Security in Blockchain Technology: A Survey

Gangu Vijay Kumar
Department of Computer Science and Engineering,
AITAM, Tekkali,
Andhra Pradesh 532201, India.

Marpu Sasikala
Department of Computer Science and Engineering,
AITAM, Tekkali,
Andhra Pradesh 532201, India.

G.V.S.S.Naveen Babu
Department of Computer Science and Engineering,
AITAM, Tekkali,
Andhra Pradesh 532201, India.

ABSTRACT

The blockchain technology can be considered as a innovative invention with this potential to bring the digital revolution to give the solutions in the sector of economy. The blockchain technology and the idea of blockchain durability are considered. The advantages of early evenness of the blockchain technology are disagreeing based on the literature and the analysis of the central blockchain immutability characteristic. By this, a plan is proposed aimed at understanding not only the depth but also the bounds of blockchain immutability. The resulting groundwork is suggested as a best practice standard for the employment of blockchain systems. Based on these efforts, the article supports initiatives to better exploit the blockchain technology's full potential by standardization.

Keywords: blockchain;privacy;bitcoin;digital ledger

INTRODUCTION

Blockchain technology [1-5], [7] is a current technolgy of secure computing without centralized authority in an open networked system. Blockchain is defined as a unique, decentralized distributed ledger that involves all transactions records related to participating members. Blockchain transactions are created and stored in sequential order, allowing digital currency to make the transaction to be secure. Blockchain is always maintains its transactions in a hierarichal chain of blocks,which helps it be act as a distributed datebase. Whenever a block chain is created and maintained using a peer to peer unduly network and secured through intelligent and putrefaction utilization of cryptography with crowd computing. All transactions on the blockchain must be approved because transactions are only valid

conclusions. Furthur, all transactions are detectable, making dishonest transactions impossible to neglect. When a user wants to make a transaction to another user with the help of blockchain, a new block is created to include the transaction. Each transaction is advertised across network nodes to correct it. If the new transaction is valid transaction, the new block is joined to the blockchain and distributed across network nodes [9] so that other nodes will update their blockchain. Certainly, the transaction is received by another user.

Blockchain Explained

The blockchain is the simple way of transforming information safely and it will not charge any transaction cost.Either of the party begins the process by creating a block for transaction and the block created is verified by lots of computers distributed over the net.And this verified block is attached to a chain and stored across the net.Its not just simply a distinct record but a record with unique history.As a record is added to the end of the chain ,disproving a single record would mean disproving the complete chain in many cases. That is pratically impossible. Bitcoin uses this model for monetary transactions,but it can be used in many other ways [2-6].

Blockchain is not only used for transcations and storing money, but it can take the place of all processes and business models that depend on by charging fee for transaction. For example, the gig economy hub Fivver charges 0.5 dollars on a 5 transaction between individuals buying and selling services. Whereas,by using Blockchain technology a transaction can be done freely. Many of the newly entrants are threatened by the blockchain technology,for example Uber and Airbnb. The one thing to be done is encode the transactional information for a car ride or an overnight stay, and again you have a perfectly safe way that disrupts the business model of the companies which have just begun to challenge the traditional economy. We are not just simlpy trimming out the fee-processing but also eliminating the need for the match-making platform [8].

As the blockchain transactions are free, one can charge small amounts, say 1/100 of a cent for a video view or article read. Is it necessary to pay the Economist or National Geographic an annual subscription fee if I can pay per article on Facebook or my favorite chat app? One can charge for anything in any amount without worrying about third parties cutting into your profits, as blockchain is free. Artists can gain profit by selling recorded music again by using blockchain by cutting music companies and distributors like Apple and Spotify. The music can be encoded in blockchain itself by making it a cloud archive for any purchased song as the charged amount is tiny.Streaming services maybe irrelevant as it goes further so Ebooks can be fitted with blockchain code.These books spread in an encoded form and profitmaking transaction would transfer money to the author and unlock the book instead of profiting the company such as Amazon and the credit cards companies that earn money through the sale [10].

These applications are clearer and the revolutionary changes are about to happen in the financial world. Blockchains will change the way stock exchanges work, loans are bundled, and insurances contracted and will eliminate practically all services offered by banks. Almost every financial institution will go bankrupt or be forced to change fundamentally, once the advantages of a safe ledger without transaction fees are widely understood and implemented. After all, the financial system is built on taking a small cut of your money for the privilege of facilitating a transaction. Bankers will become mere advisers, not gatekeepers of money. Stockbrokers will no longer be able to earn commissions and the buy/sell spread will disappear [11-13].

Properties of Blockchain technology

The three main properties of Blockchain Technology which have helped it gain widespread acclaim are as follows:

- Decentralization
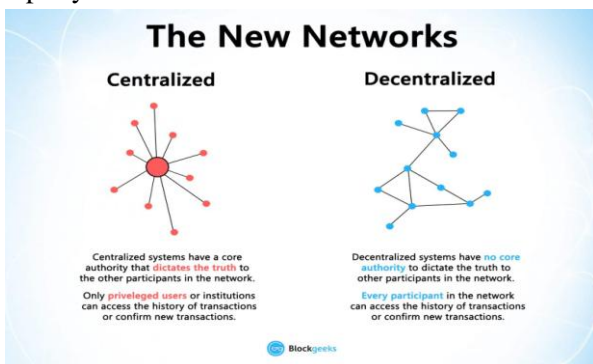- Transparency
- Immutability

Decentralization

Before the invention of Bitcoin and BitTorrent, we were more used to centralized services. The idea is very simple. You have a centralized entity that stored all the data and you'd have to interact solely with this entity to get whatever information you required. A good example of a centralized system is the banks. They store all your money, and all ongoing transactions and etc all are used to store in record format [14]. The traditional client-server model is a perfect example of this:
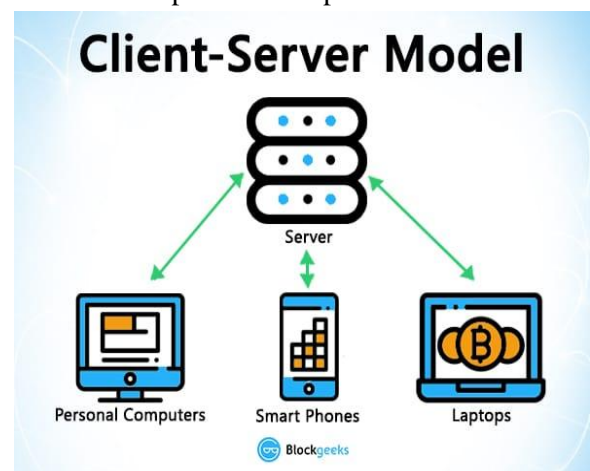
When you Google search for something, you send a query to the server who then gets back at you with the

relevant information. That is a simple client-server. Now, centralized systems have treated us well for many years, however, they have several vulnerabilities. Firstly, because they are centralized, all the data is stored at one point. This makes them easy target spots for potential hackers. If the centralized system were gone to a software upgrade, it would freeze the entire system. Worst case analysis, what if this entity gets corrupted and vicious? If that happens then all the data that is inside the blockchain will be compromise [15].

In a decentralized system, the information is stored in several entities. In fact, everyone in the network owns the information. In a decentralized network, if you wanted to interact with your friend then you can do so directly without need of a third party. That was the main theme behind Bitcoins. You are only responsible for charge of your money. You can send your money to anyone without any restrictions or also not need of any third party.

The New Networks

Transparency

Blockchain technology gives a high level of security by ensuring that transaction details are shared only amongst the participants involved in those transactions. With blockchain transactions there's no need for a third party but the level of privacy associated with blockchain payments has raised concerns among many in the finance community. However, in addition to the high

level of privacy built into blockchain technology, there is also a high level of transparency. Blockchain systems include a fully auditable and valid ledger of transactions. This ledger is indelible and unforgettable. Entries into the ledger can only be made if they are validated by the system. And in order to change it, every single other blockchain in the system would also need to be changed. For this reason it's impossible to delete a blockchain transaction in an attempt to hide it and fraudulent transactions cannot be added.

This transparency cancels the need for balance and checks. With blockchain, payment transparency is automatic. Data is also advance and simplified, making it simple to companies to adhere with rules and meet demands for data. And some of them argued due to the transparent nature of the technology, it should not be cordinated. One of the extreme concepts in blockchain technology is "transparency." Some people say that blockchain gives you privacy while some say that it is transparent, If we talk in the point of view of **cryptocurrency**, if you know the public address of one of these big companies, you can simply pop it in an explorer and look at all the transactions that they have engaged in. This forces them to be honest, something that they have never had to deal with before. However, that's not the appropriate use-cases. We are pretty sure that so many of these companies will not transact using cryptocurrencies, and even if they do, they won't do ALL their transactions using cryptocurrencies [16].

Immutability

Blockchains gives a native immutability feature which is integral and very important in each accord mechanism. In other words, immutability gives a proof of solution double spending problem and assures that each transaction should be stored on the blockchain without being duplicated. I strength the word *relative*, in the immutability property is tightly integrated with the technology beneath and relates to how difficult is for something to change. Basically, Bitcoin`s Proof of work mechanism immutability could be broken by a 55% attack on the network which would need a large amount

of computation power. However, as we have seen recently in Ethereum Classic 55% attack, immutability could not work if the network is not decentralized enough. Nevertheless, immutability is the aspect that has leveraged blockchain technology as being the most unruly technology we ever create as it provides mutability for transactions without a belief in 3rd party. With this property, can it be extended beyond transactions and also be applied to data, providing mutability for documents, records, contracts etc.

There are three reasons why we need to know about Blockchain

There is no need that Blockchain technology to exist publicly. It can also exist privately - where nodes acts as points in private network and the Blockchain acts similarly to a distributed ledger. Institutions which are under high pressure to display that their company employs follows their laws, standards, ethical practices that apply to the specified organization and hence now moving forward with Blockchain implementations.

Solutions of blockchain which are secure are major building block to decrease the compliance costs. Block-chain technology is comprehensive than finance and can be applied to any transaction with multiple steps where traceability and visibility is required. The disruptive growth of Blockchain will come only by intersection of public and private Blockchains. By combining public and private blockchain to ecosystem customers, suppliers where firms, customers and suppliers can merge in a secure, auditable and virtual way.

Blockchain Applications

- Asset Management: Trade Processing and Settlement
- Insurance: Claims processing
- Payments: Cross-Border Payments
- Unconventional money lenders/ hard money lending
- Your car/ Smartphone
- Blockchain Internet-of-Things (IoT)

- Smart Appliances
- Supply Chain Sensors
- Blockchain Healthcare
- Blockchain music
- Blockchain Government
- Public value/ community
- Vested responsibility
- Blockchain Identity
- Passports
- Birth, wedding, and death certificates
- Personal Identification

Conclusion

Through this paper it has tried to explain that blockchain technology's uses many concepts and features might be broadly expandable to a variety of situations. These appearances are apply not only markets transactions , but also beyond to segments as diverse as government, health, science, literacy, publishing, economic development, art, and culture , and possibly to all human progress. Blockchain technology could be quite integral in this future world that includes both centralized and decentralized models. Likewise with the new technologies, the blockchain is a concept that originally disturb, and extra it could advertise the evolution of a larger ecosystem that includes both the old way and the new modernization. There are some historical examples that the invention of the radio it leads to increased record sales, and ereaders such as the Kindle have increased book sales. Now, we obtain news from the *New York Times*, blogs, Twitter, and personalized drone feeds alike. We absorb media from both large entertainment companies and YouTube. By this, blockchain technology could exist in a larger ecosystem with both centralized and decentralized models.

References

[1].Banking Is Only The Start: 20 Big Industries Where Blockchain Could Be Used. (2016, July 25). Retrieved from CB INSIGHTS: https://www.cbinsights.com/blog/industries-disrupted-blockchain/

[2].Blockchain Technology Review- Bitcoin Public Ledger. (n.d.). Retrieved from Playersmoney: http://www.playersmoney.com/blockchain-technology

[3].Boersma, J. (2016). Blockchain technology: 9 benefits & 7 challenges. Retrieved from Deloitte: https://www2.deloitte.com/nl/nl/pages/innovatie/artikelen/blockchain-technology-9-benefits-and-7-challenges.html

[4].Folpmers, M., & Olijve, M. (2016, February 19). The Pros and Cons of Blockchain, and Its Impact on the FRM Community. Retrieved from GARP: http://www.garp.org/#!/risk-intelligence/all/all/a1Z400000031m2sEAA Gem Announces Title Sponsorship Of Inaugural Distributed: Health Conference. (2016, August

[5]. Retrieved from Coinidol: https://coinidol.com/gem-announces-title-sponsorship-of-inaugural-distributed-health-conference/

[6].Genovese, B. (2016, April 22). Blockchain technology: hype or reality? Retrieved from CIO: http://www.cio.com/article/3058266/security/blockchain-technology-hype-or-reality.html

[7].Greenspan, G. (2016, March 17). Blockchains vs centralized databases. Retrieved from MultiChain: http://www.multichain.com/blog/2016/03/blockchains-vs-centralized-databases/

[8].Hobey, E. (2015, September 10). Saving Time and Money through Blockchain Tech: Chain Secures $30M Series B from Industry Behemoths Visa, Nasdaq, Citi Ventures. Retrieved from CROWDFUND INSIDER: http://www.crowdfundinsider.com/2015/09/74180-saving-time-and-money-through-blockchain-tech-chain-secures-30m-series-b-from-industry-behemoths-visa-nasdaq-citi-ventures/

[9].How Will Blockchain Technology Transform Financial Services? (2016, February 23). Retrieved from MOORISH HAREM: http://moorishharem.com/how-will-blockchain-technology-transform-financial-services/

[10].Japan Drones Selects Guardtime to Deliver Keyless Signature Infrastructure for UAVs. (2013, March 25).

Retrieved from Unmanned System News: http://www.unmannedsystemstechnology.com/2013/03/japan-drones-selects-guardtime-to-deliver-keyless-signature-infrastructure-for-uavs/

[11].Mukerjee, P. (2016, April 6). All You Need to Know About Blockchain And CryptoCurrency- The Next Big Things In FinTech. Retrieved from SWARAJYA: http://swarajyamag.com/magazine/blockchain-and-cryptocurrency

[12].Our spokes are the heart of our business. (n.d.). Retrieved from Consensys: https://consensys.net/ventures/spokes/

[13].Rafi, U. (2015, May 11). P.A.W Capital's Long-term Technology Picks Stole The First Quarter. Retrieved from INSIDER MONKEY: § http://www.insidermonkey.com/blog/p-a-w-capitals-long-term-technology-picks-stole-the-first-quarter-346388/

[14].SCAP Resources. (n.d.). Retrieved from Scap: http://scap1.org/SitePages/Resources.aspx Shipley, D. (2016, June 6). Bring On the Blockchain Future. Retrieved from BloombergView: https://www.bloomberg.com/view/articles/2016-06-06/bring-on-the-blockchain-future

[15].Subramanian, I. (2016, April). The Benefits of Blockchain Across Industries. Retrieved from ORACLE: http://www.oracle.com/us/corporate/profit/big-ideas/041316-siyer-2982371.html Svetek, M. (2015, November 6). Digital Uncovered #1: What are Bitcoin and the Blockchain? Retrieved from Freeformers: https://freeformers.com/uncover-digital-bitcoin-blockchain-blog/#.WDTCoXqCCrN

[16].Sztorc, P. (2014, November 28). The Limits of Blockchain Tech. Retrieved from Truthcoin: Making Cheap Talk expensive: http://www.truthcoin.info/blog/limits-of-blockchain/