IPRPD
International Journal of Business & Management Studies
ISSN 2694-1430 (Print), 2694-1449 (Online)
Volume 06; Issue no 03: March, 2025
DOI: 10.56734/ijbms.v6n3a3

ASSESSING THE TECHNICAL AND ECONOMIC RESILIENCE OF BITCOIN ECOSYSTEM

Guych Nuryyev, Ph.D.[1]

[1]*I-Shou University, Taiwan*

Abstract

This paper examines the resilience of Bitcoin's architecture, highlighting its cryptographic security, decentralized structure, and economic principles. By tracing a transaction's journey from the mempool to confirmation on the blockchain, the study reveals how Bitcoin maintains reliability in a trustless environment. The principle of "hard money" is enabled by algorithmic cap on Bitcoin's supply. The Cantillon effect is avoided by distributing new supply via a cryptographic lottery. The decentralized network eliminates single points of failure, while the use of double-entry accounts enhances transparency and mitigates fraud risks. These features collectively make Bitcoin a robust digital currency, despite its price volatility.

Keywords

Bitcoin, Blockchain, Transactions, Decentralized Finance

I. Introduction

Satoshi Nakamoto created an algorithm that allows bitcoin to be created in declining amounts over time, with a cap on total coins to be created (Nakamoto, 2008). Despite lack of traditional backing, Bitcoin has gained prominence as a decentralized digital currency and a potential store of value, with the price recently peaking at over $108,000. This prominence stems largely from its innovative architecture, which ensures both security and resilience in a decentralized environment. Bitcoin operates without a central authority, relying instead on a distributed ledger, cryptographic principles, and a consensus mechanism to maintain its integrity and functionality.

This paper investigates what makes Bitcoin's architecture resilient, by exploring the fundamentals of Bitcoin's operations. First, we describe the basics of a Bitcoin transaction, the fundamental unit of analysis. Second, we follow a hypothetical transaction, tracking its journey from exchange to mempool to blockchain. Third, we examine the mechanisms that protect Bitcoin against security risks and potential attacks. Finally, we speculate on its future as a digital currency and its implications for global finance.

II. A Bitcoin Transaction

A. The role of algorithm in transaction security

Bitcoin transactions form the core of its ecosystem, allowing users to exchange value directly without intermediaries. Unlike traditional systems, Bitcoin relies on a decentralized network of nodes to validate the transactions, ensuring trust through cryptographic mechanisms rather than centralized oversight.

Nakamoto's algorithm creates bitcoins, on average, every ten minutes, with a cap on the total number of coins to be created. Figure 1 shows bitcoin supply since its creation, and out to 2064. Annual growth is logarithmic, decreasing to around 320 bitcoins per year by 2060. This algorithm ensures a finite supply of about 21 million bitcoins to be created by the year 2140.

The supply limit of 21 million bitcoins is supported by a consensus of node operators and hundreds of bitcoin developers dispersed around the world. As the bitcoin code is open source, anyone can submit bitcoin improvement proposals (BIPs), which would be peer-reviewed by the developers.[1] Peer-review ensures that the proposed changes maintain the integrity of the protocol and align with its principles of hard money and robust security.

[1] Bitcoin rarely has significant changes like introducing hierarchical deterministic wallets with BIP32 (Wuille, 2012).

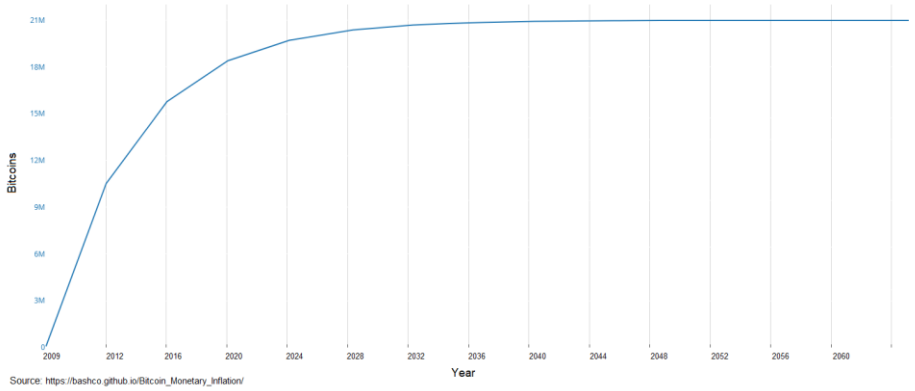

Figure 1. Bitcoin Supply Over Time

To participate in the Bitcoin ecosystem, users need an electronic wallet to store private keys securely, which are essential for authorizing transactions. Private keys, which must remain confidential, generate digital signatures that prove ownership and enable secure transfers. Wallet types vary, from beginner-friendly platforms (e.g. Coinbase) to specialized hardware wallets (e.g. Trezor Safe 3). The diversity of wallets balances convenience and security.

B. The mempool's role in the transaction

An exchange involving bitcoin is similar to an ordinary exchange involving cash. For example, suppose David agrees to sell Garry an article of furniture, for which Garry agrees to pay one bitcoin. Once Garry presses "Send," his wallet broadcasts the transaction to the nodes to which it is connected, which in turn broadcast the information to all nodes to which they are connected. Each node is usually connected to around half-a-dozen nodes. While there are over 16,000 nodes on the bitcoin network, within seconds all nodes are aware of the unconfirmed transaction.[2] The decentralized nature of the network ensures that the transaction reaches all connected nodes, enhancing the system's resilience against single points of failure.

The nodes are networking software running on thousands of computers. When a transaction is received, each node records the transaction in memory (RAM). That memory is called the "mempool," the pool of all transactions that have not yet been recorded to the blockchain: transactions in the mempool are "unconfirmed." The mempool is public: anyone can run a node. This decentralized replication across nodes prevents bottlenecks and maintains continuity even in cases of network delays or disruptions. Wallets also ask connected nodes if there are unconfirmed transactions for the addresses in the wallet. For example, when Garry sends David a bitcoin, David's wallet shows an unconfirmed incoming bitcoin from Garry.

The mempool is thus the universe of unconfirmed transactions, copied across all nodes. In the short-term, mempools might differ slightly across nodes due to internet speeds. For example, if someone sent a transaction from a wallet connected to a node in Japan, which forwards the information to a node in Taiwan and to a node in Argentina, the node in Taiwan might get the information first.

Figure 2 below shows the number of transactions in the mempool for April of 2022. On average, there are approximately 2,000 transactions in the pool, though with considerable variation and regularity.

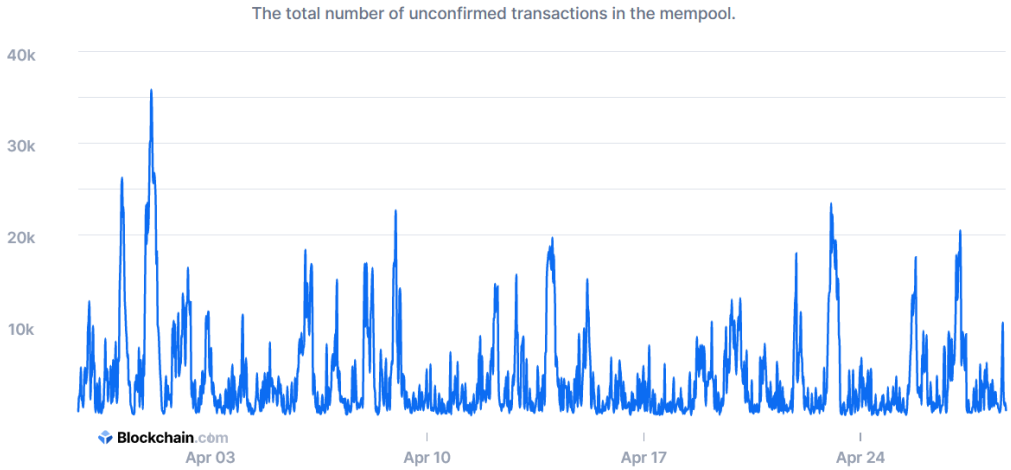

Figure 2. Transactions in the Mempool

[2] https://bitnodes.io/

Figure 3 shows the history of the mempool size that resides on each bitcoin node. It is typically under 30 MB, though there have been some significant spikes, such as around December of 2018 and the first half of 2021.

The largest that the mempool has been was around 140 Mb. Size tends to expand when the bitcoin price spikes. For example, from January to December 2017, the bitcoin price increased from $1,000 to $20,000 and the mempool went from under 5 Mb to 140 Mb. From January 2018 to December 2018, the bitcoin price then dropped to $3,000 and the mempool decreased to under 5 Mb. By mid-2019, the bitcoin price increased to $13,000 and the mempool increased to over 40 Mb.

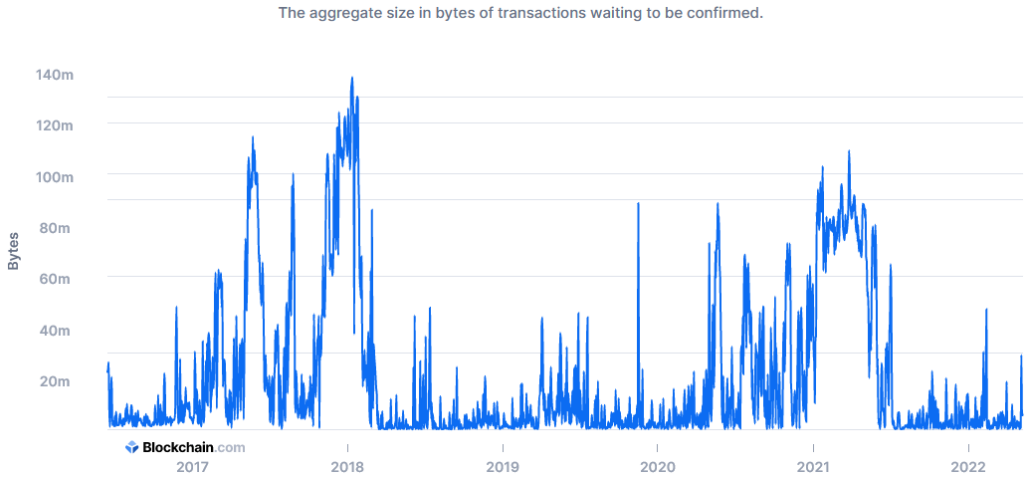

Figure 3. Mempool Size

III. From Mempool to the Blockchain

A. What is the blockchain?

The blockchain is the cumulative record of all confirmed bitcoin transactions. The mempool itself is not part of the blockchain. It is, instead, part of the raw ingredients used by miners to confirm transactions which then go into the blockchain. Figure 4 shows that there are between around 200,000 and 300,000 transactions added to the bitcoin blockchain per day. The cyclicality is due to the number of transactions dropping significantly over the weekend.

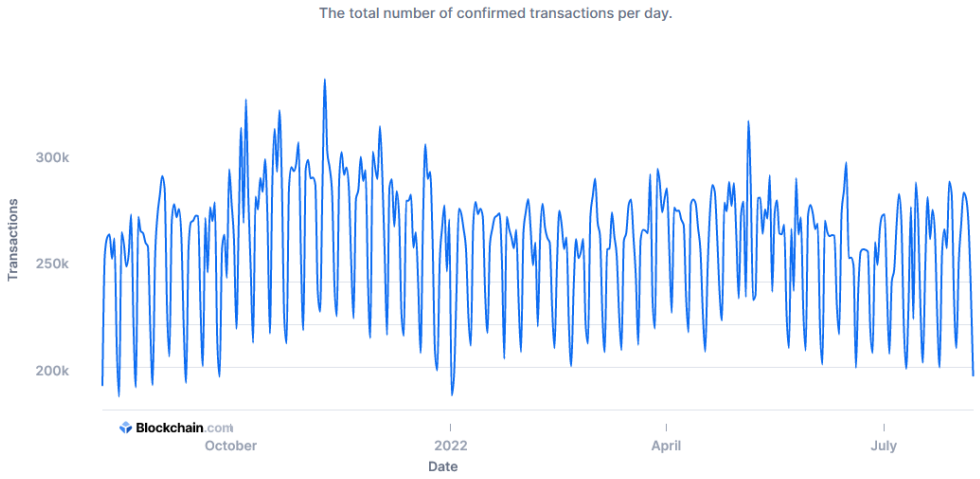

Figure 4. Bitcoin Transactions Per Day

B. What do the miners do?

The injections of unconfirmed transactions represent the supply to the mempool. The demand side, in a sense, is derived from bitcoin "miners." Miners play the central role, "confirming" a set of transactions and adding them into new blocks on the blockchain; miners also compete for this privileged by solving puzzles.

The sender chooses the transaction fee. For our example, Garry offers one coin to David. When sending the transaction to the mempool, Garry chooses the transaction fee, an offering of coins to the miners for putting the transaction into a new block. The higher the transaction fee, more likely the transaction is to be picked up. If the fee is too low, the transaction might sit in mempool for hours or days, though there are ways to deal such stuck transaction.

Miners start by picking unconfirmed transactions from the mempool to form a potential new block in the blockchain. Block size is limited to 2 MB, about 1,000 – 5,000 transactions (Haqshanas, 2023), as transactions vary by size (depending on type and number of addresses involved). This gives miners an incentive to maximize fees per byte. Each miner forms a potential block from the mempool transactions. Only one miners, however, earns the fees from the transactions in the block and newly created bitcoins – the block reward. The winner is decided with a puzzle, which involves the following.

A typical miner forms a potential block, the first transaction reflects the newly created bitcoins to be paid to himself, and the miner selects the remaining transactions (up to the block capacity) from the mempool. Then the miner hashes all the information in the block to get the block hash. A hash function is a one-way function that scrambles data of various sizes into an output of uniform size. Bitcoin uses a hash function that produces a 256 bit output. The puzzle to solve is getting a block hash (unpredictable because the hash is a one-way function) that satisfies the requirement of a given number of zeros in the beginning of the 256 bit output. For example, suppose that the requirement is eight leading zeros, and the first hashing gives the output 0011010010…. This fails, as it has only two leading zeros. In that case, the miner needs to change some information in the block and hash again.

The information that the miners change in the block is a meaningless number called "nonce." Miners change the nonce with each hashing until a required hash is found. This process, known as proof-of-work, requires substantial computational effort (Gkristi, 2023). Once a miner finds the required hash, it broadcasts the new block to other nodes. All miners are nodes, but not all nodes are miners. Each node validates the block by verifying all requirements, such as hashes, signatures, correct block rewards size, *etc*. If the block is valid, it is accepted as the next block in the blockchain, and the transactions it contains achieve finality.

C. Hard money lottery

As noted, the first miner to solve the puzzle gets the block reward and all the fees from the transactions in the block, which becomes the latest link in the blockchain.[3] The mempool is then updated ensuring that only unconfirmed transactions remain. The entire process of racing to create a new block usually takes about ten minutes. As hashing creates unpredictable hash outputs, the process can take more or less time. The expected time

also decreases with the number of miners (total computing power), as the chance of a correct hash per minute increases. Every 2,016 blocks (about two weeks' time) the difficulty (required leading zeros in the block hash) is adjusted by the bitcoin software. Difficulty is increased (decreased) if the average new block took less (more) than ten minutes in the last two weeks (Kohler, 2022).

This difficulty adjustment keeps the growth of bitcoin supply predictable regardless of the number of miners. Over time, block rewards diminish, a feature that ensures bitcoin scarcity and aligns with the principles of "hard money." As Figure 1 above shows, bitcoin supply growth diminishes over time. This is achieved by reducing the block reward by half every 210,000 blocks (about four years) (BitcoinBlockHalf, n.d.).

The puzzle is used to distribute newly created bitcoins randomly to the miners who perform the service of confirming transactions, and maintaining the blockchain's permanent, incorruptible history. Conceptually, the distribution of new bitcoins is similar to a lottery-based monetary expansion à la Jordan (1989). In traditional monetary policy, newly-created money is first distributed to bankers. Early receivers of new money benefit more than late receivers (Cantillon effect) (Adam Smith Institute, 2019). By the time the money trickles down to late receivers, prices have increased.

D. Where are the bitcoins?

Bitcoins do not exist in a wallet. They exist, instead, on the blockchain recorded in the confirmed transactions. To spend coins one needs to supply the matching digital signature for the given address. Wallets themselves only hold a list of private keys that can create a digital signature. The matching addresses can be derived from a key. So a wallet is technically a key ring with lots of keys. Anyone can randomly check any 256-bit number as a key, check if the corresponding address has funds, and steal the bitcoins. The obstacle to a successful random search is the vastness of the search space: 2^{256} exceeds the number of atoms in the observable universe (Villanueva, 2009).

IV. The Bitcoin Blockchain

The blockchain itself is an open ledger containing the record of every bitcoin transaction since the first one. Transaction records are lines in a double-entry bookkeeping ledger. A simple transaction contains the transaction ID, inputs, outputs, and transaction fee. On the left hand side, the transaction contains the input(s), which are like debits from an address. On the right hand side, the transaction contains the output(s), which are like credits to an

[3] Sometimes two blocks are simultaneously created and the chain splits. As the blockchain is bitcoin's history, a chain split resembles two timelines co-existing temporarily, until the winner of the next block. All nodes switch to the timeline of the next winner (winning timeline is the one to produce the next block first).

address. The total value of inputs is no less than total value of outputs, with the difference between them being the transaction fee (chapter 5 in Antonopoulos, 2015).

This design ensures transparency and auditability while reducing the risks of fraud or tampering, contributing to the overall resilience of Bitcoin's architecture. Each transaction leaves a verifiable trail, which, when recorded on a decentralized blockchain, strengthens its security.

Figure 5 illustrates three transactions. (1) The top panel shows Garry receiving 0.1 bitcoins from Joe. Joe paid 0.1005, implying a 0.0005 transaction fee. Joe's wallet picked one of the previously received outputs as the input for this transaction. Multiple previously received outputs can be picked for a larger transfer. (2) Garry used the output received in the first transaction as an input in the second transaction to pay 0.015 bitcoins to David (with 0.0005 transaction fee), and 0.085 back to Garry's address as change. The fee is chosen by the sender, and could be zero. (3) David used the output received in the second transaction as an input in the third transaction to pay 0.01 bitcoins to Gopesh (with 0.0005 transaction fee), and 0.0045 back to David's address as change.

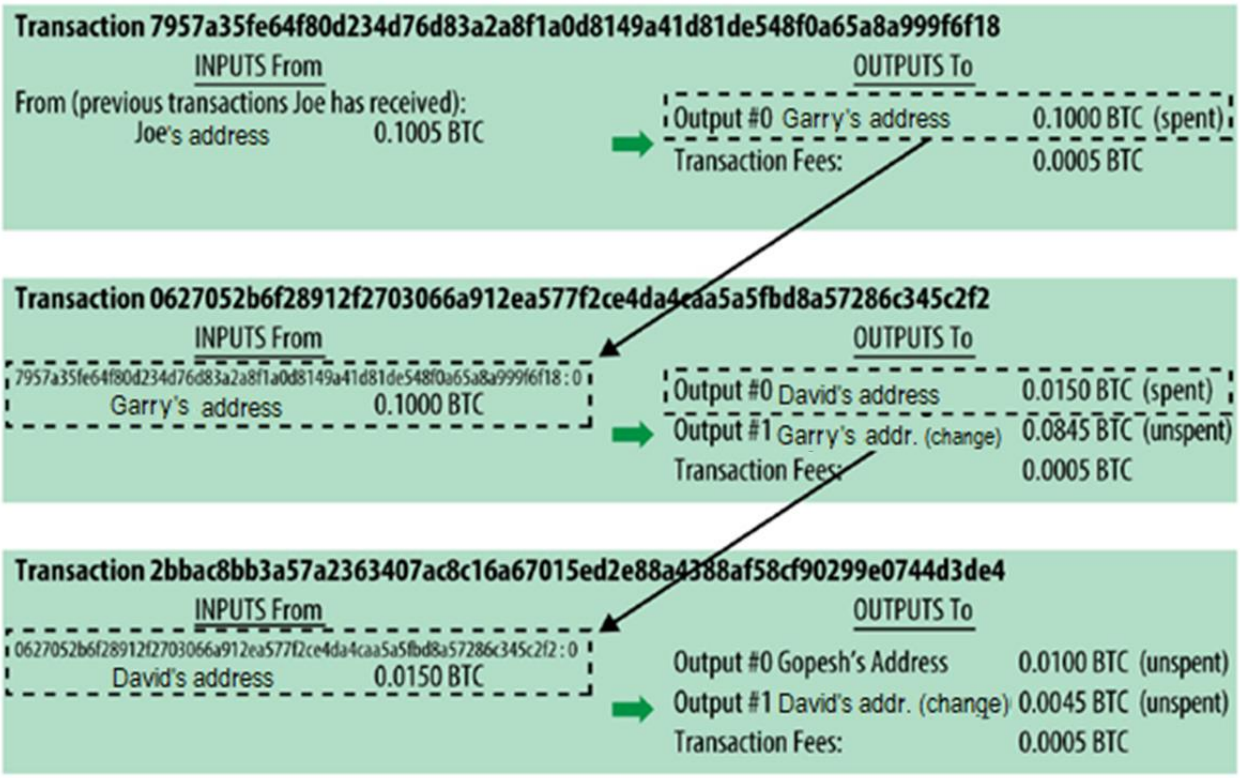

Figure 5. Bitcoin Transactions as Double-Entry Bookkeeping.

As can be seen, the blockchain doesn't explicitly sum up the balance for an address. The balances are implied by all the transactions on the blockchain back to the first bitcoin. The implied balance is calculated and shown by the wallet of each user. Since the blockchain doesn't explicitly sum the balances, instead of explicitly subtracting from the sender's balance transactions refer to previously received outputs to include them as inputs in a new transaction.

This reliance on explicit references to previous transactions reduces ambiguity and ensures integrity. By structuring transactions this way, Bitcoin prevents double-spending and ensures the reliability of the system, even in a trustless environment.

The blockchain parallels the mempool, in that a copy of the entire blockchain resides at each node. The entire blockchain now exceeds 600 Gb on each node.[4] The requirement for every node to store a full copy of the blockchain strengthens resilience by decentralizing data storage and eliminating single points of failure. Even if some nodes are compromised, the network as a whole retains its ability to verify transactions.

V. Conclusion

This paper has illustrated how a combination of cryptographic security, decentralized governance, and economic principles contribute to Bitcoin's resilience. By examining the journey of a transaction, from its inclusion in the mempool to its final confirmation on the blockchain, this paper has demonstrated how Bitcoin's architecture

[4] https://www.blockchain.com/explorer/charts/blocks-size.

ensures reliability even in a trustless environment.

The algorithmic cap on its supply creates predictability and scarcity, foundational to its value as "hard money." The predictability is maintained even with growing mining efforts over time. The Cantillon effect is avoided by distributing new bitcoin supply via a cryptographic lottery among the miners.

The decentralized nature of Bitcoin network eliminates single points of failure, which ensures security even under stress. Bitcoin operates without centralized oversight, instead relying on an open and transparent ledger maintained collectively by thousands of globally distributed nodes.

The innovative use of double-entry bookkeeping principles and the immutability of the blockchain provide transparency and reduce risks of fraud. The incentive to use bitcoin in fraudulent transactions is diminished by the fact that transactions on the blockchain might be analyzed anytime in the future.

This combination of cryptographic security and decentralization enable bitcoin to be a resilient digital currency, although with significant price volatility. Bitcoin's architecture offers valuable lessons for the future of decentralized finance and global monetary systems. Future research may further explore how the principles that enable bitcoin's security and transparency in a decentralized framework can be applied to other areas of global finance.

References

1. Adam Smith Institute (2019). The Cantillon effect. Accessed on 31 Aug 2023. https://www.adamsmith.org/blog/the-cantillion-effect
2. Antonopoulos, A. (2015). Mastering bitcoin: unlocking digital cryptocurrencies (1st ed.). *O'Reilly Media*.
3. BitcoinBlockHalf (n.d.). Bitcoin Block Reward Halving Countdown. Accessed on 4 Sep 2023. https://www.bitcoinblockhalf.com/
4. Gkristi, E. (2023, May 30). Bitcoin mining difficulty's record setting streak shows no signs of stopping. Accessed on 9 Aug 2023. https://www.coindesk.com/tech/2023/05/30/bitcoin-mining-difficultys-record-setting-streak-shows-no-signs-of-stopping/
5. Haqshanas, R. (2023). 358k ordinals inscribed on the bitcoin blockchain as average block size surges. *The Tokenist*. Accessed on 9 Aug 2023. https://tokenist.com/358k-ordinals-inscribed-on-the-bitcoin-blockchain-as-average-block-size-surges/
6. Jordan, Jerry L. 1989. "The Future of Price Stability in a Fiat Money World," *Cato Journal*, Cato Institute, vol. 9(2), pages 471-486, Fall.
7. Kohler, C. (2022). What is bitcoin block time? The Bitcoin Manual. Accessed on 4 Sep 2023. https://thebitcoinmanual.com/articles/btc-block-time/
8. Nakamoto, S. (2008). Bitcoin: a peer-to-peer electronic cash system. Accessed on 19 Aug 2022. https://bitcoin.org/bitcoin.pdf
9. Villanueva, J. C. (2009). How many atoms are there in the universe? *Universe Today*. Accessed on 4 Sep 2023. https://www.universetoday.com/36302/atoms-in-the-universe/
10. Wuille, P. (2012). Hierarchical Deterministic Wallets. *GitHub*. Accessed on 9 Aug 2023. https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki