WhiteBitcoin: A Distributed Ledger Framework for Peer-to-Peer Electronic Transactions

Watoshi Nakamoto

watoshi@whitebitcoin.org

www.whitebitcoin.org

Abstract:

WhiteBitcoin (WBTC) is a decentralized, open-source cryptocurrency developed as a purely peer-to-peer form of electronic cash. Launched on **February 14, 2018**, and built on the **Advance Blockchain (ABC20)**, WhiteBitcoin removes the need for financial intermediaries by allowing users to send payments directly from one party to another over the internet.

Drawing foundational influence from both **Bitcoin (BTC)** and **Ethereum (ETH)**, WhiteBitcoin(WBTC) introduces a hybrid blockchain model that enhances scalability, supports smart contract functionality, and expands the scope of decentralized finance (DeFi) applications.

The project was first conceptualized in **2015** by an anonymous group or individual known as **Watoshi Nakamoto**. Its core mission is to redefine value transfer and innovation within the blockchain ecosystem. WhiteBitcoin(WBTC) addresses the **double-spending problem** without requiring a centralized authority by implementing a peer-to-peer network that timestamps transactions. Each transaction is hashed and added to an ongoing chain secured by **proof-of-work**, forming an immutable ledger maintained by the collective computational power of honest nodes.

As long as a majority of computing power is controlled by honest participants, the network remains secure by continually producing the longest chain—a cryptographic proof of the transaction sequence and the work invested. The WhiteBitcoin(WBTC) network is purposefully minimal in structure, allowing nodes to freely join and exit. Transactions are shared on a best-effort basis, and returning nodes always recognize the longest proof-of-work chain as the valid ledger, preserving trust and continuity in a truly decentralized system.

1. Introduction:

Online commerce has long depended on financial institutions to serve as trusted intermediaries for processing electronic payments. While this system has enabled widespread digital transactions, it also comes with significant drawbacks—high fees from dispute mediation, restrictions on microtransactions, and an inherent vulnerability to fraud. These issues largely arise from the reversibility of traditional payment systems, which compel merchants to collect excessive customer data and accept a baseline level of fraudulent activity. While physical cash avoids these problems, it lacks a native digital equivalent that can operate seamlessly over communication networks without centralized oversight.

Bitcoin addressed these shortcomings by introducing a decentralized, trustless system based on cryptographic proof. Its innovative use of a peer-to-peer distributed timestamp server solved the double-spending problem, laying the groundwork for a transparent, censorship-resistant, and secure financial network.

WhiteBitcoin (WBTC) builds upon this foundation, evolving the original Bitcoin model by integrating the programmability and flexibility of next-generation blockchains. It retains Bitcoin's core principles—such as a fixed supply, decentralized mining, and halving mechanics—while introducing powerful new capabilities inspired by platforms like Ethereum. These include smart contracts, decentralized applications (dApps), and tokenized assets.

Built on the Advance Blockchain (ABC20), WhiteBitcoin benefits from a high-performance, scalable infrastructure designed for cross-chain interoperability and advanced use cases. ABC20 supports native tokens, coins, NFTs, and NFCs, enabling a broad range of decentralized applications and digital assets within a single ecosystem.

By fusing the security and trustless nature of Bitcoin with the advanced features of modern blockchain technology, WhiteBitcoin(WBTC) offers a future-ready platform for decentralized finance, digital ownership, and innovation at scale.

2. Transactions in WhiteBitcoin(WBTC):

In the WhiteBitcoin(WBTC) ecosystem, a digital coin functions as a chain of cryptographic signatures, forming an unbroken and verifiable trail of ownership. Each time a coin changes hands, the current owner digitally signs a hash of the previous transaction along with the recipient's public key. This signature becomes part of the coin's history, allowing anyone to verify ownership by tracing the chain of signatures.

Example Ownership Chain:

- **Owner 1's Public Key**
  ← Signed by Owner 0's Private Key → Hashed → Verifiable Transaction
- **Owner 2's Public Key**
  ← Signed by Owner 1's Private Key → Hashed → Verifiable Transaction
- **Owner 3's Public Key**
  ← Signed by Owner 2's Private Key → Hashed → Verifiable Transaction

This cryptographic chaining ensures each coin has a unique and auditable ownership record, preserving integrity without relying on a central authority.

The Double-Spending Problem

A fundamental challenge in digital currency systems is **double spending**—where the same coin is used in more than one transaction. In traditional digital payment models, this issue is mitigated by a centralized authority or "mint" that verifies and clears each transaction. Under

this model, coins must pass through the mint to be reissued, and only newly minted coins are considered valid.

While effective, this approach introduces a **single point of failure**. The system's reliability and security depend entirely on the central mint's trustworthiness and availability—similar to how conventional banks operate.

WhiteBitcoin's Decentralized Solution

WhiteBitcoin addresses this challenge with a **fully decentralized consensus mechanism**. Instead of relying on a central mint, all transactions are broadcast publicly across the network. Nodes work together to validate transactions and maintain a shared, synchronized ledger.

The breakthrough lies in **requiring consensus**: a transaction is only confirmed when the majority of nodes agree on its order and legitimacy. This ensures that only the **first valid transaction** involving a particular coin is accepted, making any later attempts at double spending automatically rejected by the network.

By replacing centralized trust with **distributed verification**, WhiteBitcoin enables secure, transparent, peer-to-peer digital payments—without the need for any central authority.

3. WhiteBitcoin(WBTC) Timestamp Server:

The core of the WhiteBitcoin network (Advance Blockchain) is the timestamp server, ensuring the integrity and immutability of transactions. It provides a verifiable proof of time and order for each data entry.

The timestamp server works by creating a hash of a block of items and publicly publishing it, often through methods like online forums or newspapers. This hash represents a snapshot of the block at a specific time, proving the data existed before that timestamp.

Each new timestamp includes the previous one's hash, forming a linked chain. This continuous chain strengthens the validity of all prior timestamps, creating an unbreakable, auditable, and secure history of data.

As a result, advance blockchain is tamper-proof. Any change to a block requires altering every subsequent block, making tampering computationally impossible. This ensures a transparent, decentralized, and trustless financial system, continuously verifiable by anyone in the network.

4. Proof-of-Work Implementation for WhiteBitcoin(WBTC) :

WhiteBitcoin (WBTC) blockchain relies on a Proof-of-Work (PoW) consensus mechanism to ensure security, decentralization, and the integrity of its distributed ledger. This system

requires miners to solve computationally intensive puzzles, which can be verified by others, ensuring decentralized control over the network. Modeled after the Hashcash system, PoW is adapted for WhiteBitcoin's unique blockchain features.

Proof-of-Work Mechanism

Miners in WhiteBitcoin's system must find a hash of a block that meets a specific condition—typically a hash beginning with a certain number of zero bits. To achieve this, miners alter a value called the nonce until the hash meets the requirement. This process requires significant computational resources and can only be verified by rehashing the block.

Once a block is mined, altering it requires recalculating the proof-of-work for that block and all subsequent blocks, making tampering increasingly difficult as more blocks are added to the blockchain.

Chain Integrity and Majority Decision-Making

PoW helps WhiteBitcoin overcome the challenge of decision-making in a decentralized system. Unlike models that rely on one-IP-address-one-vote, which are vulnerable to manipulation, PoW ties decision-making to computational effort. The longest valid chain in the network, containing the most accumulated proof-of-work, represents the majority decision. Malicious actors attempting to alter the blockchain would need to outpace the honest miners, a task that becomes exponentially harder as the blockchain grows.

Difficulty Adjustment Mechanism

WhiteBitcoin's PoW system includes a difficulty adjustment mechanism to maintain a steady block production rate. As computational power and network participation fluctuate, the difficulty is adjusted to ensure that blocks are mined at a consistent rate. This prevents sudden changes in block creation speed and maintains the blockchain's security.

Summary

In conclusion, WhiteBitcoin’s PoW mechanism secures the blockchain, enables decentralized decision-making, and adapts to changes in computational power. By requiring computational effort to alter the blockchain, WhiteBitcoin ensures its resilience against attacks, with the difficulty of tampering increasing exponentially over time.

5. **WhiteBitcoin(WBTC) Network Overview:**

WhiteBitcoin operates on a decentralized blockchain powered by nodes that validate transactions using a proof-of-work consensus mechanism. Here's a summary of how the network functions:

1. **Broadcasting Transactions**: When a user initiates a transaction, it’s broadcast to all nodes, adding it to the pending transaction pool.
2. **Transaction Aggregation**: Nodes collect transactions from the pool and group them into a block for verification.

3. **Proof-of-Work**: Nodes solve a cryptographic puzzle to add the block to the blockchain. The first to solve it gains the right to do so.
4. **Block Broadcast**: The successfully mined block is broadcast to all nodes for validation.
5. **Block Validation**: Nodes verify the transactions in the block to ensure they follow network rules, such as no double-spending.
6. **Building the Chain**: Validated blocks are linked in a chronological order, with each new block referring to the previous one.
7. **Handling Forks**: If two blocks are broadcast simultaneously, nodes work with the first one received. The longer chain with more proof-of-work becomes the accepted chain.
8. **Resilience**: The network can handle dropped messages and failures, ensuring transactions and blocks are eventually processed, maintaining the blockchain's integrity.

Conclusion
WhiteBitcoin's decentralized system ensures secure, efficient transaction validation, maintaining blockchain integrity even during network disruptions. The proof-of-work consensus and resilient network architecture guarantee reliable operations.

6. Incentive Mechanism:

WhiteBitcoin (WBTC) employs a carefully structured incentive model to uphold the integrity, security, and longevity of its decentralized network. Central to this model is the issuance of block rewards—each newly mined block initiates with a special transaction that generates a new unit of WBTC, directly awarded to the miner who successfully created the block. This mechanism not only compensates miners for their computational efforts but also ensures a decentralized and organic distribution of new coins, eliminating the need for a centralized authority.

Analogous to gold mining—where value is uncovered through physical labor and resource expenditure—WBTC miners expend computing power and electricity to validate transactions and maintain the blockchain's security. This effort-intensive process ensures that new WBTC coins enter circulation gradually and equitably.

In addition to block rewards, miners are incentivized through transaction fees. When a transaction's input value exceeds its output, the remaining balance is claimed by the miner as a fee. As the fixed maximum supply of WhiteBitcoin is gradually approached and the issuance of new coins tapers off, these transaction fees are designed to become the primary incentive for miners. This shift naturally supports a deflationary economic model, promoting long-term value retention and monetary stability.

The incentive framework is also a safeguard against malicious behavior. Any actor seeking to compromise the network must weigh the cost of attempting an attack against the predictable rewards of honest participation. Given the substantial computational resources required for such attacks, rational participants are economically motivated to act in the network's best interest. In this way, WhiteBitcoin's incentive design aligns the interests of individual actors with the health and sustainability of the broader ecosystem.

7. Reclaiming Disk Space in WhiteBitcoin (WBTC):

Efficient storage is vital for blockchain scalability. WhiteBitcoin (WBTC), built on the Advance Blockchain (ABC20), tackles this challenge with innovative pruning techniques and compact block structures.

Merkle Trees for Efficient Storage
WBTC uses Merkle Trees to hash transactions in a compact and verifiable format. Instead of storing every transaction, WBTC only retains the Merkle root in each block header. This allows for secure transaction verification while significantly reducing data size.

Pruning and Compacting Blocks
As transactions age and are no longer needed for verification, they can be safely discarded—leaving only the Merkle root. This process, known as pruning, preserves blockchain integrity while reclaiming disk space.

Minimal Storage Impact
With only 80 bytes per block header and blocks generated every 10 minutes, WBTC's annual storage need is about 4.2 MB. This remains well within modern hardware capabilities, even as the network grows.

Scalable by Design
Thanks to pruning and smart data handling, WBTC is built to scale. It minimizes storage bloat while maintaining decentralization, security, and performance—ensuring long-term sustainability.

8. Simplified Payment Verification (SPV) in WhiteBitcoin:

WhiteBitcoin (WBTC) supports Simplified Payment Verification (SPV), allowing users to confirm transactions without running a full node. This lightweight method improves speed and accessibility while keeping the system decentralized.

SPV works by using only block headers from the longest Proof-of-Work chain. Users query full nodes to find the valid chain, then request a Merkle branch—an efficient cryptographic proof that links their transaction to a block.

Although SPV clients can't verify the full transaction details, they trust that full nodes have already confirmed it. More blocks added on top further strengthen the transaction's validity.

To protect SPV users from potential attacks, WhiteBitcoin includes an optional alert system. Full nodes can notify SPV wallets of suspicious activity, prompting them to download full blocks for deeper verification.

For maximum security, especially in high-volume or business use, running a full WhiteBitcoin node is still recommended.

SPV offers a smart balance—fast, lightweight verification for everyday users, with options for stronger validation when needed.

9. Value Aggregation and Distribution:

WhiteBitcoin (WBTC) is designed for flexible and efficient value management. Instead of fixed or single-use transaction models, WBTC supports seamless splitting and merging of digital value—ideal for both microtransactions and large transfers.

Each transaction can have multiple inputs and outputs, allowing users to combine small amounts into a larger payment or divide a large amount among multiple recipients. Typically, transactions include one or more inputs and two outputs: one for the recipient and one for the sender's change.

This design improves usability, supports transaction chaining without slowing the network, and avoids the need to reconstruct full transaction histories. WBTC's structure makes it scalable and efficient for everyday use and high-volume transfers alike.

10. Development and Launch Timeline:

2015: Conceptualization and development of WhiteBitcoin(WBTC) by WhiteBitcoin Org / Watoshi Nakamoto.

February 14, 2018: Official launch via Initial Coin Offering (ICO).

June 22, 2018: Listed on exchanges; distribution begins.

June 2018 to June 2026: Token distribution via VIP Wallet, an affiliate marketing mechanism.

Post-June 2026: Advance Blockchain becomes fully public and open to developers for creating native coin, native tokens, NFTs, and NFCs.

11. Advance Blockchain (ABC20):

ABC20 is a modular blockchain architecture supporting:

- High-performance consensus algorithm.
- Native support for Coin, Token, NFTs, NFCs, and smart contracts.
- Interoperability with other blockchains, including Bitcoin and Ethereum.
- Secure and scalable dApp environment.
- Community-driven governance and developer access.

12. Coinomics:

- **Coin Name**: WhiteBitcoin (WBTC)
- **Blockchain**: Advance Blockchain (ABC20)

- **Initial Maximum Supply**: 84,000,000 WBTC
- **Post-Burn Maximum Supply (After FEB 2026)**: 21,000,000 WBTC
- **Burn Mechanism**: 75% of supply burned to increase scarcity and value.
- **Utility**:
    - Asset storage and investment vehicle
    - Gas fees on ABC20 network
    - Cross-chain transactions (e.g., with Bitcoin)
    - Governance and staking in ABC20 ecosystem

13. Mining and Distribution:

WhiteBitcoin follows a deflationary mining schedule similar to Bitcoin but adapted to its unique lifecycle. The halving mechanism ensures decreasing supply over time, preserving long-term value.

Mining Rewards and Schedule

Period	Block Reward (WBTC)	Daily Reward (WBTC)
Jun 2018 - Jun 2022	38.6655608	5567.84075
Jun 2022 - Jun 2026	19.3327804	2783.92038
Jun 2026 - Jun 2030	9.6663902	1391.96019
Jun 2030 - Jun 2034	4.8331951	695.980095
Jun 2034 - Jun 2038	~2.4165975	~347.990047
Final Mining Block	< 1 WBTC	Final fractional unit in Jun 2038

Note: These figures are based on a 10-minute block interval.

14. Ecosystem Expansion:

From June 2026 onward, the Advance Blockchain (ABC20) transitions into an open development environment where:

- Any developer or organization can launch native tokens or coins.
- NFT and NFC minting becomes accessible via smart contracts.
- Interoperable blockchain ecosystems can be built on top of ABC20.
- New sectors like supply chain, healthcare, metaverse, and AI can integrate blockchain components using ABC20's infrastructure.

15. Innovation:

WhiteBitcoin and ABC20 introduce groundbreaking capabilities:

- **Native Coin (Mineable Coin and Burnable Coin)**: Designed as a **mineable** and **burnable** coin, ABC20 combines decentralized security with controlled supply mechanics to create a sustainable digital currency ecosystem.
- **Native Token (Token and Burnable Token):** A distinctive fusion of native token functionality and burnable features, crafted to represent monetary value while

enabling identity verification, certification, and the recording of unique ownership.
- **Non-Fungible Coin (NFC)**: A unique blend of NFC with monetary properties, designed for identity, certification, and unique ownership records.
- **Non-Fungible Token (NFT)**: A distinctive integration of NFT technology with monetary features, tailored for identity verification, certification, and the secure recording of unique ownership.
- **Cross-Chain Bridging**: Direct interaction with Bitcoin and Ethereum.
- **Decentralized Governance**: Voting rights for WBTC holders in future upgrades and protocol decisions.
- **Asset-Backed Tokenization**: Real-world asset representation on-chain.

16. Motivation:

WhiteBitcoin emerged with a mission to combine the best aspects of the leading blockchain platforms while solving their limitations. Its creation was motivated by:

- The immutability and value preservation of Bitcoin.
- The programmable financial logic of Ethereum.

Through VIP Wallet distribution, community-driven mining, and a visionary roadmap, WhiteBitcoin seeks to build an ecosystem where blockchain is accessible, scalable, and revolutionary. Its reduced supply, halving model, and open-access future ensure a lasting economic model supporting both scarcity and innovation.

17. Privacy and Anonymity in WhiteBitcoin(WBTC):

Privacy remains a cornerstone of WhiteBitcoin's vision for a decentralized, trustless economy. While traditional banking systems rely on restricted access and trusted intermediaries to maintain user confidentiality, blockchain-based systems must adopt fundamentally different approaches to achieve privacy—ones that are compatible with transparency and decentralization.

WhiteBitcoin departs from conventional privacy models by embracing *pseudonymity*. Every user interacts with the WhiteBitcoin network through cryptographic public keys rather than personal identifiers. Transactions are publicly recorded on the Advance Blockchain (ABC20), allowing anyone to view the amount, timestamp, and wallet addresses involved. However, the identity behind each address remains undisclosed—no names, no centralized registries, no institutions involved.

This is similar to how financial markets disclose trade volumes and times without revealing the identities of buyers and sellers. In WhiteBitcoin, the transaction "tape" is open for analysis, yet no direct connection is made between public addresses and real-world identities.

To enhance unlinkability and reduce traceability, WhiteBitcoin encourages the use of a new key pair for every transaction. This practice, often referred to as **key rotation**, ensures that transactions cannot easily be linked back to a single wallet or user. While certain types of

transactions—like multi-input transactions—may expose common ownership of inputs, the system is designed to minimize the aggregation of personal data.

Despite these safeguards, it's important to acknowledge that absolute anonymity cannot be guaranteed solely through public key obfuscation. To mitigate linkage risks further, users are encouraged to adopt best practices in address management, avoid address reuse, and consider complementary privacy solutions that integrate with WhiteBitcoin, such as mixers or second-layer protocols.

Privacy Model Evolution:

Model	Identities	Transactions	Visibility
Traditional Finance	Known	Private	Third Party Controlled
WhiteBitcoin (WBTC)	Pseudonymous	Public	Decentralized & Transparent

In this new paradigm, privacy is not sacrificed—it is transformed. Ownership becomes masked through cryptographic methods, and transparency empowers the network without exposing the individuals behind it.

Absolutely! Here's a **fresh, short, and simplified rewrite** of the **Calculations** section for the WhiteBitcoin (WBTC) white paper, keeping it technically accurate but easy to digest for a wide range of readers:

---

18. Calculations (Simplified):

WhiteBitcoin (WBTC) relies on probability and game theory to stay secure. One key risk is an attacker trying to reverse a recent transaction by secretly mining a competing blockchain.

This scenario is similar to a **coin toss race**:

- **p** = chance an honest node finds the next block
- **q** = chance the attacker does
- If the attacker falls *z* blocks behind, their odds of catching up **drop exponentially** if **p > q**

Probability of Attack Success

If the attacker tries to undo a transaction buried under *z* blocks, the odds of success are:

- **If p ≤ q** → Attacker *will* catch up eventually
- **If p > q** → Probability = **(q/p)^z**

To be more accurate, we use a **Poisson model** to estimate how much progress the attacker makes over time, and calculate the total success chance.

Here's a snippet of the code used to compute it:

```
double AttackerSuccessProbability(double q, int z) {
    double p = 1.0 - q;
    double lambda = z * (q / p);
    double sum = 1.0;
    for (int k = 0; k <= z; k++) {
        double poisson = exp(-lambda);
        for (int i = 1; i <= k; i++) poisson *= lambda / i;
        sum -= poisson * (1 - pow(q / p, z - k));
    }
    return sum;
}
```

Example: Attack Probability

With 10% hash power (q = 0.1):

Confirmations	Success Chance
0	100%
1	20.5%
3	1.3%
6	0.02%
10	0.0001%

✅The more confirmations, the safer your transaction.
✅The fewer resources an attacker has, the harder the attack becomes.

 Safe Thresholds

Attacker Power	Confirmations Needed (for <0.1% Risk)
10%	5
20%	11
30%	24
40%	89
45%	340

As long as attackers control less than 50% of mining power, **WhiteBitcoin remains secure**.

19. Conclusion

WhiteBitcoin (WBTC) is the result of an evolving vision — a decentralized system for secure, trustless transactions that stands on the shoulders of cryptographic innovation and peer-to-peer consensus. Building upon the foundational idea of digital signatures to ensure ownership, WBTC advances the paradigm by integrating a robust, proof-of-work-based protocol on the Advance Blockchain (ABC20) to prevent double-spending and promote network integrity.

This network is purposefully decentralized and resilient. Nodes operate independently, without needing identification or central coordination, and achieve consensus through computational power. By continuing the legacy of voting with CPU power, WBTC maintains

a dynamic and permissionless environment where consensus is reached through shared economic incentives.

Yet, WBTC is not just a technical solution — it is a vision for the future of digital finance. With a capped supply of 21 million coins, a halving cycle every four years, and compatibility with cross-chain protocols, WhiteBitcoin fuses monetary soundness with modern scalability. It enables the creation and movement of value across ecosystems while ensuring that its core principles — decentralization, transparency, and security — remain intact.

As decentralized economies mature, WhiteBitcoin is positioned not merely as a store of value, but as a programmable foundation for future innovations. Whether powering next-generation financial tools or serving as a bridge across digital platforms, WBTC is built to thrive — not just today, but for decades to come.

References

[1] W. Dai, "b-money," 1998.
[2] H. Massias, X.S. Avila, J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," 1999.
[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," 1991.
[4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," 1993.
[5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," 1997.
[6] A. Back, "Hashcash - a denial of service counter-measure," 2002.
[7] R.C. Merkle, "Protocols for public key cryptosystems," 1980.
[8] W. Feller, "An Introduction to Probability Theory and Its Applications," 1957.