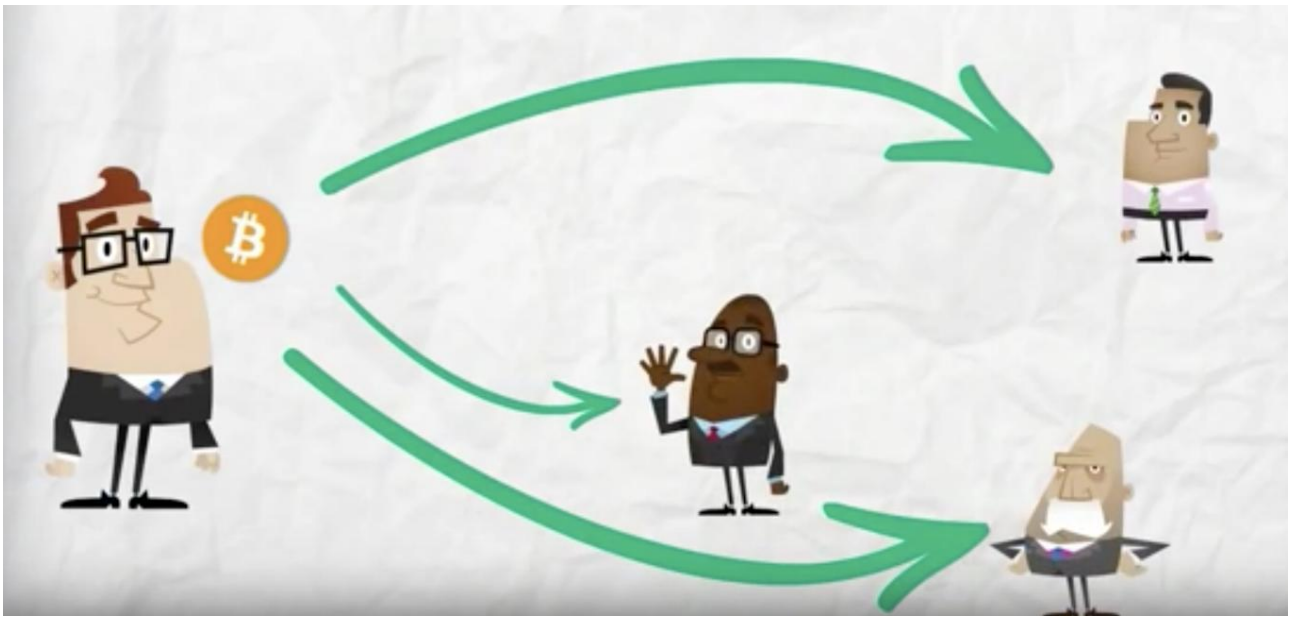
'Double Spending fraud

' **(**https://99bitcoins.com/double-spending/)
https://www.youtube.com/watch?v=UxyGt58EPa4

Crypto currency is nothing but just a file & it can we possible that we can duplicate the same and land up with the two transactions which means that single money paid to more then one party .

To be more precise , if let say I have one coin in the block chain which I transferred to Bob , then in actual this transaction first land-up into the 'Unconfirmed transactional pool ' & wait for conformation

Meanwhile, I can send the same coin to Alice & which again goes into the 'unconfirmed transaction pool ' .



Transaction A ——> Send to Bob ————> Waiting in transactional pool for conformation ——> post confirmation that will get add into the Block chain post validity check

Transaction B ——> Send to Alice ————> Waiting in transactional pool for conformation ——> post confirmation that will get add into the Block chain post validity check but in this case , it is Invalid so no entry to block chain

Now think about a situation where the validation process for both A&B happened simultaneously, in that case both the transactions show the money & leads to creation of two branches and race will get start in order to get the first conformation from the next block will get win .

But this anomaly will initial allows the merchant to provide the respective products, services against the Transaction B also .

Solution : It has been recommended to wait until 6 conformation post transaction to be tagged as 'Complete transaction' because they can reach the next block simultaneously for six times .

8. Quantum Attack

In [12] Serguei Popov , Russian mathematician et al, proposed that miners will randomly select 2^68 random unique Nonce combinations for creating a single block in blockchain . Just to understand the computing power of a Quantum computer and a classical computer , lets understand in this way if a if the classical computer lets say take some N iteration to solve the problem then quantum computer will just take Square-root of (N) to solve the same problem

9. Conclusion

Vulnerabilities in the smart card are very dangerous, Exploiting these vulnerabilities might be leads to few instances but may they have global consequences. For example famous DAO attack where people lost somewhere around 60 million USD.

It is recommended that we should pay attention for these vulnerabilities at the time of designing the smart contracts. We should always put **Maker-checker concept** & ensure that same should be get audited by the industry experts before they put into the block chain.

References

1. https://www.xorbin.com/tools/sha256-hash-calculator
2. Federico Matteo Benc˘ic´ and Ivana PodnarZ˘arko , Distributed Ledger Technology: Blockchain Compared to Directed Acyclic Graph , 2018
3. https://www.blockchain.com/pools
4. Shin'ichiro Matsuo "How formal analysis and verification add security to blockchain-based systems" , KeioUniversity
5. LI Yue, HUANG Junqin, QIN Shengzhi, WANG Ruijin , "Big Data Model of Security Sharing Based on Blockchain", 2017
6. S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In Journal of Cryptology, vol 3, no 2, pages 99-111, 1991.
7. YeLiu , W.K. Chan, Bo Jiang , "ContractFuzzer: Fuzzing Smart Contracts for Vulnerability Detection"
8. Cryptocurrency Market Capital. https://coinmarketcap.com. Last access, 2018.
9. A.Akentiev, "Parity multisiggithub." Available: https://github.com/paritytech/parity/issues/6995
10. Analysis of the DAO exploit. http://hackingdistributed.com/2016/06/18/analysis-of-the-dao-exploit/. Last access, 2018.
11. The Parity Wallet Hack Explained. https://blog.zeppelin.solutions/on-the-parity-wallet-multisig-hack-405a8c12e8f7. Last access, 2018
12. The Wallet Smart Contract Frozen by the Parity Bug. https://github.com/paritytech/parity/blob/4d08e7b0aec46443bf26547b17d10cb302672835/js/src/contracts/snippets/enhanced-wallet.sol. Last access, 2018.
13. Ivica Nikolic´, Aashish Kolluri, Ilya Sergey, Prateek Saxena, Aquinas Hobor "Finding The Greedy, Prodigal, and Suicidal Contracts at Scale"
14. https://blog.bankex.org/nine-pitfalls-of-ethereum-smart-contracts-to-be-avoided-f7464761211c
15. https://www.bsigroup.com/LocalFiles/zh-tw/InfoSec-newsletter/No201706/download/BSI_Blockchain_DLT_Web.pdf
16. https://www.forbes.com/sites/shermanlee/2018/04/19/bitcoins-energy-consumption-can-power-an-entire-country-but-eos-is-trying-to-fix-that/#5bdc1e7b1bc8

