International Interdisciplinary Virtual Conference on
'Recent Advancements in Computer Science, Management and Information Technology'
International Journal of Scientific Research in Computer Science,
Engineering and Information Technology| ISSN : 2456-3307 (www.ijsrcseit.com)

The Future of Blockchains in Creating Decentralized Networks and Solution for Risks Associated to its Security

Aditya Khade
BCA Second Year, Shankarlal Khandelwal College of Science, Akola 444002, Maharashtra, India

ABSTRACT

One of the most economically disruptive technologies yet revolutionary innovations made in January 2009 by Satoshi Nakamoto was Bitcoin which was stiff backed by the emerging technologies such as the blockchain and smart contracts at its backend. Blockchain enabled a decentralized architecture network that is secured and transparent, compared to the current infrastructure with centralized tech giants governing over the data. The peer-to-peer transactions and shared ledger exchanges made possible using blockchain and smart contracts can resolve major problems and fuel innovations. However, it is still forwarding flaws and security issues like 51% attack, sybil attack, DDoS and censorship governance. We have discussed the future potential applications and challenges blockchain technology concept might face, as well as possible solutions and preventive measures.

Index terms: Blockchain, Smart Contracts, Decentralization, Peer-to-Peer, Ledger

I. INTRODUCTION

Bitcoin introduced Blockchain technology in 2009 which has potential to change the world. The use of a blockchain system enables an open ledger accessibility without intervention from third parties. A blockchain at core base consists of multiple interconnected blocks that hold data in a decentralized network, with each computer retaining its own version for reliability purposes throughout the database. The entire structure lacks any singular failure point due to this design feature as well.[1] Furthermore, once an entry is permanently established on it sequentially, no modifications can occur because they are immutable by nature and irreversible thereafter.

The start of a blockchain involves the creation of an inaugural block, often known as the Genesis block. This primary record captures initial transactions and also receives a unique alphanumeric identifier called a cryptographic hash that is based on its timestamp. A few examples of Secure Hashing Algorithms are SHA-256 and SHA-512 that are used in Blockchains. The blocks are added in order to form an interlinked chain where each following block uses information from the previous ones & their own hashes- to create its own distinctive code for continued sequential ordering.[5]

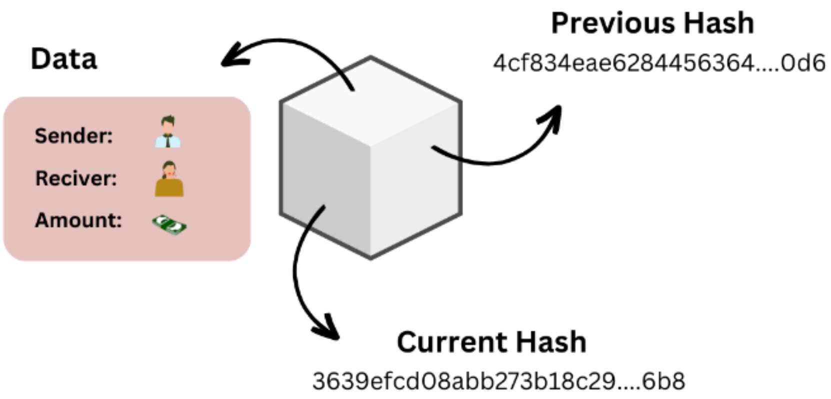

Fig.1 : A Block Contains.

A blockchain can majorly assist with building the next generation of web known as Web 3.0 at its backend. The currently in-use web 2.0 is a read, write, edit, upload, download etc. With the help of web applications hosted on a centralized server that gave rights to tech giants to rule over the data of end user of the service application which could be sold, manipulated or misused in certain unethical ways. Web 2.0 is commonly used for content creation and interaction, depicted through the current social media we use currently. On the other hand, In Web 3.0 there might not be such necessity to build such web applications that host on a centralized single server or database to store user data. Alternatively, a developer might deploy a Web 3.0 Application on decentralized Blockchain Platform which could be hosted on a peer-to-peer server.[4]

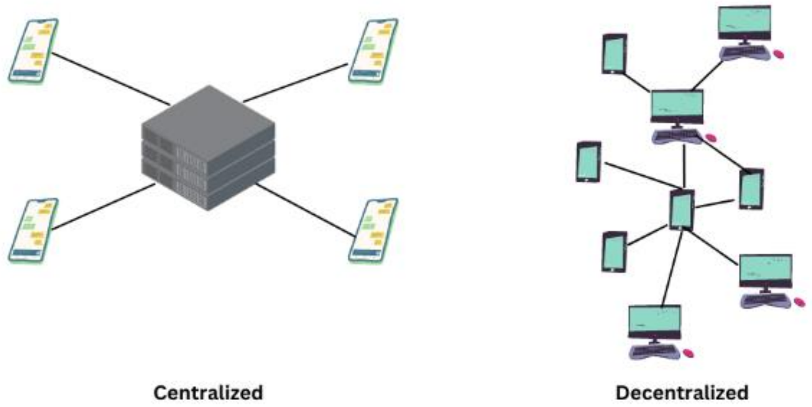

Fig 2: Centralized & Decentralized Network.

The most recent development is the introduction of smart contracts to blockchain. A Smart contract in a blockchain acts as contract just like in real life. A smart contract is a computer program used to exchange digital currency or tokens based on certain condition, commonly used for trading between two parties and stored on blockchain itself. They are preprogrammed to meet certain conditions and the end user at any node cannot change it.

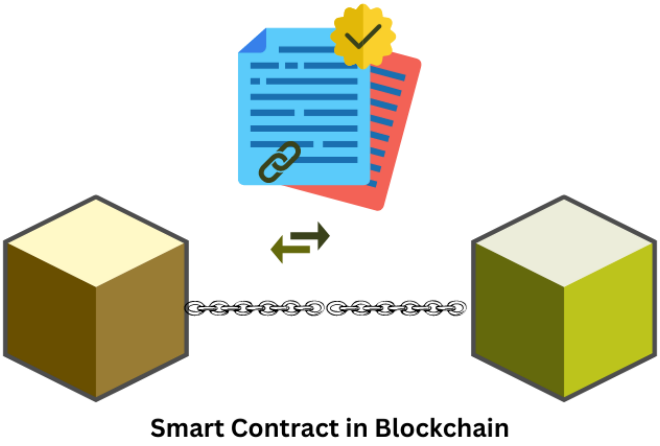

Fig 3: Smart Contract in Blockchain

Blockchain is capable of using consensus mechanisms or proof of work to provide transparency to ledger, also maintaining the integrity making intruders very tough to deploy a malware or compromise with the chain. If a hacker manages to compromise a single block by cracking the hash, it will make all following blocks invalid. We will further discuss the potential of how using this technology can improve and help in further to betterment of the society.

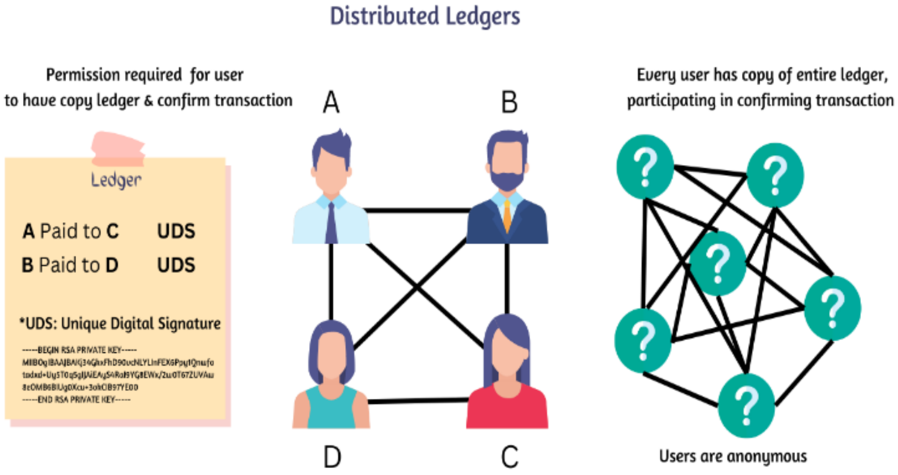
Distributed Ledgers
Permission required for user
to have copy ledger & confirm transaction
Ledger
A Paid to C UDS
B Paid to D UDS
*UDS: Unique Digital Signature
-----BEGIN RSA PRIVATE KEY-----
MIIBOgIBAAJBAKj34GkxFhD90vcNLYLInFEX6Ppy1Qnufo
txdxd+Uy5T0q5gIJAIEAyS4RaI9YG8EWx/2w0T67ZUVAw
8eOMB6BIUg0Xcu+3ahCIB97YE00
-----END RSA PRIVATE KEY-----
A
B
D
C
Every user has copy of entire ledger,
participating in confirming transaction
?
Users are anonymous

Fig 4: Distributed Ledger

II. METHODS

The end goal of this paper is to provide a brief overview of blockchains creating a better future for decentralized distributed ledger in terms of supply chains, a potential smart city that utilizes Blockchain technology in areas of developing infrastructure like healthcare, cryptocurrencies, supply chains, finance, web services, networks, and renewable energy and a free web (Web 3.0). Although the technology is not full proof it has some risks, in continuation possible solutions also have been mentioned.

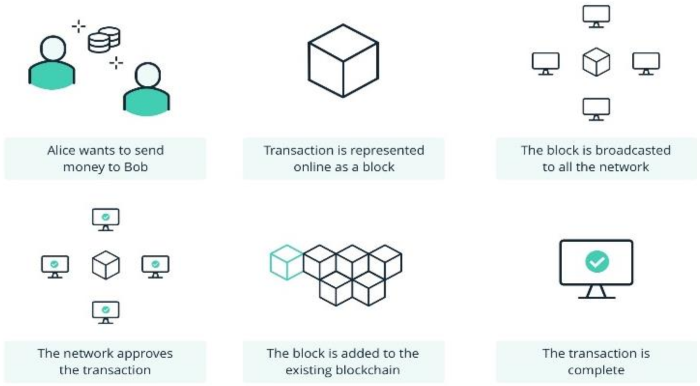
Alice wants to send money to Bob
Transaction is represented online as a block
The block is broadcasted to all the network
The network approves the transaction
The block is added to the existing blockchain
The transaction is complete

Fig 5: Working of blockchain, source: ledger.com

III. APPLICATION AND POTENTIAL

A. Green Energy Trading with Blockchain:

Blockchain could be the key to the green future. By generating renewable energy through solar power, hydro energy and windmills in resource rich areas with the help of government. The excess electricity could be transferred at the point of consumptions village and rural areas having scarcity of electricity using smart contracts evaluating units exchanged and the digital tokens used to make trusty and fair trade possible between both parties (producer and consumer) eliminating any intermediaries.

B. Trading in Game assets and NFT:

The Gaming industry is blooming undeniably in the world. With Triple A title games like CSGO individually has an active player base of 2 million players every day. These games have in-game tradable skins like NFT, allowing players to play with it inside the game. These skins have their own unique patterns allowing some of the assets to be much rarer and more different than each other, making it a valuable collectible for enthusiasts and collectors. A P2P Decentralized marketplace with smart contract can decide the price according to the demand and supply chain of these skins allowing them to profit without the need to deduct tax from a third-party marketplace, profiting in favor of both seller and buyer instead of third-party centralized marketplace who deduct 15% tax for both selling and buying.

C. Reduced Voting Frauds:

E-voting using blockchain could drastically reduce voting frauds and provide transparency to voting system while hiding the private information of the voter at the same time. Blockchain based e-voting smart-contract utilizes computer, smartphone to cast vote with use of signature algorithm to store digital signature of voter to prevent tempering after a vote is casted displaying result data publicly making sure no data is being manipulated.

D. Crowd Funding:

Smart contracts will set rules for transactions, that can be created using private blockchain technology. A smart contract is a self-executing system that uses blockchain to carry out exchange governed by its explicit terms and conditions. Smart contracts work with simple "if/when... then." statements that are written into code on a blockchain using Solidity (a programing language similar to JS used to code blockchain applications). A network of computers executes the operations after the predetermined requirements have been met and verified. The blockchain is automatically updated once the transaction is complete. [*]

Applications of Blockchain are many more, for instance:

- Storing healthcare records
- Managing small to big supply chains
- Solving Video Piracy etc.

Fig 6: Applications.

IV. RISKS

A. 51% Attacks:

A 51% Attack is when a hacker or an organization successfully decrypts hashes of equal or more than 51% of the block in the chain, making hacker gain full control over the blockchain. Most of the time hackers target small chains due to the ease of decrypting the length of blocks inside of a chain. Usually this takes a load of computational power to calculate and crack the hash of every single block making it impossible to crack long length chains. [2]

B. Censorship Governance:

Web 3.0 with blockchain provides freedom of speech to everyone.Removal of censorship after terms and regulation of a certain central governing entity is removed, it might create chaos of arguments on the Web 3.0. A problem in peer-to-peer network starts to shine when these arguments start to become uncontrolled then we might feel a need for governing force.

C. Bugs:

A program or a code written by humans is not always error proof, sometimes a coding error might start to work in certain way where it is not intended to creating threats and loopholes in application.

D. Scalability and DDoS:

DDoS also known as distributed denial of service attack, is when a hacker uses botnet to flood network with overwhelming request with fake traffic or malwares resulting bringing whole network infrastructure down. [3]

E. Sybil attack:

The perpetrator makes multiple personas to acquire power over the network or affect its decision-making process. With control of numerous nodes in their hands, they can tamper with the consensus mechanism and cause chaos within the network's operations while excluding legitimate participants from joining. Such actions result in trust disintegration as well as compromising security and integrity standards of these networks.

In General:

Greater Utilization of computational power like CPU and GPU produces heat & the energy consumption can be intensive, which can limit the adoption of the technology. However, if a solution is proposed to these problems in further research, Blockchain can potentially revolutionize the technology behind every simple thing that we see today giving birth to a new digitalization era.Limitations of research include major limitations such as scalability, interoperability, security, and energy consumption. Scalability has the inability to process and verify transactions in a timely manner due to the growing size of the blockchain network. Interoperability makes it difficult to transfer data between different blockchains. Security is also a concern, as new security threats may arise.

V. SOLUTION TO REDUCE SECURITY RISKS

A. Carefully Designed Pre-secured DAs and smart contracts:

Carefully developed decentralized application and smart contracts where secure coding should be the priority. Furthermore, Vulnerability checks, Development security operations, properly implemented access controls, crowd sourced bounty programs, regular audits can also improve overall results.

B. Community Voting based content removal:

Decentralization removes censorship. As before the Ruling centralized entity was the one that created rules and regulations in web 2.0, this creates a problem for other users to filter out the explicit or the content that should not be on internet. Hate Speech, Adult Content, Disturbing Images etc. To solve this a community-based voting could be carried out so the other users with similar decisions can ban or remove the uncensored content.

C. Proof-of-Authority:

Multiple layers of private blockchain systems often select the "Proof-of-Authority" (PoA) consensus method, specifically within confidential and restricted corporate settings. This method allows for the management of various duties including record keeping, access control as well as authentication. Typically, transaction data remains hidden from outsiders or unauthorized parties involved with the network operations.

D. Load Balancer and Filtered Trafficking:

The most effective way to prevent DDoS is to implement load balancers, Distributed storage techniques to store data across multiple nodes in network. Increasing Network Capacity & Employing Anti-DDoS protection services.

E. Verification Mechanisms:

Some decentralized networks can implement identity verification mechanisms, such as Proof of Work, Proof of Stake, or Proof of Identity. These mechanisms require participants to demonstrate a certain level of computational power, or identity verification before they can participate in the network. This makes it more difficult for an attacker to create multiple identities and gain control of the network nodes.

VI. FUTURE SCOPE

- **Smart cities:** Smart cities are collective integration of multiple applications enabled by blockchain, Finance, health, supply-demand chain, renewable energy, digitalized currency exchange, decentralized web, cyber security, removing the requirement of the third party, tracking world trade etc.
- Improved Anonymity of an individual.
- Improved accuracy by removing human involvement in verification.
- Cost reductions by eliminating third-party verification.
- Decentralization makes it harder to tamper with.
- Transactions are secure, private, and efficient.
- Transparent technology.
- Efficiency and speed.

VII. CONCLUSION

In the upcoming research, blockchain technology will be under scrutiny to investigate its potential extensions beyond cryptocurrency usage. Various domains such as healthcare, financeand decentralized data sharing among others shall be examined in this study for possible implementation of blockchain applications.[6] The goal is also to explore how it can benefit open science initiatives and Internet of Things projects by ensuring security and transparency while enhancing efficiency through smart contracts or distributed ledger systems.

VIII. ACKNOWLEDGMENTS

We would like to express kind gratitude to Prof. Megha Tijare from Department of BCA, Shankarlal Khandelwal College of Science, Akola and Akshay Jain from Synack Security Network helping and guiding me in this paper.

IX.REFERENCES

[1]. Zibin Zheng, ShaoanXie, Hongning Dai, Xiangping Chen, and HuaiminWang “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trend ” (2017 IEEEE)

[2]. Md Rafiqal Islam, Muhammad mahbuburRahaman, Md Mahmud “A Review on Blockchain Security Issues ans Challenges” (2021 IEEEE)

[3]. Shweta Singh, Anjali Sharma, Dr. Prateek Jain “A Detailed Study of Blockchain: Changing the World” (2018)

[4]. Christos Karapapas, Iakovos Pittaras, George C. Polyzos “Fully Decentralized Trading Games with Evovable Characters using NFTs and IPFS” (2021 IFIP)

[5]. Santoshi Nakamoto “Bitcoin: A Peer-to-Peer Electronic Cash System. www.bitcoin.org, 1 November 2008. www.bitcoin.org/bitcoin.pdf, accessed”(20 June 2017)

[6]. Cai Y, Zhu D Fraud “Detections for Online Businesses: A Perspective from Blockchain Technology. Financial Innovation”(2016).

[7]. Mohsen Attaran, California State University, Bakersfield, Harrisburg “Blockchain for GamingChapter”(September 2019).