Blockchain For Secure Transaction

Amit Walia, Sumeet Kumar Monti, Aniket Kumar, Adarsh Raj, Keshav Kumar
CSE, Chandigarh University, Amit Walia
Amitwalia812@gmail.com
CSE, Chandigarh University, Sumeet Kumar Monti
Sumeetkrm07@gmail.com
CSE, Chandigarh University, Aniket Kumar
Aniketkumar62055@gmail.com
CSE, Chandigarh University, Adarsh Raj
Adarshraj82945@gmail.com
CSE, Chandigarh University, Keshav Kumar
Keshav15118225@gmail.com

ABSTRACT

With the development of digital transactions a need for fraud-proof, transparent and tamper-evidence system is emerge. Given the decentralized, immutable and cryptographic nature architecture of Blockchain technology this has proven to be one of the best solutions for secure transactions. This paper discusses the basics of blockchain, which provides decentralized shared ledger for secure transactions regarding financials and some of the health, supply chain sectors. Scalability, regulation concerns and computational energy are among the challenges addressed together with use-cases and possible future developments in the form of a case study.

I. INTRODUCTION

The number of online transactions on different platforms, from finance, health care, logistics, government services have all boomed through this digital era. Using centralised financial institutions as well as third-party intermediaries (banks and payment processors puts you at risk of security issues like data breaches, frauds or cyberattacks.

A new way of secure transactions as intermediaries are eliminated, transparency, immutability and cryptographic security are the basic features actually available on Blockchain (a Decentralized distributed ledger technology) The foundation of blockchain technology is a peer-to-peer (P2P) network that confirms transactions in a trusted and verifiable manner.

A block stored multiple transaction, chained together with cryptographic hash of previous block. The nature of blockchain being a distributed prevents from a single point of failure, thus it is better candidate for securing both financial as well as non-finance transactions.

This will be a broad-ranging publication about the blockchain regarding transactions security, case studies, advantages and limitations followed by an outlook to future.
2. Introduction to Blockchain Technology

2. Structure of Blockchain

A blockchain has many blocks in it, every block each having;

Transaction: The information of transactions (sender, receiver, amount, timestamp)

Hashes: A cryptographic identifier for the block.

Previous Hash- Links the current block with the previous one, so the chain coherent.

Blocks are added one by the consensus method, therefore doing the way it must be to keep upright from tampering.

2.2 Consensus Mechanisms

Types of consensus: helps with authenticating transactions that must occur on the blockchain and keeps accurate. Some popular ones are

Proof of Work (PoW) You gotta do a little bit of work to solve cryptographic puzzles (= Bitcoin)

PoS (Proof of Stake):Validators are picked based on how many tokens are with them and how much they "stake" in the network

Delegated Proof of Stake (DPoS) Allows users to vote and determine the trusted validators.

Byzantine Fault Tolerance (BFT): Guarantees network security even some nodes fail.

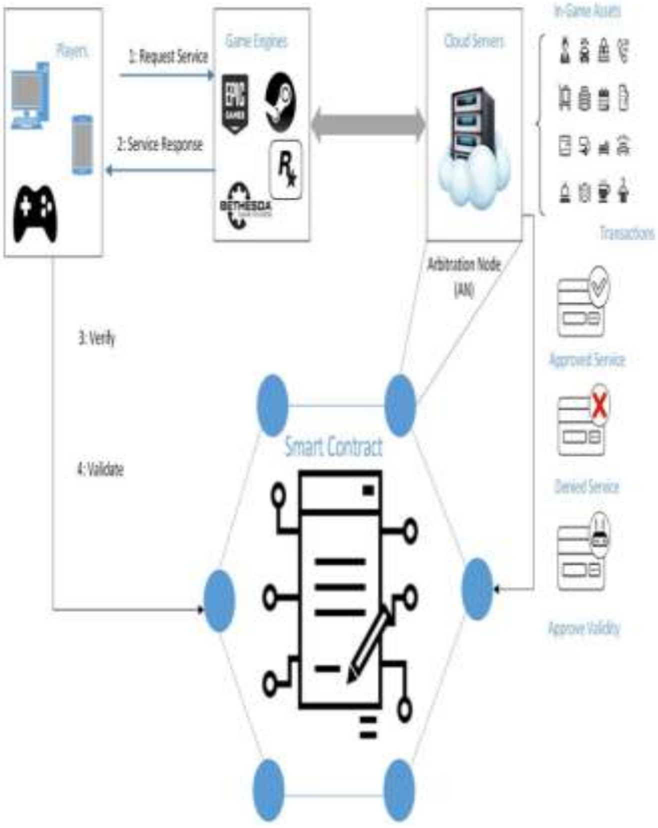
Blockchains Advancements in Cryptographic Security

How blockchain uses a complex set of cryptographic methods to secure transactions;

Hashing (SHA-256): Input data is taken and converted to a fixed length hash simply for immutability reasons.

Public-Key Cryptography: Every one has a public and private key for secure authentication.

Digital Signatures: It provides the transaction authentication and non-repudiation i.e. ability to verify.



`

3. Secure Transactions using Blockchain for App

3.1 Finacial Transactions

Decentralized financial transactions are changed with Blockchain as it first removes the intermediaries and then reduces the cost to usability for mass as well as security. A few of these include;

Cryptocurrencies (Bitcoin, Ethereum): De centrale, belastingun vereermde digitaal geld dat preventief aangegeven is aan fraud en dwars klikkering.

Trans-national Exchanges: Solutions exist in the space of Blockchain based near-100% instant and low-cost cross border exchange.

Fraud Prevention: Because blockchain is immutable (it literally can not go backwards) modification or identity theft is impossible.

3.2 Supply Chain Management

The use of Blockchain can help make supply chain more secure and transparent:

Supply Chain Tracing All products registered with you via the system can track from production to delivery so authenticity is not an issue and hence no counterfeit device.

A contract that is a smart contract — an automatically enforceable code provision that defines the terms of a contract without third parties

IBM Food Trust (Food Safety), for example: Companies like IBM are using blockchain to track food supply chains and ensure safety at the largest scale.

3.3 Healthcare Security

Blockchain makes healthcare operations secure and efficiently executed on a centralised platform :

Tamper-Evident Medical Records: The medical history of patients are securely stored only accessible to authors ridden personnel.

Drug Falsification — authenticates supply chain transaction to prevent the counterfeit of drugs.

Clinical Trials: Makes research data transparent and authentic possible.

3.4 Government end Management of Identity

In public services in a secure, transicendental and meaningful way, governments use blockchain:

Digital IDs: The most common use-case is to enhance secure identity verification (E.g.: Estonia's e-Residency)

Voting systems: Blockchain powered elections increase transparency and decrease fraud.

Example: blockchain-based land registry systems - Countries like India and Sweden are trying out blockchain solutions for land records.

4. How Blockchain Enabled Secure Transaction Benefits

4.1 Immutability

In switch from a blockchain records cannot be edited anymore the probability for fraud and unauthorized modifications is decreased.

4.2 Decentralization

No need for central agencies, decrease the duration of central failure and increases the security.

4.3 Transparency and Trust

Public blockchains provide traceable transaction histories that build trust in the community

4.4 Improved Security

Cryptographic techniques of blockchain ensure hacking, hacking, and identity theft by unauthorized access.

.

5. Challenges and Limitations

5.1 Scalability Limitations

Blockchain network, especially PoW based ones, suffer large issues with transaction throughput and speed, resulting in a congestion to much higher fees.

5.2 Energy Consumption

Environmental concerns due to massive energy spent on maintaining PoW mechanisms

5.3 Regulatory Uncertainty

Legal & Regulatory headaces from a blockchain perspective (different countries have different regulations)

5.4 Privacy Issues

While Public blockchains are transparent and permit access to transactions details which are vulnerable in nature.

6. Blockchain case studies in secure transactions

6.1 Bitcoin: Money plus financial security

The first blockchain-based cryptocurrency, Bitcoin allows secure peer-to-peer transactions without intermediaries. Bitcoin has stayed secure albeit extremely volatile since its beginning in 2009

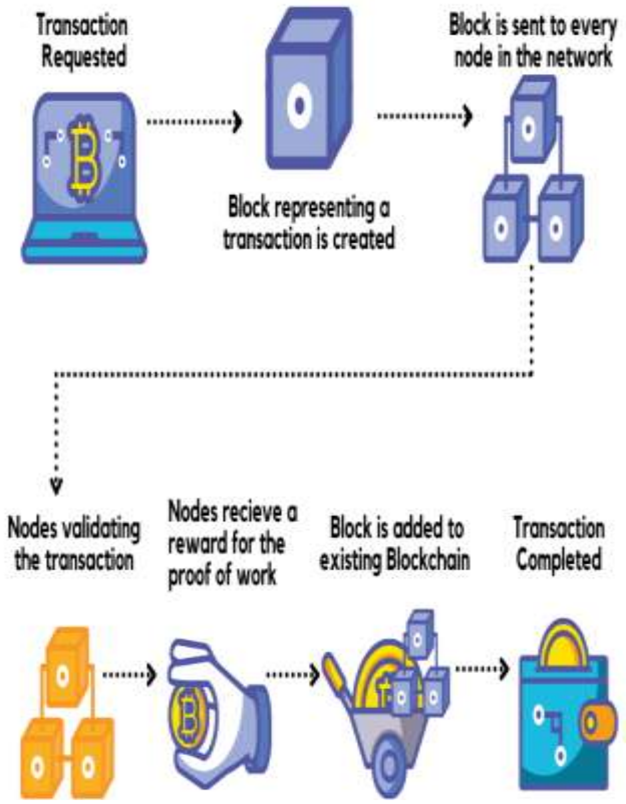
6.2 IBM Food Trust and Chain of Custody Security

IBM Food Trust leverages blockchain to follow the trace of food products so that consumers can trace contaminated food and recall it quickly.

6-3 Governance in the Blockchained

Governance of Estonia Block-based democracy—Estonia made its national digital ID system super secure to provide better e-government services and protect citizen data.

7. Blockchain Future for Secure Transactions


Transaction Requested
Block representing a transaction is created
Block is sent to every node in the network
Nodes validating the transaction
Nodes recieve a reward for the proof of work
Block is added to existing Blockchain
Transaction Completed

7.1 Layer 2 Scaling Solutions

Layer 2 Scalable solutions Lightning Network and Plasma boost speed of transactions reducing fees.

7.2 Quantum-Resistant Cryptography

By the time quantum computing further develops, blockchain developers will have been building quantum resistant encryption functions.

7.3 Hybrid Blockchain Models

Use both public and private blockchain features to compromise on transparency of a blockchain while providing privacy.

7.4 Integration of Blockchain and AI

Artificial Intelligence (AI) can make blockchain secure by using advanced algorithms to identify illegal activities and unutilized smart contracts.

8. Current Trends in Blockchain for Secure Transactions

With blockchain advancing more and more, new trends around it are also coming that make transactions secured, effective as well as more practical in real-world environments. Those trends can included:

8.1 Decentralized Finance (DeFi) and Smart Contracts

Decentralized Finance (DeFi) — Financial Intermediaries outsourced by users to help facilitate direct P2P transactions over a competitor of centralized infrastructureDeFi causes disruption on traditional financial systems through eliminating all the intermediaries. Smart contracts help to provide transparency and security verifying transactions, based on the conditions set before. DeFi applications ranging from lending to staking up and decentralizd exchanges (DEXs) that are proliferating shows the scope blockchain has in securing funds.

8.2 Zero-Knowledge Proofs (ZKP) for Privacy

Zero-Knowledge Proofs: allows a holder of secret information to prove that they know or own some information, without revealing this information. Further enhances privacy in blockchain transactions without trust. Privacy-preserving blockchain implementations, e.g., zk-SNARKs or STARKs are increasing the security level of blockchain.

8.3 Central Bank Digital Currency (CBDCs)

There is active work by governments and central banks in relation to the issuance of blockchain-based digital currencies. CBDCs are a secure and efficent way to execute financial transactions as well as compliance with the regulatory environment. With countries like China issuing its own digital yuan and the European Union exploring to launch a digital euro closer look at blockchain powered national currencies.

8.4 Blockchain Networks Interoperability

Most blockchain networks operate in silos and do not communicate with each, which means no inter-communication nor cross-chain transactions. New proposals in the form of Polkadot, Cosmos and Chainlink, among others are surfacing as blockchain interoperability to bring over seamless data & asset transfers between blockchains together they simplify the structure of widespread uses.

9. Blockchain Ethical and Social Implications

There are many ethical and social challenges of the blockchain that need to be solved in order for it grow in such a way that is sustainable.

9.1 An Ongoing Digital Divide and Accessibility

Blockchain Acceptance is Still Variable In The World Developed nations automatically have a faster start into blockchain, underdeveloped regions are still having to go the digital zero suddenly amidst lack digital infrastructure or technical competency. Universal blockchain accessibility to all users is pivotal in the globalized adoption.

9.2: "Privacy vs. transparency"

The transparency of blockchain, breeds trust but gives detail to transactions. Maximizing transparency versus privacy is imperative, particularly the various fields where data is engraved from healthcare to finance (GDPR, HIPAA…). Privacy-oriented blockchains such as Monero and Zcash are trying to work for example.

9.3 Traditional Jobs & Industries Affected

Blockchain can automate the financial services, legal contracts and supply chain management — which is going to disrupt a lot of jobs. Traditional roles in banking, auditing and legal arbitration may be replaced with more efficient operations via blockchain. On the other hand, blockchain development, security audits and smart contract management chances are flying.

10. Risks and Security Threat

Blockchain aside its benefits, not all consequences are beneficial. It is not puzzling to think of these security threats;

Incentive Rollups and Compact Proofs 01(block/real/time)
51% attack is when an entity owns more than half of mining power and thus has the ability to defraud transactions. Though rare in large networks like Bitcoin, there are plenty of smaller blockchains which can be attacked in the same way.

Smart contract vulnerabilities Watch
Code errors in the smart contract can be manipulated by hackers. The 2016 DAO hack for instance was responsible for the theft of 36KETH (~$50 million) from a smart contract bug. Risks can be reduced as well by high-quality security audits and methodology of formal verification.

Quantum Computing Danger (threat 10.3)
Once we have full-fledge quantum computers they will be able to crack the traditional cryptographic encryption in use with blockchain. Quantum-resistant Cryptography algorithms are in fact being worked on by cryptographers to protect from such attacks.

Risk Classification: 10.4 Regulation and Compliance Risks
Blockchain adoption is at the mercy of an often tenuous regulatory backdrop. While Governments around the world are creating different legislations, potentially conflicting policies will make blockchain innovation harder. We need a consistent and globally incorporated reg frame work for mass adoption.

11 Future Research Directions in Blockchain Security

However, for blockchain to remain not only a secured and scalable place for transactions, continued research must take place. This paper identifies the following research directions of interest to this field:

11.1 Cryptography Strong Against Quantum

Quantum computing is rolling out in droves and new crypto systems, such as lattice-based cryptography and hash-based signatures have to be accepted into blockchain networks.

Hybrid Blockchain Models 11.2

Combining public and private blockchain features can be used to improve the security layer simultaneously with one another with scalability. Hybrid blockchains such as Hyperledger Fabric are becoming popular due to purpose of openness and propriety access in many industries.

11.3 New Consensus Mechanisms

However, new consensus mechanisms like Proof of History (PoH) already implemented by Solana ultimately try to deliver faster transactions at lighter load equated with security. Research on alternative consensus algorithms will be able to scale up blockchain.

11.4 Blockchain Security powered by AI

It is through the dawn of Artificial Intelligence (AI) that blockchain security will be improved using pattern recognition to detect fraud, recognize bad actors & automate threat detection. Hopefully, AI with blockchain will greatly advance the cyber-security in the near future.
Conclusion
BlockChain has changed the Secured transaction of Industries anywhere from transparency, immutability and decentralization. Yet to gain broad adoption face challenges like scalability and regulatory uncertainty, along with new generation security threats .

Quantum resistant cryptography, better privacy mechanisms and AI enabled security will be key to the advancement of blockchain security in the future as well, a clear evolution of blockchain security.

As long as blockchain is still in use worldwide, it will be basic technology in securing digital transactions. with future research and innovation.

Acknowledgement
I would like to express my gratitude to all who supported the completion of my research paper. I would like to thank my mentors and professors for all the insights provided during this research. I hope they have helped me understand blockchain technology and secure transactions a bit more.

REFERENCES

https://ieeexplore.ieee.org/document/10182668/
https://www.researchgate.net/publication/350933679_Blockchain-Based_Framework_for_Secure_Transaction_in_Mobile_Banking_Platform
https://www.igi-global.com/chapter/blockchain-based-secure-transactions/324626
https://www.sciencedirect.com/science/article/pii/S2096720922000070
https://scispace.com/papers/blockchain-based-framework-for-secure-transaction-in-mobile-54zv26xwc6
https://ijrpr.com/uploads/V5ISSUE11/IJRPR35428.pdf
https://www.sciencedirect.com/science/article/pii/S2096720922000070