Theoretical Framework for Offline Transactions in Bitnet: Smart Checks, Master Pool, and Payment Networks

Masayoshi Kobayashi
masayoshikob@gmail.com
www.bitnet.money

Abstract. This whitepaper introduces a theoretical framework for enabling offline transactions within the Bitnet blockchain, addressing the critical need for transactional continuity in varied network conditions. At the heart of this framework are Smart Checks, the Master Pool, Payment Networks, and an Arbitrage Panel, each playing a pivotal role in ensuring transactional integrity and resilience. Smart Checks are conceived as encrypted, digital instruments for offline transactions, crafted to be secure, non-fractionable, and transferable solely within the Bitnet ecosystem. The creation, encryption, and storage of these checks are facilitated by specialised software, ensuring the integrity and security of transaction data. The Master Pool functions as a central repository, critical in the movement of funds between online and offline environments. It acts as a protective layer, safeguarding the broader network from potential systemic risks associated with the offline transaction system. Payment Networks, akin to social network groups, enable members to transact in BTN tokens, thereby fostering localised economic communities. These networks function autonomously yet remain seamlessly connected to the Bitnet blockchain, enhancing economic resilience, particularly in scenarios of network disruption. The Arbitrage Panel, composed of stakeholders with a vested interest in the network's integrity, adjudicates transactional disputes. The implementation of an Arbitration Score System incentivises efficiency and fairness in dispute resolution, contributing to the trust and reliability of the network. This innovative framework not only addresses the limitations of internet dependency in digital transactions but also heralds a new era in blockchain technology. It paves the way for adaptable, inclusive blockchain ecosystems, empowering localised, self-sufficient economic networks and securely linking them to the global blockchain infrastructure. The theoretical framework for offline transactions in Bitnet thus signifies a significant stride in enhancing the resilience and adaptability of blockchain technology.

Introduction

The ubiquity of blockchain technology has markedly transformed the landscape of digital transactions, primarily relying on the constancy of internet connectivity. This reliance, however, introduces inherent limitations in scenarios where network access is sporadic or absent. To address this, a novel framework is proposed for the Bitnet blockchain, introducing the capability for offline transactions. This is achieved through the utilisation of mobile device technology and Near Field Communication (NFC).

At the core of this framework are Smart Checks – encrypted, digital representations of transactions. These are uniquely crafted to be secure, non-fractionable, and transferable, solely within the Bitnet ecosystem. The creation, encryption, and storage of these Smart Checks are facilitated via specialised Bitnet software, installed on users' mobile devices. This software serves as the exclusive interface for managing these transactions, ensuring the integrity and security of the encrypted data contained within the Smart Checks.

The implementation of NFC technology is critical in this system, enabling the transfer of Smart Checks between devices, effectively bypassing the need for live internet connectivity. This approach fundamentally enhances the resilience and functional scope of the Bitnet blockchain, offering a robust solution to the challenge of internet dependency in digital finance.

Conceptual Framework

1. Master Pool

The Master Pool operates as a central repository within the Bitnet ecosystem, functioning as a critical nexus between the online blockchain environment and the offline transactional space. This pool records and maintains user deposits of BTN tokens, playing an essential role in the fluid movement of funds across these two realms. A key feature of the Master Pool is its ability to insulate and protect the broader network from potential systemic risks that could arise from partial or complete failures of the offline transaction system. By serving as this safeguard, the Master Pool ensures the stability and integrity of the entire Bitnet infrastructure.

2. Payment Networks

Envisaged within the Bitnet system, Payment Networks resemble social network groups, designed to facilitate transactions in BTN tokens amongst their members. These networks can be established by various entities, such as merchants, community leaders, or governmental bodies, and are particularly valuable in providing economic resilience in situations of natural disasters or geopolitical upheavals. Users engage in transactions within these networks after transferring funds from the Master Pool, thereby initiating both online and offline exchanges. The autonomy of each Payment Network, coupled with its integration into the broader Bitnet system via the Master Pool, enables the creation of specialised economic communities. These networks provide a secure and localised platform for transactions while maintaining a connection to the Bitnet blockchain.

3. Smart Checks: Structure and Information

Smart Checks are integral to facilitating offline transactions within Bitnet's Payment Networks. These digital entities, encrypted for security, encapsulate a range of transactional data, ensuring the accurate and intended transfer of funds. Each Smart Check file contains several key pieces of information:

I. **Signed Transaction**: At the core of each Smart Check is the signed transaction. This includes all essential details such as the 'from' and 'to' wallet addresses, the amount being transferred, and the digital signature of the sender. The signature verifies the authenticity of the transaction, linking it indisputably to the originating wallet.

II. **Encrypted Serial Number**: Each Smart Check is assigned a unique serial number, generated automatically and encrypted for security. This encryption is performed using robust cryptographic algorithms like Keccak or SHA-2, ensuring that the serial number remains protected and tamper-proof.

III. **Processing Status**: The status of each Smart Check is dynamically recorded and updated based on its position in the transaction process. The statuses are as follows:

   a. **Issued**: The default status upon creation of the Smart Check.

   b. **Processed**: Updated when the Smart Check has been successfully cashed in and the transaction is complete.

   c. **Challenged**: Assigned when the check clearing is rejected by the network, automatically triggering an arbitration process.

By embedding these critical elements within each Smart Check, Bitnet ensures the seamless facilitation of transactions within its Payment Networks. This comprehensive approach to transactional data within the checks underpins the security and efficiency of the offline transaction system.

The integration of Smart Checks within the Bitnet ecosystem symbolises a significant advancement in blockchain technology. It addresses the challenge of internet dependency and initiates a new era of blockchain ecosystems that are adaptable and inclusive. Localised economic networks, empowered by these checks, can function autonomously yet remain securely tethered to the broader Bitnet blockchain, redefining the potential and scope of blockchain applications.

4. The Processing of Smart Checks: Transaction Integrity and Arbitration in Bitnet

a. Network Processing and Validation

In the Bitnet ecosystem, the processing of Smart Checks begins as users connect to the internet. The first party (payer or receiver) to go online initiates the clearance of these checks. Each check, encrypted with a unique serial number, is marked as "processed" by the network upon successful validation. This mechanism is underpinned by real-time balance updates, ensuring the availability of funds for each transaction.

b. Time-Lock on Withdrawals from Payment Networks

When withdrawing funds from a Payment Network to the Master Pool, a 40-day time-lock is activated. This time-lock serves as a vital period for monitoring transaction integrity and preventing double-spending. It also allows for additional users to update their balances, enhancing the overall robustness of the protocol.

c. AI-Driven Analysis and Human Arbitration

If discrepancies arise during the time-lock period, such as insufficient funds for transaction clearance, the transaction is flagged by an AI-driven system. These flagged transactions are then subject to review by the Arbitrage Panel, composed of human arbitrators. The panel examines the transaction, with the authority to rectify any discrepancies, ensuring the transaction's validity.

d. Forwarding and Processing Checks

Users receiving offline payments via Smart Checks can forward them within their Payment Network. These checks, while non-divisible, can be encapsulated in a new check file by the forwarder. The network processes a series of transactions based on the sequential holders of the check, ensuring the integrity and historical accuracy of each transaction.

e. Withdrawal Time-Lock and Challenge System

Post the 40-day time-lock within Bitnet, users opting to withdraw funds to their personal wallet trigger a subsequent 20-day time-lock. In this phase, the system permits direct challenges to the withdrawal from users who have previously sent funds to the withdrawing wallet. The permissible challenge is capped at the historical amount sent by the challenger to that wallet. This challenge mechanism adheres to a dynamic fee structure and an arbitration process, ensuring the integrity and fairness of the withdrawal procedure.

f. Dynamic Arbitration Fee

Challenges to transactions prompted directly by users within this framework incur a dynamic arbitration fee. Initially, challengers deposit a fee equating to 10% of the transaction value. The actual fee, however, is adjusted based on the arbitrator's response time, ranging from 1% to 10% of the transaction value. This fee structure incentivises swift and efficient resolution by the Arbitrage Panel.

This framework for processing Smart Checks in Bitnet ensures a high level of transactional integrity and security. The integration of AI analysis, combined with the human judgment of the Arbitrage Panel and the implementation of time-locks and dynamic fees, establishes Bitnet as a blockchain network capable of handling complex transactional scenarios with precision and reliability.

5. Arbitrage Panel and Arbitrators

The Arbitrage Panel within Bitnet serves as a pivotal component in the network's dispute resolution framework. Comprising individuals with a vested interest in the network's integrity, the Panel operates under a system designed to ensure fairness and accuracy in transactional disputes.

The Arbitrage Panel epitomises the principles of decentralisation and anonymity, underpinned by a system of staked BTN and meritocracy. This stake acts as both a commitment and a deterrent against partiality, ensuring that decisions are guided by fairness and integrity. Moreover, the anonymity of the Panel members is preserved, preventing undue influence or bias in their decision-making process. The allocation of cases to these arbitrators is governed by a quasi-random meritocratic Arbitration Score System, which assesses their performance based on the timeliness and accuracy of their dispute resolutions. This system ensures that the more proficient arbitrators handle a larger share of cases, fostering an environment where efficiency, fairness, and expertise are paramount. Such a framework not only reinforces the decentralised nature of the network but also upholds the principles of anonymity and meritocracy, crucial for maintaining the trust and reliability of the Bitnet blockchain.

a. Composition and Appointment

The Arbitrage Panel is formed from users who have staked a significant amount of BTN, aligning their interests with the network's overall health and stability. This stake acts as collateral, ensuring that Panel members adjudicate disputes impartially and diligently.

b. Functions

I. **Dispute Resolution**: The primary function of the Arbitrage Panel is to resolve disputes arising from flagged transactions. These could be due to inconsistencies in transactional data, potential double-spending, or challenges to withdrawals.

II. **Arbitration Process**: When a transaction is flagged by the AI system, either during the withdrawal process or within the Payment Network operations, it is forwarded by an AI-driven algorithm to an Arbitrator from the Arbitrage Panel on a quasi-random fashion, partially influenced by the Arbitrator's score. The members review the transaction details, considering historical data and the specifics of the case, to reach a decision.

III. **Challenge Review**: In cases where withdrawals are challenged, the Arbitrator examines the legitimacy of the challenge, ensuring that the claimant has historical grounds for their claim. The Arbitrator's decision in these matters is crucial to maintain trust and order within the network.

IV. **Dynamic Fee Structure**: The Panel operates under a dynamic fee structure, with fees imposed on challenges to transactions. These fees are adjusted based on the response time of the Arbitrator, incentivising prompt and efficient resolution of disputes.

V. **Maintaining Network Integrity**: Beyond dispute resolution, the Panel plays a role in maintaining the overall integrity of the Bitnet network. Their decisions set precedents for future transactions and help refine the network's protocols and safeguards.

c. Decision-Making

Decisions made by the Arbitrage Panel are final and binding within the network. The Panel is expected to base their judgments on a thorough understanding of the blockchain technology, Bitnet's specific protocols, and the broader principles of fairness and transparency.

d. Arbitration Fee Structure

Arbitrators are compensated for their services through an Arbitration Fee, contingent upon their response time to disputes. The fee structure is as follows:

- Respond within 1 hour: Retain 10% of the transaction value as a fee.
- 1-6 hours: 8% fee.
- 6-12 hours: 5% fee.
- 12-24 hours: 2% fee.
- 24-36 hours: 1% fee.
- Exceed 36 hours: Reallocation to another Arbitrator.

e. Arbitration Score System

In Bitnet, the Arbitration Score System quantifies the performance of Arbitrators, fundamentally influencing the distribution of cases. Points are allocated based on the timeliness and accuracy of their resolutions, ensuring efficient and just arbitration across the network.

Points Allocation Based on Response Time

The score of each Arbitrator is determined as follows:

- Less than 1 hour: Awarded 10 points for swift response.
- 1-6 hours: 8 points for a moderately quick response.
- 6-12 hours: 5 points for an acceptable response time.
- 12-24 hours: 2 points, reflecting a slower response.
- 24-36 hours: 1 point for minimal responsiveness.
- Over 36 hours: Deduction of 5 points for non-responsiveness.

Case Allocation Weighting

Arbitrators with higher scores benefit from up to a 20% increased likelihood of being allocated cases, fostering a meritocratic environment where efficiency and accuracy are rewarded.

Deductions for Non-Responsiveness

The system penalises non-responsiveness stringently. Arbitrators failing to address cases within 36 hours face point deductions, thereby discouraging inaction and ensuring that all disputes are addressed in a timely manner.

This scoring system ensures that the Arbitrage Panel operates at an optimal level, with members incentivised to maintain high standards of performance. By directly linking case allocation to the Arbitration Score, Bitnet guarantees a consistent, fair, and efficient arbitration process, vital for the network's integrity and user trust.

Process Rundown & Flow Chart: Offline Transactions in Bitnet

a. Depositing Funds into the Master Pool

The user initiates the process by depositing BTN tokens into the protocol. This deposit is recorded in the Master Pool, a central repository that serves as a bridge between online and offline transaction spaces within the Bitnet blockchain.

b. Allocating Funds to a Payment Network

The user then allocates a portion or the whole of these deposited funds to a specific Payment Network. Payment Networks, akin to social network groups, enable members to transact in BTN tokens. The user’s balance within the Payment Network is updated to reflect this allocation.

c. Making an Offline Payment

Within the Payment Network, the user can make payments to other members even in the absence of internet connectivity. They create and send a Smart Check, a secure digital instrument representing the transaction, using NFC technology. This check includes essential details such as transaction amounts, wallet addresses, and an encrypted serial number.

d. Sender or Receiver Coming Online and Processing the Smart Check

When the sender or the receiver of the Smart Check comes online, the Bitnet network processes the check. The network validates the transaction based on the check's details and updates the balances within the Payment Network. The status of the Smart Check is updated to "Processed" in the network.

e. Receiver Withdrawing Funds to the Master Pool

The receiver, now wishing to withdraw their funds, transfers the balance from the Payment Network back to the Master Pool. This action triggers a 40-day time-lock, a period designed for monitoring and preventing potential fraudulent activities.

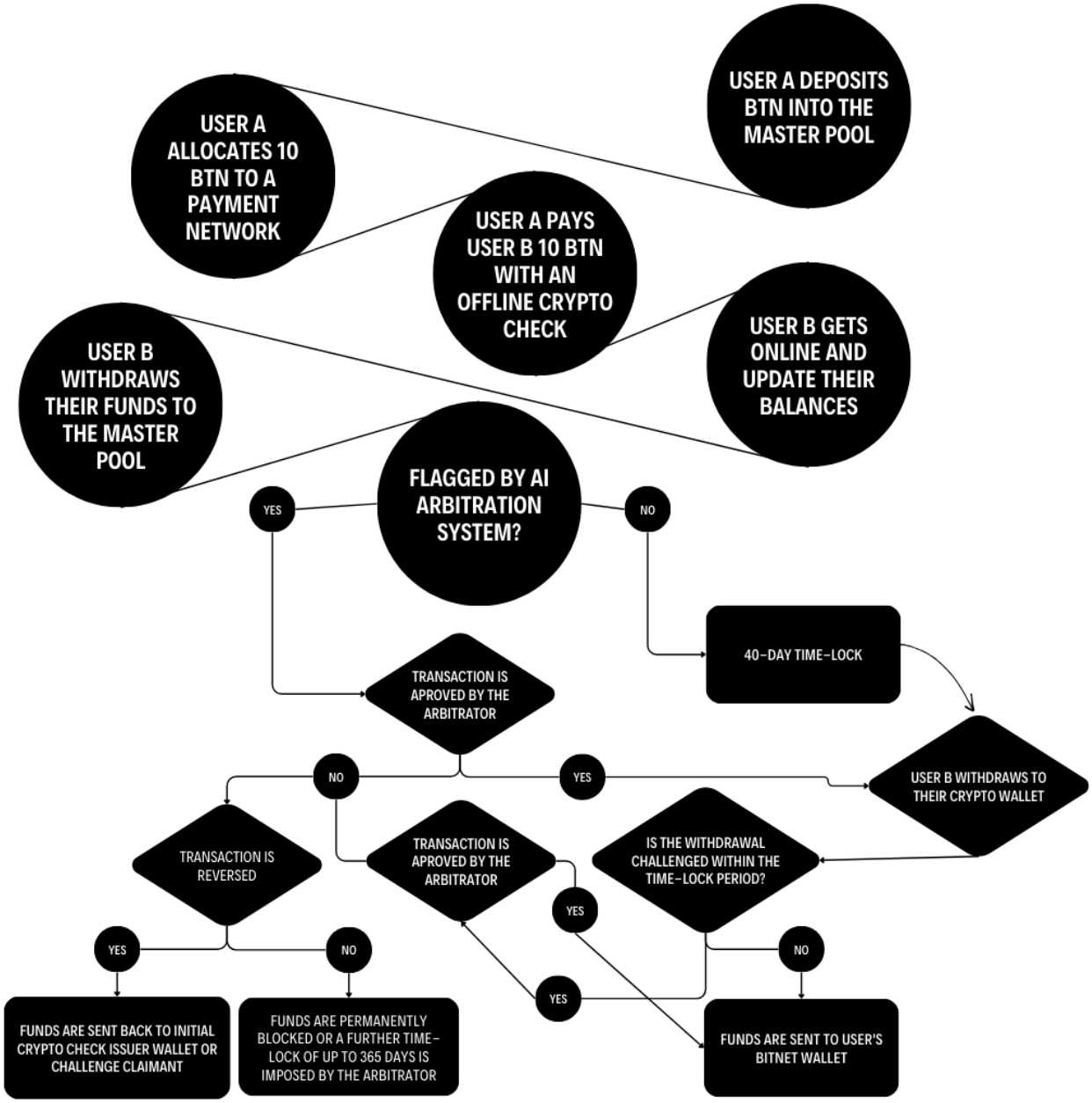
f. Withdrawing Funds to Personal Wallet

After the 40-day time-lock, the receiver can initiate a withdrawal from the Master Pool to their personal wallet. This step involves an additional 20-day time-lock, during which the transaction can be challenged

by any user who has previously sent funds to the receiver's wallet. The challenge is subject to a dynamic arbitration fee and is reviewed by the Arbitrage Panel.

g. Finalisation of Withdrawal

Once the 20-day time-lock period expires without any challenges, or after any challenges have been resolved, the funds are released from the Master Pool to the receiver's personal wallet. The transaction is then deemed complete, and the receiver has full access to their BTN tokens.



Implementation Challenges

In conceptualising the offline transaction framework for the Bitnet blockchain, we must acknowledge and address several potential challenges and drawbacks, including budgetary constraints, that may arise during its implementation.

1. Technical Complexity

The integration of Smart Checks, the Master Pool, Payment Networks, and an Arbitrage Panel into the existing Bitnet infrastructure is a task of considerable technical complexity. Developing a seamless and secure system for offline transactions requires not only advanced cryptographic solutions but also robust software capable of handling NFC technology and real-time balance updates. This complexity extends to ensuring the efficient functioning of the Arbitrage Panel and the Arbitration Score System, demanding significant resources for development and testing.

2. Network Security and Stability

Maintaining the security and stability of the network during the implementation of this new framework is paramount. As users engage in offline transactions, safeguarding against potential vulnerabilities that could be exploited in the absence of continuous network connectivity is crucial. This includes robust mechanisms to prevent double-spending and fraudulent activities within the Payment Networks and upon reconnection to the online environment.

3. User Adoption and Trust

Encouraging widespread adoption among users presents another challenge. Convincing users to trust and utilise a new system for offline transactions requires not only demonstrating its reliability and security but also ensuring its ease of use. Building this trust is essential for the successful implementation and long-term viability of the framework.

4. Budgetary Constraints

The financial aspect of implementing such an intricate system cannot be overlooked. Budgetary constraints may limit the scope of development, especially in areas requiring extensive research and innovation. Balancing the cost of implementation with the need for high-quality, secure, and reliable technology is a critical consideration.

5. Decentralisation and Anonymity

Maintaining the decentralised nature of the network while implementing a system that requires a certain degree of control and oversight, particularly in the Arbitrage Panel, is a delicate balance. Preserving the anonymity of Panel members while ensuring their accountability and performance is another aspect that demands careful consideration.

Conclusion

In this whitepaper, we have presented a detailed conceptual framework that is one of maybe many ways of implementing offline transactions within the Bitnet blockchain. This system, encompassing the Master Pool, Payment Networks, Smart Checks, and the Arbitrage Panel, marks a significant advancement in the realm of blockchain technology, particularly in addressing the challenges of internet dependency and transactional integrity.

The introduction of Smart Checks as encrypted, non-fractionable, digital representations of transactions enable users to conduct secure transactions offline. These checks, managed through specialised Bitnet software, utilise NFC technology for transfer, reinforcing Bitnet's resilience in varied network conditions.

The Master Pool serves as a central repository, playing a crucial role in the fluid movement of funds and acting as a safeguard against systemic risks. It also forms the nexus between the online blockchain environment and the offline transactional space, thus enhancing Bitnet's robustness and stability.

Payment Networks, resembling social groups, facilitate transactions among members and foster localised economic communities. They operate autonomously yet remain connected to the broader Bitnet blockchain, offering economic resilience in challenging scenarios.

The Arbitrage Panel and the Arbitration Score System ensure fair and efficient dispute resolution within the network. The Panel, comprising stakeholders with a vested interest in the network's health, adjudicates disputes

impartially. The dynamic fee structure and scoring system incentivise prompt and accurate resolution of disputes, contributing to the network's trustworthiness.

This framework not only mitigates the limitations of internet reliance but also heralds a new era of adaptable, inclusive blockchain ecosystems. By empowering localised, self-sufficient economic networks and securely linking them to the larger blockchain infrastructure, Bitnet redefines the boundaries and capabilities of blockchain technology.

The theoretical framework for offline transactions in Bitnet, as outlined in this whitepaper, offers a comprehensive solution to the challenge of ensuring continuous transactional capability in varied connectivity scenarios. It stands as a testament to the innovative potential of blockchain technology in creating more resilient, inclusive, and adaptable financial systems.