

7536439-blockchain-and-the-transformation-of-central-bank-currency-functions

SUMMARY: The article discusses how Blockchain technology is transforming the role of central banks in currency issuance and circulation. It highlights the potential benefits of Blockchain, such as reducing operational costs and enhancing transparency, but also acknowledges the challenges of legal frameworks, cybersecurity, and societal acceptance. The study uses a qualitative and conceptual approach, synthesizing literature from the post-2008 financial crisis to the present. The research question is how Blockchain can redefine the role of central banks in issuing and managing currency. The theoretical framework integrates trust theory, Blockchain as a "protocol of trust," and the theory of disintermediation. The findings suggest that Blockchain can improve monetary management by lowering operational costs and enabling the issuance of CBDCs. However, these opportunities are accompanied by challenges related to legal frameworks, cybersecurity, and societal acceptance.

METHOD: The study adopts a qualitative and conceptual approach, synthesizing international and domestic literature from the post-2008 financial crisis to the present. The theoretical framework combines three pillars: trust theory in financial transactions, Blockchain as a "protocol of trust" that replaces human intermediaries with algorithmic consensus, and the theory of disintermediation highlighting the rise of decentralized finance.

KEY FINDINGS:

- Blockchain can significantly improve monetary management by lowering operational costs and enhancing transparency.
- Blockchain-based digital currencies can be used as complementary instruments or substitutes for traditional systems.
- The shift from emotional trust to digital trust is a theoretical implication of Blockchain.
- The practical contribution is providing policy recommendations for central banks to adapt to the digital economy.

IMPLICATION FOR TRADING: The implications for trading are significant. Central banks may need to adapt their policies and regulations to accommodate the rise of CBDCs and decentralized finance. Traders and investors should be aware of the potential for new digital currencies and the potential impact on traditional financial systems. Additionally, the use of Blockchain technology can lead to more secure and transparent transactions, which can benefit traders and investors. However, the challenges of legal frameworks, cybersecurity, and societal acceptance must be addressed to fully realize the potential of Blockchain in the financial sector.

Blockchain and the Transformation of Central Bank Currency Functions

Nguyen Hoang Giang
Mekong University, Vinh Long Province, Vietnam
giangnguyenldxh@gmail.com

Abstract

The rapid evolution of Blockchain technology is reshaping the foundations of global financial systems, particularly the functions of currency issuance and circulation by central banks. With its inherent features of transparency, security, and decentralization, Blockchain offers new opportunities to reduce the costs of printing and transporting physical money while simultaneously enhancing the efficiency of monetary supervision. The purpose of this paper is to analyze how Blockchain can redefine the role of central banks in issuing and managing currency, and to evaluate the potential of Blockchain-based digital currencies as either complementary instruments or substitutes for traditional systems. The theoretical framework integrates three pillars: trust theory in financial transactions, Blockchain as a “protocol of trust” that replaces reliance on human intermediaries with algorithmic consensus, and the theory of disintermediation highlighting the rise of decentralized finance. Methodologically, the study adopts a qualitative and conceptual approach, synthesizing international and domestic literature from the post-2008 financial crisis to the present. The findings suggest that Blockchain can significantly improve monetary management by lowering operational costs, strengthening transparency, and enabling the issuance of central bank digital currencies (CBDCs). However, these opportunities are accompanied by challenges related to legal frameworks, cybersecurity, and societal acceptance. The theoretical implication lies in the shift from emotional trust to digital trust, while the practical contribution provides policy recommendations for central banks to adapt to the digital economy. Societally, Blockchain has the potential to reinforce public confidence in financial systems and foster innovation in modern economies.

Keywords: Blockchain, Central Bank, Digital Currency, Digital Trust, Smart contracts

1. Introduction

In the context of the global economy entering the digital era, Blockchain technology has emerged as a groundbreaking platform capable of reshaping the structure and functions of the financial and banking system. More than just a data storage and transmission technology, Blockchain introduces a new trust mechanism based on algorithms, cryptography, and distributed consensus, replacing the traditional reliance on intermediaries. This is particularly significant for the role of central banks - the institutions responsible for issuing, circulating, and supervising currency in the economy.

The development of digital currencies and decentralized finance (DeFi) applications presents both challenges and opportunities for central banks. On one hand, Blockchain can help reduce operating costs, enhance transparency, and improve

monetary management efficiency; on the other hand, it compels central banks to redefine their role in maintaining financial stability and strengthening public trust. The research question posed is: how will Blockchain technology transform the mechanism of trust creation, and how will this transformation affect the functions of currency issuance and circulation by central banks in the future?

The current research gap lies in the lack of in-depth analysis from the perspective of “digital trust” associated with the evolving role of central banks. Therefore, this paper aims to provide an interdisciplinary approach - combining technology, economics, and sociology - to clarify the impact of Blockchain on monetary issuance and management functions, while offering policy recommendations to help central banks adapt to the new context of the digital economy.

2. Theoretical Framework

Trust has always been the foundation of all financial and banking activities. In the traditional model, trust is placed in intermediaries such as central banks and commercial banks, which serve to verify, authenticate, and ensure the safety of transactions. According to Luhmann (1979), trust helps people reduce complexity and uncertainty in communication. Gambetta (1987) also emphasized that trust is formed through indirect signals such as reputation, consistent behavior, and credible evidence. In the financial system, the central bank is the focal point of these signals, thereby creating stability for the economy.

The emergence of Blockchain technology has introduced an entirely new approach to the issue of trust. With its decentralized, immutable, and transparent nature, Blockchain is regarded as a “protocol of trust” (Tapscott & Tapscott, 2016), where trust no longer depends on humans or intermediaries but is embedded directly into the system through consensus algorithms and cryptography. Nakamoto (2008), in the Bitcoin white paper, demonstrated that a decentralized system can operate effectively without a central authority, thanks to distributed verification and cryptographic security. This opens up the possibility of fundamentally changing the role of central banks in issuing and managing currency, as trust shifts from a centralized model to a decentralized digital one.

On this basis, the theoretical framework of this study combines three main pillars:

- Theories of trust in financial transactions: emphasizing the role of central banks as intermediaries that guarantee trust and system stability (Luhmann, 1979; Gambetta, 1987).
- Theories of Blockchain technology: affirming Blockchain as a new trust protocol, replacing reliance on humans with algorithmic consensus and distributed ledgers (Nakamoto, 2008; Tapscott & Tapscott, 2016).
- Theories of changing intermediary roles: analyzing the trend of reducing or eliminating the role of banks in many financial activities, while highlighting the rise of DeFi and CBDCs (BIS, 2020; IMF, 2021).

Beyond these three pillars, the study also draws on theoretical frameworks of digital trust systems (Brynjolfsson & McAfee, 2017), which argue that digital technologies not only replace intermediaries but also create a transparent transaction environment, reducing moral hazard and fraud. At the same time, theories of disintermediation in the digital economy (Chesbrough, 2010) are applied to explain how

Blockchain fosters the emergence of new financial models, where users directly participate in transactions without relying on traditional banks.

3. How Blockchain has influenced the transformation of Central Bank Currency Functions

The next section of the study - particularly significant for policy-making - demonstrates that Blockchain is simultaneously challenging and creating opportunities for central banks. Trust, once maintained by intermediaries, is now embedded into the digital system through cryptography, consensus mechanisms, and distributed ledgers. This creates an urgent requirement: central banks must shift from the role of “guarantor of trust” to that of “designer and supervisor of digital trust.”

In practice, this transformation can help reduce operating costs, enhance transparency, and facilitate the issuance of CBDCs. However, it also necessitates new legal frameworks, robust security mechanisms, and communication strategies to strengthen social acceptance.

Thus, the following analysis not only carries academic value but also provides crucial policy guidance for central banks as they adapt to the digital economy.

3.1 Paper Money – A Symbol of Trust

- Paper money has no intrinsic value like gold or silver. Its value comes from societal acceptance and trust in the issuing institution.

- When paper money became a medium of exchange, a trusted organization was needed to ensure secure transactions between unfamiliar parties - this led to the birth of commercial banks.

- Banks act as third-party intermediaries: holding money, verifying transactions, and ensuring reliability between strangers.

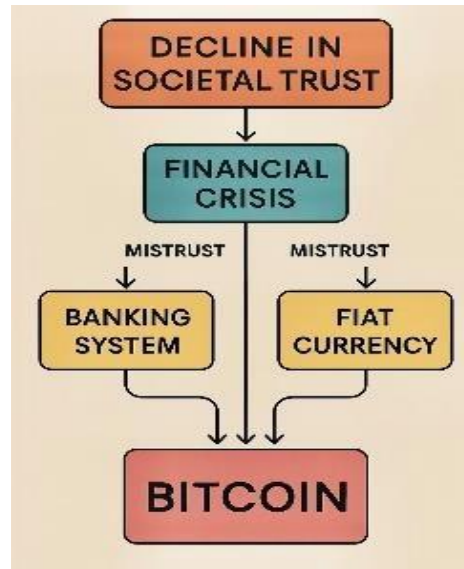
- From paper money to commercial banks and issuing banks (the predecessors of central banks), all have been great human inventions because they transformed trust into real value.

- There is no gold in a banknote, but there is trust in the financial system, in the state, and in the third-party intermediary.

3.2 The Birth of Bitcoin

- The 2008 financial crisis was the catalyst for the emergence of Bitcoin. It was not just a new currency, but a revolution in how we think about money, trust, and control.

- Bitcoin was born in 2009 as a direct response to the financial crisis, aiming to create a transaction system independent of banks.



(Source: Author's own design based on historical developments in blockchain)

Figure 1. From crisis to trust in financial intermediaries and the birth of Bitcoin

- According to Marc Andreessen - a prominent investor and tech entrepreneur who strongly supports decentralized technology - he stated:

“Bitcoin is truly the first application of blockchain technology that allows us to send a digital asset over the internet to another user, and this transaction is secure and protected. Everyone knows the transfer has occurred, and no one can interfere, tamper with, or alter the process.”

- Blockchain possesses these features thanks to its foundational characteristics.

3.3 Characteristics and Components of Blockchain Technology

3.3.1 Characteristics of Blockchain

What is Blockchain?

Blockchain is a technology that enables secure data transmission through an extremely complex encryption system - similar to a company's accounting ledger, where cash flow is tightly monitored. In this case, blockchain functions as a digital ledger.

One of blockchain's most distinctive features is that data transmission does not require an intermediary to verify the information. The blockchain system consists of numerous independent nodes capable of validating data without relying on “symbols of trust.” Information stored in the blockchain cannot be altered and can only be added with the consensus of all nodes in the system. This makes it highly secure against data theft. Even if part of the blockchain system collapses, other computers and nodes will continue to protect the data and keep the network running.

Blockchain technology is essentially a combination of three foundational technologies:

- Cryptography: Uses public key infrastructure and hash functions to ensure transparency, integrity, and privacy.
- Peer-to-peer networking: Each node in the network acts as both a client and a

server, storing copies of the application.

- Game theory: All nodes must follow consensus rules (e.g., Proof of Work, Proof of Stake) and are incentivized economically to do so.

From a business perspective, blockchain can be seen as:

- An accounting ledger
- A database of assets
- A data structure for recording asset history among members in a peer-to-peer network

From a technical perspective, it is an immutable method for storing the history of asset transactions.

From a social perspective, it is a phenomenon that establishes trust through consensus rules among members in a decentralized system.

3.3.2 Key Components of Blockchain Technology

Before delving into the components that explain the technical details and convey a general concept of the logic and underlying mechanisms of blockchain, the study presents the following example:

To predict tomorrow's weather - Party A bets that it will be sunny, while Party B bets that it will rain. If the result is either sun or rain, the losing party will pay \$50 to the winner. This agreement between the two parties usually relies on mutual trust or a neutral third party acting as an intermediary. However, this is often not an optimal solution. Blockchain technology is fascinating because it offers us a method that does not require trust in a third party, and it is extremely fast and inexpensive.

Blockchain allows us to write code to create a program that runs on the blockchain. In this example, both parties send \$50. The program securely holds the \$100 and automatically checks the weather the next day using various data sources. Based on whether the result is sunny or rainy, it will automatically transfer the entire amount to the winning party. Each participant can verify the contract's logic, and once it is uploaded and executed on the blockchain, it cannot be altered or stopped.

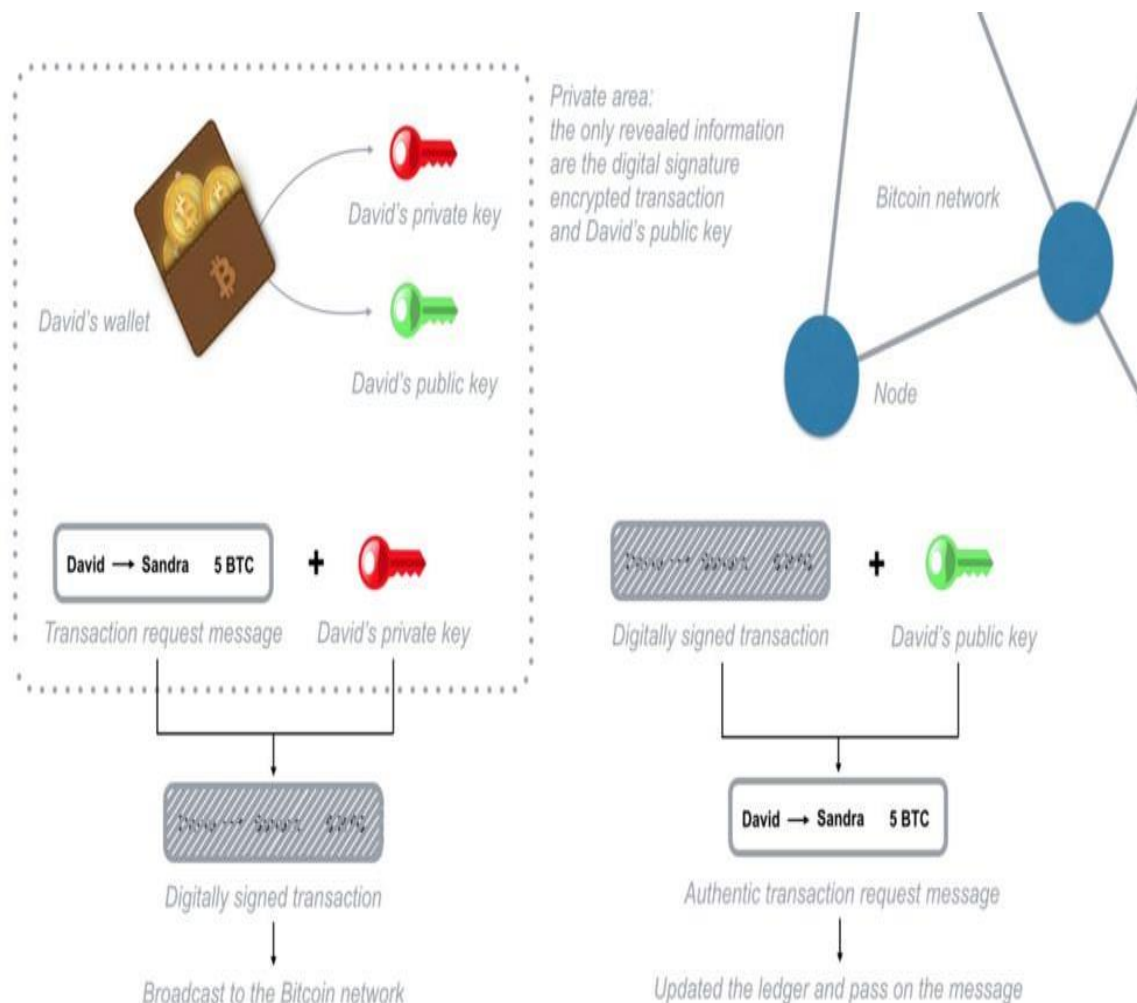
After approaching Blockchain technology in simple terms through the above example - next, we will go into each component of blockchain technology - in the logical order of the system's architecture as follows:

3.3.2.1 First Component – Blockchain Encryption Principles

We can define blockchain as a system that enables a group of computers to remain connected while securely updating a shared ledger. To make transactions on the blockchain - as previously described - you'll need a digital wallet, which is a software application that lets you store and exchange your Bitcoins. Because only you can spend your Bitcoins, each wallet is protected with a unique encryption method using a pair of security keys: a private key and a public key.

If a message is encrypted with a specific public key, only the owner of the corresponding private key can decrypt and read it. So when David wants to send Bitcoin, he encrypts a message using his wallet's private key - meaning he can only spend Bitcoin he actually owns - and since only he knows his private key, it's essential for accessing his wallet. Every node in the network can cross-check whether David's transaction request is legitimate by decrypting the message using his public key.

Encrypting a transaction request with your wallet's private key creates a digital signature. This signature is used by computers across the blockchain network to verify the sender's identity and validate the transaction. It's a string of text generated by combining the transaction request and your private key. If you alter even one character in the transaction request, the signature changes too - making it impossible for attackers to tamper with your transaction or change the amount of Bitcoin being sent. See Figure 2 for a clear visual of how private and public keys are used to secure and validate transactions.



(Source: Author's illustration based on cryptographic principles in blockchain)

Figure 2. Transaction Encryption and Validation Process in the Bitcoin Network

To send Bitcoin, you must prove that you own the private key of a particular digital wallet, as you'll need it to encrypt the transaction request. Once the encrypted message is sent, your private key never needs to be revealed.

3.3.2.2 Second Component – Blockchain Security Algorithm

If there's any disagreement about the final block in a chain, it could lead to potential fraud. For instance, if a transaction takes place in a block that belongs to the shorter tail when the next block is resolved, that transaction becomes unconfirmed again, since all other transactions have been grouped into the other block.

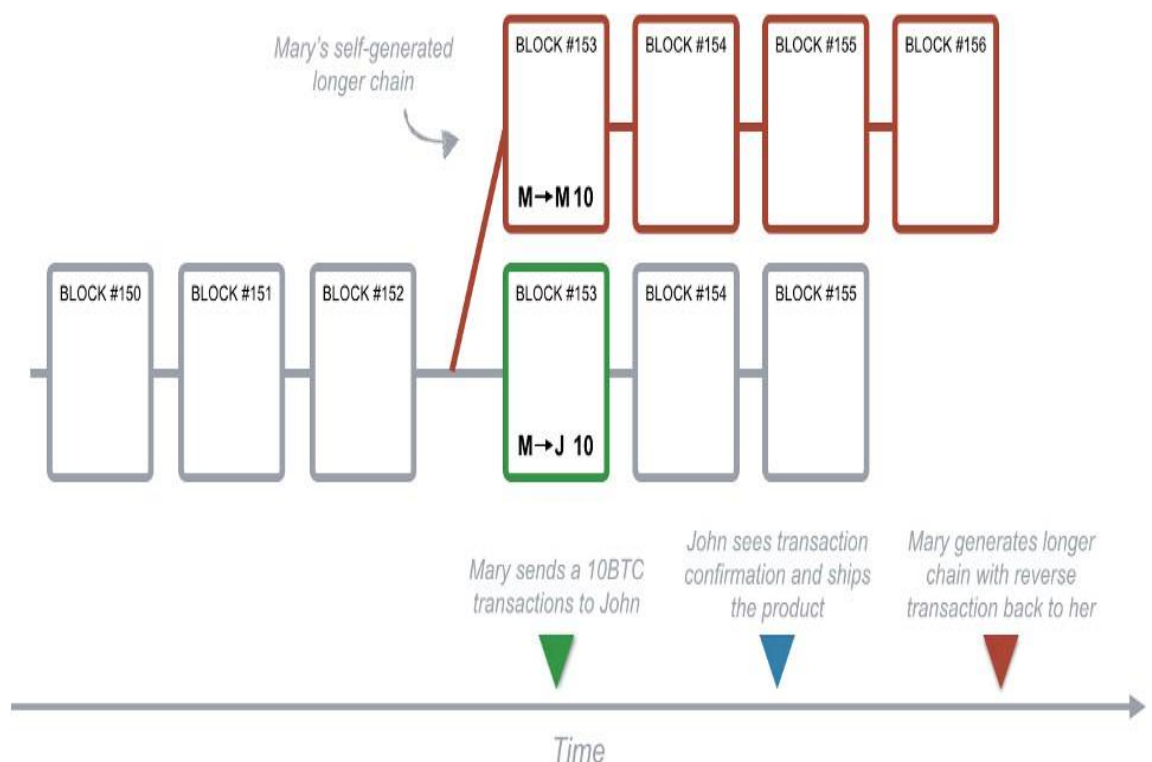
Let's look at how Mary could exploit ambiguity in the ending chain to perform an attack known as a "double-spending." Mary sends money to John, who then delivers goods to her. Because nodes always regard the longer tail as containing confirmed transactions, if Mary can produce an even longer tail - with a reversed transaction referencing the same input - John would lose both his money and his goods.

So how does the system prevent this kind of fraud? Each block contains a reference to the previous block, and that reference is part of the mathematical problem that must be solved to broadcast the next block to the network. It's very difficult to precompute a series of blocks because it requires generating a large number of random numbers to solve a block and add it to the blockchain.

Mary would be in a race against the rest of the network to solve the mathematical problem and get her block onto the chain. Even if she solves it first, it would be extremely difficult to continue solving 2, 3, or more blocks in succession, because she'd be competing with the entire network. Could Mary use a super-fast computer to generate random predictions quickly enough to outperform the entire network? In reality, even with high-speed hardware, the sheer number of participants makes it very hard for Mary to solve several blocks in a short time to execute a "double-spending" attack.

To make this clearer, see Figure 3 – it analyzes how an attacker can exploit ambiguity to reverse transactions and how the system defends against it.

Mary would need to control 50% of the computing power of the entire network to have a 50% chance of solving a block before another node does. Even then, she would only have a 25% chance of solving two consecutive blocks. The more blocks are solved in a row, the higher the probability of Mary's success.



(Source: Author's original diagram based on blockchain security concepts)

Figure 3. Double-Spending Attack Model and Blockchain's Defense Mechanism

Bitcoin blockchain transactions are protected by a computational race: any attacker must compete against the entire network's mathematical effort. Over time, transactions become increasingly secure. Blocks added earlier in the chain are always more secure than newly added ones. Since one block is added on average every 10 minutes, within about one hour from when a transaction is grouped into its first block, there is a fairly high probability that it has been successfully processed and cannot be reversed.

In blockchain technology, security algorithms and consensus algorithms are not merely separate technical components, but rather two closely intertwined pillars that together uphold the system's integrity, immutability, and decentralization. The consensus algorithm is the mechanism by which nodes in a blockchain network reach agreement on the current state of the ledger. With widely used mechanisms such as Proof of Work (PoW), the consensus algorithm ensures that no single entity controls the entire network, and that all changes must be approved by the majority - thus preserving decentralization.

Security and consensus algorithms are not just two layers of protection, but also two complementary and mutually reinforcing mechanisms that sustain trust in a system without intermediaries. This synergy is what gives blockchain its strength: a system that is transparent, secure, and resistant to manipulation.

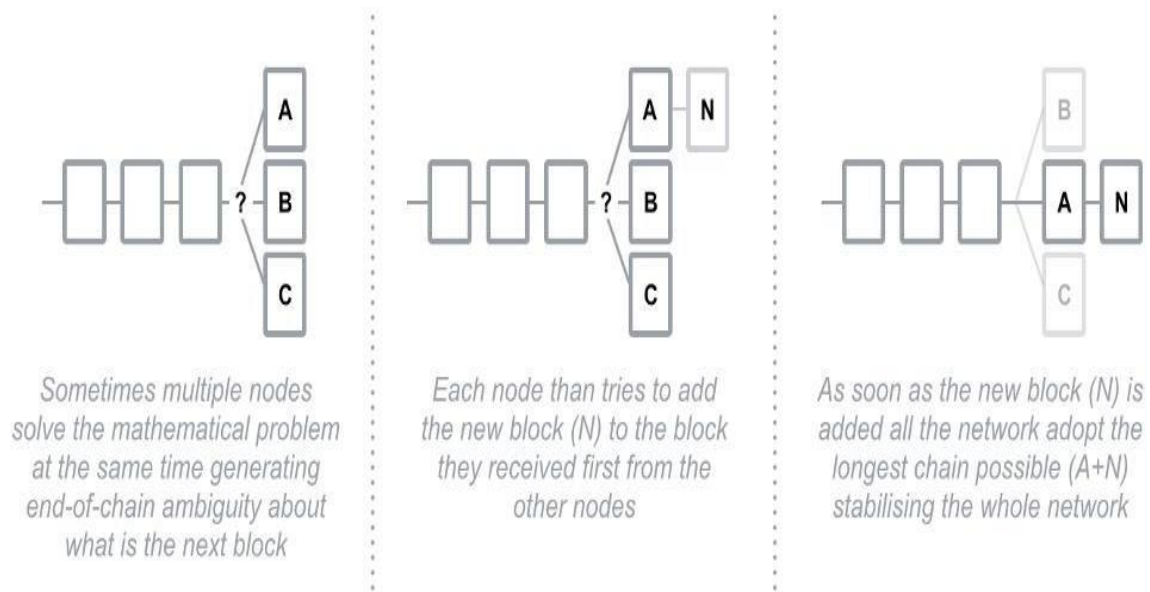
3.3.2.3 Third Component – Principles of Block Creation

Once transactions are submitted to the blockchain network, they are grouped into blocks. All transactions within a given block are considered to have occurred simultaneously, while transactions not yet included in any block are deemed unconfirmed. Each node in the network can organize transactions into a block and broadcast it, proposing it as the next candidate for addition to the blockchain. Since any node may create a new block, a key question arises: how does the network reach consensus on which block should be accepted as next in the chain?

To be added to the blockchain, each block must contain a special code that serves as the solution to a complex mathematical problem. This problem is generated using an irreversible hashing function, and the only way to solve it is to guess random numbers. These numbers, when combined with the content of the previous block, must produce a predefined result accepted by the system. For a standard computer with basic configuration, solving such a problem could take up to a year.

However, because many computers across the network simultaneously attempt to solve the problem, the protocol is designed to allow a new block to be created roughly every 10 minutes. The node that successfully solves the puzzle earns the right to attach its block to the chain and broadcast it to the network.

But what happens if two nodes solve the problem at the same time and broadcast their blocks simultaneously? In this case, both blocks enter the network, and each node starts building subsequent blocks on top of whichever block it received first. Nonetheless, the blockchain system has a rule: each node must build upon the longest valid chain it receives. So, if there's ambiguity about which block is the most recent, once a new block is added to either chain, every node will adopt the longer chain. This mechanism ensures consistency and prevents divergence.



(Source: Author's illustration of decentralized consensus principles)

Figure 4. Consensus mechanism when multiple nodes generate blocks simultaneously

Because the probability of simultaneous block creation is low, such conflicts are rare. When they do occur, the blockchain quickly converges into a single unified chain accepted by all nodes.

3.3.2.4 Fourth Component – Ledger Rules

Each node in the blockchain maintains a copy of the accounting ledger, so every node knows your account balance. However, the blockchain system doesn't actually track balances - it only records the requested transactions (see Figure 5).

In reality, the ledger doesn't monitor balances but keeps a history of every transaction sent across the Bitcoin network. To know your wallet balance, you need to validate and verify all past transactions that involve your wallet.

LEDGER	
Transactions	Value
Mary → John	10.000
John → Lisa	0.345
Sandra → David	18.4332
Lisa → Sandra	7.156
David → Mary	12.3402
Brian → Lisa	3.029381
...	...

(Source: Author's own design simulating blockchain ledger architecture)

Figure 5. Structure and Operating Principles of the Blockchain Ledger

Verifying this "balance" is done through computations based on references to previous transactions. To send 10 bitcoins to John, Mary must create a transaction request that includes links to previous transactions totaling at least 10 bitcoins. These links act as input values, and the nodes in the network will verify if their sum equals or exceeds 10 bitcoins. See Figure 6 for a detailed illustration of transaction structures, inputs and outputs, and how asset ownership is verified.

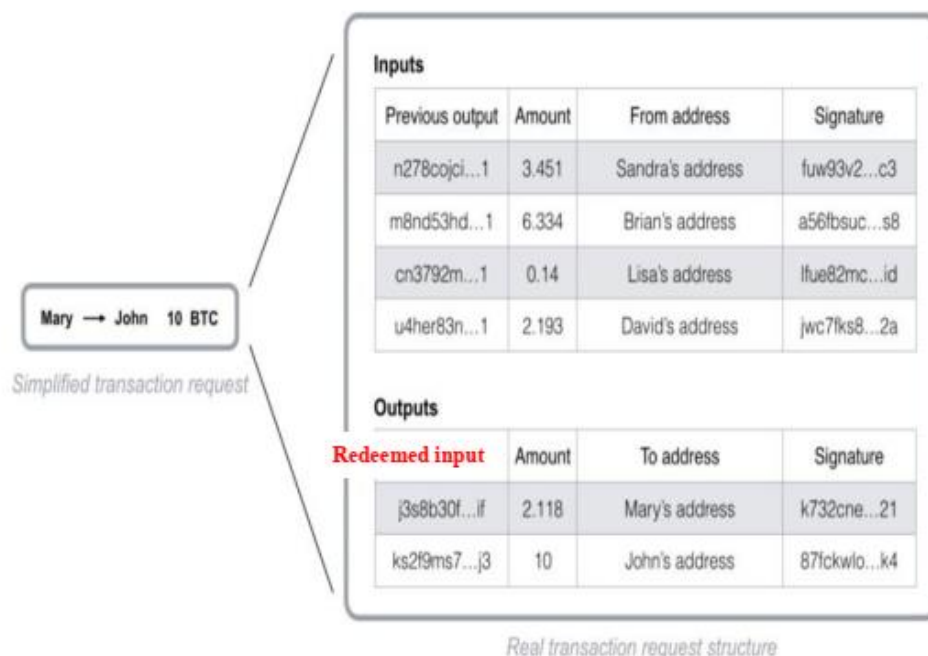
All of this is performed automatically by Mary's e-wallet and checked by Bitcoin nodes. Mary simply sends a transaction of 10 BTC to John's wallet using his public key. This raises the question: how does the system trust the transaction inputs and validate them? The answer lies in the nodes checking all prior transactions related to the wallet used - Bitcoin is sent using historical transaction references.

To simplify and speed up verification, a special record tracks all unspent Bitcoin - these unspent coins are stored by network nodes. Thanks to this checking mechanism, e-wallets help prevent "double-spending."

Owning Bitcoin essentially means having transactions in the ledger linked to your wallet address that haven't yet been used as inputs.

All source code for executing transactions in the Bitcoin network is open-source, meaning anyone with a laptop and an internet connection can join the network and make transactions. However, if there's a bug in the code used to send the transaction request, the related Bitcoins could be lost forever. Keep in mind that these networks are decentralized - there's no intermediary, no customer support, and no one who can help you recover a lost transaction or a forgotten wallet password.

For that reason, if you're interested in trading on the Bitcoin network, you should store your wallet password or private key very carefully and securely.



(Source: Author's illustration of digital signature verification in blockchain)

Figure 6. Transaction Verification Mechanism Using Digital Signatures and Encryption Keys

Note. Redeemed Input:

A “redeemed input” refers to a transaction input that has already been used in a new Bitcoin transaction. In the Bitcoin system, each transaction consumes one or more unused outputs (from previous transactions). When a Bitcoin is used as an input in a new transaction, it's said to be "redeemed" or "spent".

Example:

Imagine you possess 1 Bitcoin from an earlier transaction. When you send that 1 Bitcoin to someone else:

- (1) The new transaction redeems (uses) that previous Bitcoin as its input.
- (2) Once confirmed, that Bitcoin is no longer available - it has become a redeemed input.

Why redeemed inputs are important:

They help ensure the integrity of the transaction system by preventing the same Bitcoin from being used more than once (i.e., avoiding double spending). This concept is fundamental to transaction verification and maintaining the immutability of the blockchain.

3.3.2.5 Fifth Component - The origin of the term blockchain

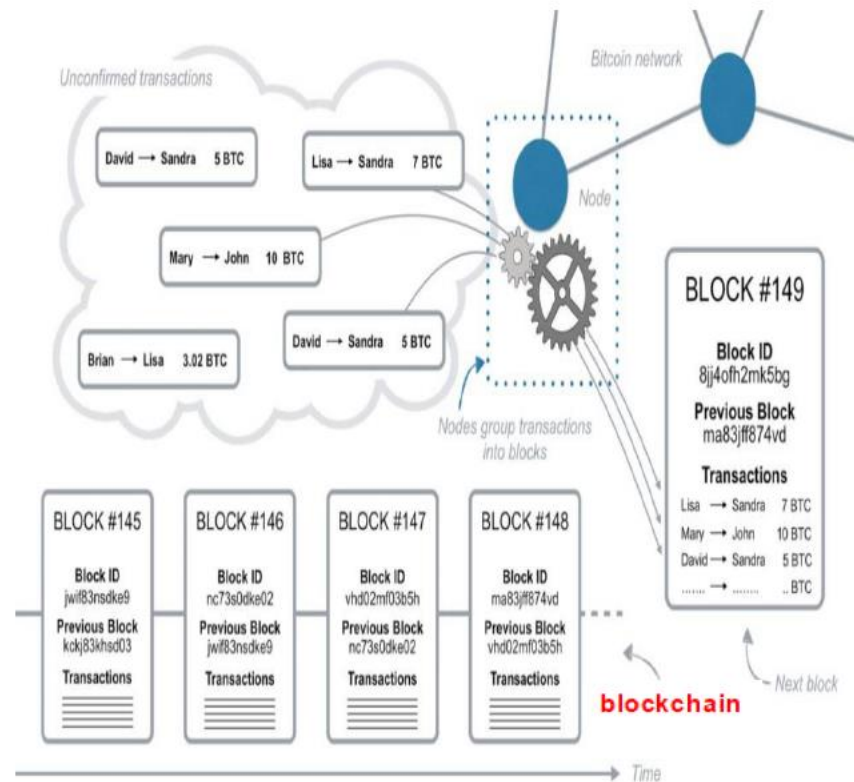
Anyone can access the Bitcoin network through anonymous connections and send or receive transactions using their public key information. However, if someone uses the same public key multiple times, it's possible to aggregate all those transactions under one owner. The Bitcoin network allows users to create unlimited wallets, each with its own private and public key pair. This enables users to receive payments on different wallets without linking them. There's no way to know a person owns all these different keys unless they consolidate their holdings into a single wallet. With up to 2^{160} possible addresses, this high number protects the network from attacks while giving users complete anonymity.

A Security Vulnerability

Despite this system, a major security flaw could be exploited to recover Bitcoin after it's been sent. Transactions are distributed across network nodes - each node might receive them in a different order. An attacker could send a transaction, wait for the partner to respond with goods, then send a reverse transaction back to themselves. Some nodes may accept the second transaction first, invalidating the original payment. Since timestamps can be forged, there's no reliable way to determine which transaction came first, opening the door for fraud and inconsistencies across the network.

Blockchain's Solution

To resolve this, the blockchain system was designed to ensure transaction consensus and prevent fraudulent behaviors. It groups pending transactions into blocks and links them sequentially to form a chain - hence the name “blockchain.” Each block stores a set of transactions and a reference to the previous one, creating an immutable and time-based chain of trust.



(Source: Author's original diagram based on blockchain formation principles)

Figure 7. The process of blockchain formation in the bitcoin network

In summary, the term “Blockchain” accurately reflects the essence of the system: a chain of data blocks linked by cryptographic algorithms, validated by the network community, and resistant to manipulation. This technical foundation establishes trust in a decentralized environment, where transactions are safeguarded by processes rather than by human actors. These technical features not only construct digital trust in general but also directly transform the way banks perform their intermediary role.

From all the above analyses, it is clear that Blockchain has created an entirely new trust mechanism - transparent, immutable, and independent of intermediaries. In the past, banks played a central role in verifying and certifying transactions, whereas today consensus algorithms, cryptographic mechanisms, and distributed ledgers have taken on that function. This raises an important question: when trust has been “encoded” into the system, how does Blockchain technology transform the traditional role of banks?

4. Blockchain Technology and the Reshaping of Central Bank Functions in Currency Issuance and Circulation

4.1. Blockchain and Fundamental Changes in Currency Issuance

Blockchain technology has opened up the possibility for central banks to issue digital currencies CBDC, partially or fully replacing the role of traditional paper money. Whereas currency issuance in the past was tied to printing, circulation control, and physical management, Blockchain now enables issuance in the form of digital tokens with absolute transparency, traceability, and protection against counterfeiting (BIS,

2021). This not only reduces operating costs but also enhances the efficiency of money supply management, while limiting risks related to counterfeit currency and losses in circulation.

4.2. Reshaping the Function of Currency Circulation

Within the Blockchain ecosystem, currency no longer circulates through commercial banks in the traditional manner but can instead be transferred directly between parties via smart contracts and digital wallets. The central bank will act as the architect of digital infrastructure, ensuring that all transactions are recorded on the distributed ledger, thereby reducing intermediary costs and accelerating payment speed (European Central Bank, 2022). This means that the central bank's function of "coordinating currency circulation" will shift from managing physical cash to supervising digital data flows, where every transaction can be tracked in real time.

4.3. Forecasting Future Changes

In the digital economy, the functions of currency issuance and circulation by central banks will undergo specific transformations:

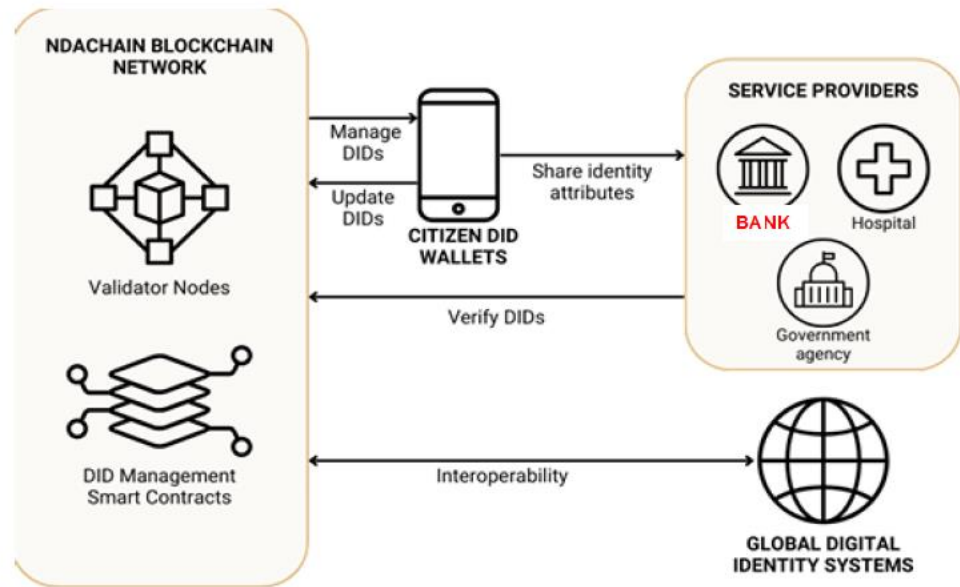
- **Decline of paper money's dominant role:** It is projected that within the next 10 to 20 years, the share of paper money in total payment instruments will decrease significantly, serving mainly as a backup or for populations without access to digital infrastructure (IMF, 2023).

- **CBDC as the primary instrument:** Central banks will focus on issuing and managing CBDCs, positioning them as the standard means of payment in the digital economy.

- **Supervision replacing physical management:** Instead of managing the volume of circulating paper money, central banks will monitor transaction data on Blockchain.

- **Integration with the digital ecosystem:** CBDCs will directly connect with fintech platforms, e-commerce, and public services, creating a comprehensive, transparent, and efficient payment ecosystem. blockchain, adjusting monetary policy in real time.

To illustrate this transformation, we can refer to the model that introduces the position of the banking system within the NDACHain Blockchain ecosystem.



(Source: NDAchain White Paper)

Figure 8. The Position of Banks in the NDAchain Blockchain Ecosystem

According to this model, the banking system of the future will serve as the central coordinator of data and trust across the entire ecosystem. Commercial banks, fintech enterprises, and users all connect directly to Blockchain, with the central bank acting as the guarantor, ensuring the legality and stability of digital currency. This demonstrates a shift from the model of “central bank issuance – commercial bank distribution” to the model of “central bank issuance and direct supervision on Blockchain,” in line with the global digitalization trend.

5. Conclusion and Policy Recommendations

The development of Blockchain technology marks a critical turning point in reshaping the functions of currency issuance and circulation by central banks. With its transparency, security, and decentralization, Blockchain not only reduces operating costs and enhances management efficiency but also establishes a “digital trust” that replaces traditional trust based on intermediaries. The emergence of CBDCs is clear evidence of this trend, while simultaneously creating an urgent need to redefine the role of central banks in the digital economy.

However, opportunities come with challenges. The application of Blockchain and CBDCs requires clear legal frameworks, robust security mechanisms, and communication strategies to strengthen social acceptance. Without adequate preparation, risks such as cybersecurity threats, fraud, and loss of public trust could undermine the financial system.

Policy Recommendations:

- Develop flexible legal frameworks: Issue clear regulations on the issuance and management of CBDCs, while ensuring compatibility with the international financial system.

- Strengthen cybersecurity: Invest in secure infrastructure, monitoring mechanisms, and risk prevention to protect the national Blockchain system.
- Promote experimentation and pilot programs: Apply sandbox models to test Blockchain applications in controlled environments before scaling up.
- Enhance public awareness: Organize communication campaigns and public education programs on the benefits and risks of digital currency to reinforce trust.
- Foster international cooperation: Participate in global forums on CBDCs and Blockchain to learn from experiences and ensure interoperability in cross-border transactions.

In summary, Blockchain is not merely a supporting technology but a driving force for fundamental transformation in the functions of central banks. If implemented in the right direction, it will help strengthen public trust, improve monetary management efficiency, and foster innovation in the modern economy.

References

- Allen, F., Gu, X., & Jagtiani, J. (2020). Fintech, bigtech, and the future of banks. *Journal of Financial Intermediation*, 41, 100310.
- Antonopoulos, A. M. (2017). *Mastering bitcoin: Programming the open blockchain* (2nd ed.). O'Reilly Media.
- Arner, D. W., Barberis, J., & Buckley, R. P. (2017). FinTech, RegTech, and the reconceptualization of financial regulation. *Northwestern Journal of International Law & Business*, 37(3), 371–414.
- Auer, R., & Böhme, R. (2020). The technology of retail central bank digital currency. *BIS Quarterly Review*, March, 85–100.
- Auer, R., Cornelli, G., & Frost, J. (2023/2024). *Rise of the Central Bank Digital Currencies. International Journal of Central Banking*, Vol. 19, No. 4, pp. 185–214.
- Bank for International Settlements. (2018). *Central bank digital currencies*. BIS.
- Bank for International Settlements (2025). *Advancing in Tandem – Results of the 2024 BIS Survey on Central Bank Digital Currencies and Crypto*. BIS Papers No. 159.
- Brunnermeier, M., James, H., & Landau, J. (2019). *The digitalization of money*. Princeton University.
- Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. *Journal of Economic Perspectives*, 29(2), 213–238.
- Casey, M., & Vigna, P. (2018). *The truth machine: The blockchain and the future of everything*. St. Martin's Press.
- Catalini, C., & Gans, J. (2020). *Economics of blockchain*. MIT Sloan Research Paper.
- Cong, L. W., & He, Z. (2019). Blockchain disruption and smart contracts. *Review of Financial Studies*, 32(5), 1754–1797.
- European Central Bank. (2021). *Report on a digital euro*. ECB.
- Gans, J. (2019). *The case for an electronic currency*. MIT Press.
- Giang, T., Lan, H., & Hanh, N. (2025). Controlling Transfer Pricing Activities in Vietnam through the Application of Blockchain Technology. In *Proceedings of AGBA International Conference 2025*.
- Harvey, C. R., Ramachandran, A., & Santoro, J. (2021). DeFi and the future of finance. Duke University Working Paper.
- International Monetary Fund (2024). *Central Bank Digital Currency: Progress and Further Considerations*. IMF Policy Papers, Volume 2024, Issue 052.
- International Monetary Fund. (2019). *The rise of digital money*. IMF.
- Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton University Press.
- Pilkington, M. (2016). Blockchain technology: Principles and applications. In O. Olleros & M. Zhegu (Eds.), *Research handbook on digital transformations* (pp. 225–253). Edward Elgar.
- Schär, F. (2021). Decentralized finance: On blockchain- and smart contract-based financial markets. *Federal Reserve Bank of St. Louis Review*, 103(2), 153–174.
- Swan, M. (2015). *Blockchain: Blueprint for a new economy*. O'Reilly Media.

- Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world*. Penguin.
- Yermack, D. (2017). Corporate governance and blockchains. *Review of Finance*, 21(1), 7–31.