Blockchain for Secure Online Transaction

Introduction:
Blockchain is a digital ledger technology that facilitates decentralized, secure and transparent transactions across the network of computers. In today's world, we can see the expansion of this technology especially in cryptocurrency. Cryptocurrency (Bitcoin) and blockchain technology were introduced by an individual or group in 2008 using the pseudonym Satoshi Nakamoto (Nakamoto, 2008). The rise of other cryptocurrencies such as Ethereum, Litecoin etc. has introduced us to this technology further. There have been several research on Blockchain technology and why it should be an alternative to the digital banking system.

But for some limitations such as the public trust issue due to the fluctuation of cryptocurrencies and its volatile nature the perception of cryptocurrency and the blockchain technology itself have been affected as both are related to each other. Money such as UDS, EUR, AUD is considered fiat currency and it has value because the government or central authority declares it to be legal tender and which creates trust in currencies like UDS, EUR, AUD. But cryptocurrency is digital-only currency and due to the chance of being hacked or breach of privacy, the trust in this type of currency is still comparatively lower than the fiat currency.

In other studies, it's been explored that Blockchain achieves trust not through a centralized third-party authority, like a bank, but through peer-to-peer interactions among nodes in the network. This decentralized trust model is essential to the blockchain's ability to function securely without reliance on a central entity (Xu et al., 2017) and it eliminates the risk of facing a malicious third-party authority or central entity. In Bitcoin, by contrast, for an attacker to change history, they must solve computational puzzles at a faster rate than the rest of the participants combined. This is not only more secure, it allows us to quantify the security of the system (Narayanan, Bonneau, Felten, Miller & Goldfeder 2016).

Motivation:
Blockchain technology can be implemented in various sector including but not limited to banking, supply chain management, personal privacy maintenance. As security is the major concern for banking and blockchain technology is a recent breakthrough of secure computing, the implementation of blockchain in banking system can mitigate security risks related to hacking and vulnerability. Conventional banking system puts regulations to monitor the transactions and limitations to transfer money specifically internationally. But blockchain technology can eliminate these regulations and the costs related to the transaction.

This paper will explore the potential of Blockchain technology compared to traditional banking systems, how blockchain technology enhances the security of online transactions by using cryptographic techniques and decentralization. This paper will investigate how blockchain eliminates intermediaries in online transactions, improving efficiency, reducing transactional costs and will also investigate current challenges blockchain technology facing to be implemented in banking including scalability and energy consumption and explore potential solutions.

How does the blockchain works:
Blockchain is a public ledger, recording all transactions in a network across multiple nodes without relying on a centralized authority. This decentralization enhances security and transparency, as all participants in the network can verify transactions independently.

Each transaction is stored in a "block," which contains a list of transactions and a unique identifier, known as a hash. This hash links each block to the previous one, creating an immutable chain of blocks, hence the name "blockchain" (Xu et al., 2017). The integrity of each block is ensured by cryptographic hashing (often SHA-256). Modifying any data within a block would change its hash, which would be detectable by all network participants (Perez et al., 2018).

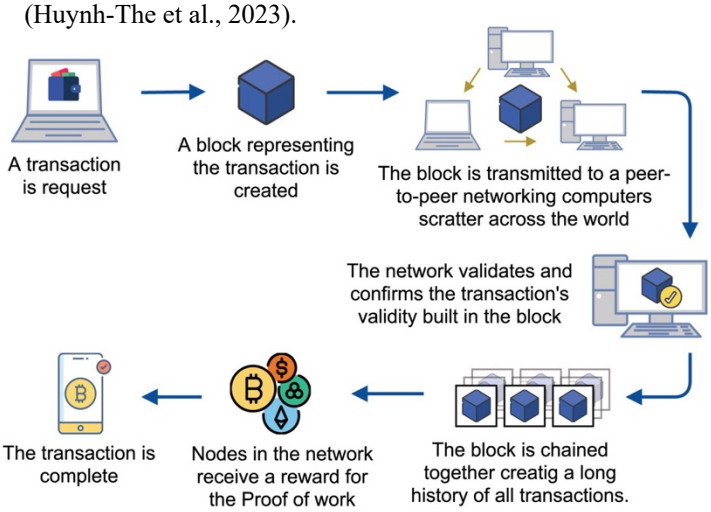
To add a new block, blockchain networks use consensus algorithms. In systems like Bitcoin, "proof-of-work" (PoW) is a common method where miners solve complex mathematical puzzles to validate transactions and create new blocks (Nakamoto, 2008).

Alternative consensus mechanisms, like proof-of-stake (PoS), exist to reduce energy consumption and increase scalability by relying on participants' stakes in the network rather than computational power (Guntara, Nurfirmansyah, and Ferdiansyah, 2023).

Transactions in blockchain involve transferring assets between participants, validated by digital signatures that ensure the transaction's authenticity. The signature confirms that the sender is legitimate, and that the transaction hasn't been altered. Modern blockchain platforms, such as Ethereum, support programmable transactions called "smart contracts." These are self-executing contracts with terms written directly into code, allowing for automated transactions without intermediaries

Once added, a block cannot be modified without altering all subsequent blocks, which is computationally impractical. This immutability is a key security feature, preventing unauthorized changes and ensuring a trustworthy transaction history (Niranjanamurthy, Nithya, and Jagannatha, 2018).

Fig. 1. General structure of a blockchain, in which blocks connected with each other through their respective hash codes (Huynh-The et al., 2023).



Challenge and Current Solution:

In the traditional banking system, banks operate as the central authority and often rely on third parties to facilitate international operations. The bank holds customers' funds and is responsible for securely facilitating all transactions, which builds trust among its customers. However, verifying these transactions takes time, and for larger or international transactions, additional approvals are often required, which can further delay the process. Banks use their own infrastructure to maintain the system, increasing maintenance costs. As a result, banks often impose high transaction fees, particularly for cross-border transactions, to cover these expenses.

Banks follow strict government regulations and their own policies, which creates a strong and secure system. While banks keep customer information private and secure, they may be required to disclose certain details to regulatory authorities working with the government. Each bank follows the regulations of its respective country, which can complicate overseas money transfers for customers. These limitations, although necessary to protect against inflation and economic instability in specific countries, can result in banks profiting through transaction fees, which may be high at some institutions.

Centralized servers, while essential for banks, are vulnerable to security breaches that could compromise customer data. To mitigate this, banks use centralized cybersecurity protocols, such as encryption and multi-factor authentication. These measures require ongoing upgrades and monitoring to ensure that the security of the system stays strong. Because of the growing use of cryptocurrencies, governments are increasingly taking steps to regulate their use. At the same time, banks are working to simplify the transaction process by implementing innovations like online banking and digital payment systems (e.g., mobile wallets).

In the realm of blockchain technology, there are public and private blockchains. Public blockchains are open-source networks with no restrictions, on the other hand private blockchains require authentication of participant identities and authorization of their permission levels. These private blockchains are often created and used by companies and banks to operate within specific regulations, with access limited only to those organizations (Lai and Lee, 2018). Many banks are experimenting with private blockchain technology to develop new international transaction systems that are faster and more cost-effective. Private or consortium blockchains are often used by banks for example, Hyperledger Fabric which is a modular blockchain framework designed to be used privately.

Many countries are also developing Central Bank Digital Currencies (CBDCs), a form of digital currency issued by a country's central bank. Governments are exploring digital currencies backed by the state as an alternative to cryptocurrencies. CBDCs are designed to eliminate third-party risks, reduce high cross-border transaction costs, and lower the costs associated with maintaining financial infrastructure within a country (Investopedia, 2024).

Critique of the current solutions:

Use of Third Parties in International Transactions (Traditional Banking) ensures compliance with complex international regulations, making transactions legally secure. These third parties also help build trust between banks, ensuring smooth transfers across borders. But these dependencies on intermediaries significantly increases transaction costs, especially for cross-border payments, making it expensive for customers. These third parties slow down the overall process, which contradicts the current need for speed in global financial transactions. Also, the traditional banking infrastructure is costly to maintain, and fees for international payments can become obstacle for smaller businesses or individual customers.

By following strict regulations banks protect both themselves and their customers from financial risks, including inflation and economic crises. These regulations often complicate international transactions, adding layers of bureaucracy which reduces efficiency. Though these regulatory compliances are necessary, banks tend to pass on the cost of these operations to their customers, leading to high transaction fees. Profit-seeking behaviour through high fees can be seen as exploitative, especially when fees seem disproportionate to the service provided.

Protocols such as encryption and multi-factor authentication are essential in protecting sensitive customer data. Even though these protocols offer a degree of protection, centralized systems remain vulnerable to large-scale breaches. If a centralized bank’s server is compromised, it can affect millions of customers at once. Centralized security solutions are reactive as they often address breaches after they occur, which might not be sufficient in an age where data is highly valuable and prone to targeted attacks. The costs of maintaining these centralized cybersecurity measures further increases operational expenses, which are often passed on to customers through fees.

Private blockchains provide controlled, secure environments and can reduce transaction times and costs. But the key problem is that private blockchains, by their nature, lack the decentralized benefits of public blockchains. This could limit the technology’s potential to provide true transparency, as it’s still controlled by a central authority (the bank). Also, the adoption rates are currently slow which could take years before this solution becomes widespread. Private blockchains are not solution for some vulnerabilities, such as insider threats or poor governance, and they could still be subject to regulatory overreach.

The introduction of CBDCs presents risks of government overreach, because central authorities may have too much control over a citizen's financial activities, leading to privacy concerns and it is nothing like blockchain technology. CBDCs can lower transaction costs, but their adoption could decrease the profitability of commercial banks and his could lead to resistance from existing financial institutions and slow down implementation. There is also a risk of technological hurdles, because implementing CBDCs on a large scale requires extensive and costly infrastructure updates and many countries may not be ready to adopt that quickly.

Solution to challenge:

To get solution of this problem we need to look at the implementation of blockchain technology in other sector for example construction industry to see the success of this

technology and to analyse whether this technology is just a hype or there is real potential of this technology in real world application. Research has been done of this technology in the construction and the document suggests that while blockchain technology has real potential in the construction industry, it is still at an experimental phase. The construction industry has been slow to adopt new technologies in past, including information technology, and blockchain is no exception.

However, blockchain shows credible promise in areas like procurement, addressing trust issues, security of transactions, and streamlining construction processes, particularly when combined with other digital tools such as Building Information Modelling (BIM). In conclusion, the paper argues that blockchain is not just hype but has credible application potential in the construction industry (Perera et al., 2020).

As blockchain can be a potential solution for real world problem, we need to focus on banking to implement this technology. There are protentional solutions we can implement. Banks can adapt blockchain technology not by replacing their whole existing system rather they can integrate to their present system.

For example, by using private consortium blockchains like Hyperledger fabric described earlier banks can maintain the regulatory compliances. This hybrid system can provide necessary trust while it can also reduce transactional cost and time. Currently banks use SWIFT messaging system which provides secure communication between financial institutions but does not actually move the money. Payments often involve multiple banks (correspondent banks) acting as intermediaries, especially for cross-border transactions. Each intermediary adds a layer of processing, which increases the time needed to complete the transaction. But the Hyperledger Fabric reduces this time by using peer to peer transaction. It provides real time transaction processing by instantly adding the transaction to the immutable ledger and make it visible to all authorized parties eliminating the delays caused by intermediaries.

Banks can implement smart contracts for transactions that require multiple approvals or verification steps, a smart contract can be programmed to automatically execute once predefined conditions are met, such as regulatory approvals. The blockchain is then updated when the transaction is completed. That means the transaction cannot be changed, and only parties who have been granted permission can see the results (IBM, 2024).

Discussion:

It is feasible for all banks to combine and create a blockchain network where any transaction is validated using consensus mechanisms. A system like that would work as a consortium blockchain, where each participating bank acts as a node in the network, and the blockchain records all transactions across banks. Here's how this could work and the benefits it could offer:

All participating banks would form a consortium blockchain, it would be a permissioned blockchain where only authorized banks can participate as nodes. The blockchain would allow banks to act as validators for transactions happening across the network, ensuring that all transactions are securely processed and recorded in real time. A consensus algorithm could be used for example Kafka or Raft, where validators are selected based on their trust in the system

When a customer initiates a transaction (e.g., transferring money between two banks), the transaction is broadcast to the blockchain network. Other banks in the network would use the consensus mechanism to validate the transaction. Once the transaction is validated, it is added to the blockchain, ensuring that all banks have a consistent, immutable record of the transaction.

Once a transaction is validated and added to the blockchain, it is effectively settled in real time. Unlike traditional systems, which may involve delays due to intermediaries or multiple systems needing reconciliation, blockchain would ensure immediate settlement, reducing processing time significantly.

Each transaction on the blockchain is encrypted and immutable, which provides high security and ensures that the transaction history cannot be tampered with. The system would also provide full transparency to all participating banks, who can access a shared, consistent ledger of all transactions.

in this system, there will be implementation of public blockchain as well. The consortium blockchain system that has been described above cannot interact with cryptocurrencies. But in this system, the transactions that are validated on the private blockchain can be confirmed on a public blockchain as well so that it can create an extra layer of trust and security. In this system, the consortium blockchain can be able to interact with cryptocurrencies. But it will depend on the main two parties between whom the transaction is going on and whether they want the interaction with cryptocurrencies or not. Using PoS in a public blockchain allows for smooth interaction between fiat currencies and cryptocurrencies. In this hybrid system, customers can convert fiat currencies to cryptocurrencies for international transactions. The public blockchain enables the exchange and management of these digital assets across borders, adding flexibility to the banking system.

This system will allow the bank's customers to convert their fiat currencies to cryptocurrencies on a public blockchain. On the other hand, as different countries have different banking regulations, based on that countries will create a consortium blockchain inside the country but for international transactions, they will use a public blockchain system which will add more trust and as the consensus mechanism for that purpose can be used PoS. In a public blockchain setting, PoS can ensure that validators (those who approve transactions) have a stake in the system, meaning they are financially motivated to act honestly. The stake (tokens or assets) serves as a security deposit, which can be lost if a validator behaves maliciously. This financial incentive helps prevent attacks such as double-spending or manipulation of transaction records. When handling cross-border payments involving multiple countries and regulatory environments, decentralized trust is necessary to ensure security. PoS allows validators from around the world to maintain the security of the blockchain without relying on a central authority.

While the private consortium blockchain handles most of the transactions within a country or group of banks, confirming transactions on a public blockchain adds trust, particularly for

international transactions where parties may not fully trust the private system. The public blockchain provides a global, transparent ledger that anyone can verify.

In traditional banking systems, international transactions are often processed by a few central authorities, which creates risks of centralization and single points of failure. A public blockchain using PoS helps decentralize transaction validation, distributing control among many independent validators.

Kafka and Raft are excellent consensus mechanisms for private, permissioned blockchains because they are designed for trusted environments where participants are known and trusted. These mechanisms provide high throughput and performance in closed, controlled networks like those used within a consortium of banks (Lai and Chuen, 2018).

However, for public blockchain interactions in cross-border or international contexts, PoS is preferred because it offers decentralized trust, meaning validators do not need to trust each other, as they are incentivized through staking. This is not achievable through Kafka or Raft, which rely on trust among known participants.

Conclusion:

This study delved into how blockchain technology could be incorporated into the banking industry to enhance transaction security and efficiency while reducing costs compared to traditional banking platforms. It highlights the benefits of blockchains nature and robust cryptographic security measures that remove the reliance, on external intermediaries. The discussion points out the potential of blockchain technology to solve various issues seen in traditional banking today like slow processing times and expensive international transaction fees through methods, like peer-to-peer validation, consensus mechanisms, and real-time settlement.

The research also recognizes the constraints such, as scalability issues and high energy usage alongside the uptake of blockchain technologies like private blockchains or Central Bank Digital Currencies (CBDCs). Despite these obstacles it's evident that blockchain holds promise as a reliable and effective substitute for current banking systems as seen through its successful applications in various fields, such as construction.

Combining public blockchains in an approach seems like a good way to go forward for banks as it offers the necessary regulatory compliance and control while also benefiting from the decentralized trust system of public blockchains for handling cross border and cryptocurrency transactions effectively. The integration of both systems can help banks offer clearer services that're efficient especially in international scenarios where trust and transparency play a key role. The inclusion of consensus mechanisms such, as proof of stake (PoS), in interactions further boosts security by encouraging validators to act with honesty.

A combined blockchain system using PoS consensus across multiple banks is not only technically feasible but also offers significant advantages in terms of speed, cost efficiency, security, and transparency over traditional systems like SWIFT. While there would be some challenges in terms of coordination, regulation, and initial costs, the long-term benefits of such a system could greatly transform global banking and financial transactions.

Overall, blockchain technology has the potential to transform the banking industry, by providing enhanced security, reduced costs, and faster transaction processing time. However, its widespread adoption will require overcoming regulatory, technical, and operational challenges, and future research should focus on addressing these obstacles to fully unlock the benefits of blockchain in the financial sector and should explore the integration of public and private blockchain technology together to improve the banking security and inclusion of more banking features.

References:

1. Nakamoto, S., 2008. *Bitcoin: A peer-to-peer electronic cash system*. Available at: https://bitcoin.org/bitcoin.pdf.

2. Narayanan, A, Bonneau, J, Felten, E, Miller, A & Goldfeder, S 2016, *Bitcoin and cryptocurrency technologies*, draft edn, Princeton University Press, Princeton.

3. Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., Pautasso, C., & Rimba, P., 2017. A taxonomy of blockchain-based systems for architecture design. *IEEE International Conference on Software Architecture (ICSA)*, 243-252.

4. Perez, M.R.L., Gerardo, B. & Medina, R., 2018. Modified SHA256 for Securing Online Transactions based on Blockchain Mechanism. *IEEE International Conference on Information Systems*, Technological Institute of the Philippines.

5. Guntara, R.G., Nurfirmansyah, M.N., and Ferdiansyah, 2023. Blockchain Implementation in E-Commerce to Improve The Security Online Transactions. *JSRET (Journal of Scientific, Research, Education, and Technology)*, 2(1), pp. 328-338.

6. Niranjanamurthy, M., Nithya, B.N., and Jagannatha, S., 2018. Analysis of Blockchain technology: pros, cons and SWOT. *Cluster Computing*, 22(S5), pp. S14743–S14757.

7. Huynh-The, T., Gadekallu, T.R., Wang, W., Yenduri, G., Ranaweera, P., Pham, Q.V., and Benevides da Costa, D., 2023. Blockchain for the metaverse: A review. *Future Generation Computer Systems*, 143, pp. 401–419.

8. Lai, R. and Lee, D. K.C., 2018. *Blockchain – From Public to Private*. *In*: *Handbook of Blockchain, Digital Finance, and Inclusion*, Vol. 2. Available at: https://www.sciencedirect.com/science/article/pii/B9780128122822000073, pp.147

9. Investopedia, 2024. *Central Bank Digital Currency (CBDC)*. Available at: https://www.investopedia.com/terms/c/central-bank-digital-currency-cbdc.asp

10. Perera, S., Nanayakkara, S., Rodrigo, M.N.N., Senaratne, S. and Weinand, R., 2020. Blockchain technology: Is it hype or real in the construction industry? *Journal of Industrial Information Integration*, 17, p.100125. Available at: https://doi.org/10.1016/j.jii.2020.100125

11. IBM, 2024. *Smart Contracts*. Available at: https://www.ibm.com/topics/smart-contracts#:~:text=Smart%20contracts%20are%20typically%20used,when%20predetermined%20conditions%20are%20met.

12. Lai, R. and Chuen, D.L.K., 2018. Blockchain – From Public to Private. In *Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2*. Elsevier Inc., pp. 145-177.