Bullet Pay

0xKJ 0xFBY

Sepetmber 2024 v1

Abstract

This whitepaper introduces Bullet Pay, a blockchain-native off-chain payment solution designed for fast confirmation and low-cost transactions. Unlike existing solutions like the Lightning Network, which rely on channel design, Bullet Pay utilizes innovative technologies such as the One-Time Spend Account and Transparent Payment Gateway. These innovations enable secure, decentralized settlement while ensuring rapid transaction processing, making Bullet Pay a robust alternative for everyday blockchain payments.

1 Introduction

Blockchain technology, by its very nature, is designed for secure and transparent asset storage and transfer. However, it is not optimized for fast payment confirmation, which is a critical requirement for everyday transactions. The blockchain's decentralized architecture and consensus mechanisms, while ensuring security and transparency, introduce latency in transaction processing. This latency can be detrimental to the user experience, particularly in scenarios where instant payment confirmation is essential. The importance of blockchain payment solutions cannot be overstated. However, existing solutions like the Lightning Network, which rely on channel design, have proven to be impractical for widespread adoption. In response, we propose an alternative approach, drawing inspiration from the concept of One-Time Spend Account and pre-consensus.

Our solution, Bullet Pay, strikes a balance between asset storage and payment, leveraging the strengths of blockchain for secure and efficient transactions. One of the significant advantages of Bullet Pay is its ability to facilitate instant payment confirmation, even in blockchain systems with large block time intervals. This is achieved through combining the centralized and decentralized system. The decentralized nature of blockchain technology, while ensuring security and transparency, inherently introduces inefficiencies in transaction processing. To address this, it is beneficial to strike a balance between decentralized and centralized approaches, ensuring a better user experience while maintaining the security guarantees of blockchain technology. By combining the strengths of both decentralized and centralized systems, we can create a more efficient and user-friendly payment experience, particularly in scenarios where instant payment confirmation is crucial.

While assets are stored on a decentralized blockchain, the payment process leverages a centralized system for payment confirmation. This hybrid approach allows for the benefits of both worlds: the security and transparency of blockchain technology for asset storage, and the speed and efficiency of a centralized system for payment processing. This instant payment confirmation capability is particularly important for everyday blockchain usage, where speed and efficiency are crucial. It enables users to make transactions with confidence, knowing that their payments will be processed quickly and securely.

As blockchain technology continues to evolve, the need for efficient payment solutions becomes increasingly evident. Existing approaches, like the Lightning Network, while groundbreaking, have significant limitations that hinder widespread adoption. Bullet Pay offers a simple solution by addressing these limitations and presenting a more practical and scalable way to facilitate blockchain payments.

Key Features of Bullet Pay:

- **Instant Payment Confirmation:** Achieved through a hybrid of centralized and decentralized systems, ensuring quick and secure transactions.
- **Reduced Fund Lock-in:** Funds are allocated dynamically, enhancing liquidity and usability.

- **Simplified User Experience:** Streamlined processes make Bullet Pay suitable for everyday transactions, with an emphasis on ease of use.

2 Transfer and Payment

In the context of financial transactions, it's crucial to differentiate between transfers and payments, as they have distinct purposes and characteristics. Payments requiring immediacy, which can be challenging for decentralized systems like blockchain to achieve fast payment confirmation. The additional centralized services beneficial for facilitating payments.

2.1 Transfers

Transfers typically involve:

- **Longer Processing Time**: Traditionally, transfers could take days to complete, especially for inter-bank or international transactions. With advancements in financial technology, transfers can now often be completed in minutes but still longer for international.
- **No Direct Exchange**: Usually doesn't involve an immediate exchange of goods or services.
- **Examples**: Sending money to a family member in another country, moving funds between personal accounts.

2.2 Payments

Payments, in contrast, have different characteristics:

- **Short Duration**: Traditionally, payments were often instantaneous, face-to-face transactions using cash.
- **Immediate Exchange**: They represent an immediate exchange of money for goods or services.
- **Direct Interaction**: Historically, payments often involved direct, personal interactions between buyer and seller.
- **Examples**: Paying for groceries at a local market, buying a coffee at a café.

2.3 Payment Solution for Blockchain

When considering blockchain technology in the context of financial transactions, it's important to recognize its strengths and limitations:

- **Low Capacity**: Blockchain networks, particularly public ones like Bitcoin, have limited transaction throughput due to factors such as block size and confirmation times.
- **Transfer-Oriented**: Blockchain excels as a transfer solution, providing a secure and transparent method for moving value on the chain network.
- **Lack of Payment Solution**: Traditional blockchain networks are not optimized for frequent, small-value payments due to their relatively slow confirmation times and transaction fees.
- **Settlement Layer**: Despite its limitations for everyday payments, blockchain can serve as an excellent settlement layer for payment systems built on top of it.

This understanding of blockchain's capabilities leads to a two-layer approach:

1. **Payment Layer**: Fast, efficient systems can handle frequent, small-value transactions off-chain.
2. **Settlement Layer**: The underlying blockchain acts as the final settlement layer, periodically recording the net results of numerous off-chain transactions.

This layered approach leverages the security and decentralization of blockchain for final settlement while enabling scalable, efficient payment solutions for everyday transactions.

3 Insufficient for Lightning Network

The Lightning Network is a second-layer solution built on top of Bitcoin networks, to address scalability issues and enable faster, cheaper transactions. This section will discuss two key concepts in the Lightning Network: one-to-one channel and one-to-N channels with relay nodes.

- The network aims to make payments as quick and seamless as traditional cash transactions.
- It also seeks to speed up transfers, potentially reducing them from minutes to seconds.
- The distinction between payments and transfers becomes less pronounced in terms of speed, but remains relevant for the purpose and context of the asset security.

The Lightning Network, while effective in theory, have limitations that make them less practical for widespread adoption. One of the primary concerns is the value locked up in these channels. The one-to-N Lightning channels deviate from the fundamental principle of one-to-one channel, enabling the channel to send funds to more than one recipient.

These limitations highlight the need for alternative solutions that can address the issues of blockchain payment.

3.1 One-to-One Lightning Channel

One-to-one Lightning channel forms the basic building blocks of the Lightning Network. In this setup:

- Two parties open a payment channel by committing funds to a multi-signature address on the blockchain.
- They can then conduct multiple off-chain transactions between themselves without broadcasting to the main blockchain.
- The channel can remain open indefinitely in theory, with only the final balance being settled on-chain when the channel is closed.

This approach significantly reduces transaction fees and confirmation times for frequent transactions between two parties. A significant drawback of the one-to-one Lightning channel is that it locks up user funds, making them unavailable for other transactions until the channel is closed. As more channels are created, the more funds are required for a single user to maintain liquidity across all channels. This can lead to a significant upfront cost for users, making it less practical for widespread adoption.

3.2 One-to-N Lightning Channels with Relay

The concept of one-to-N channels with relay nodes extends the capabilities of the Lightning Network:

- A relay user can open multiple channels with different parties, acting as a hub.
- Payments can be routed through these relay users, enabling transactions between parties that don't have a direct channel.
- This creates a network of interconnected channels, allowing for more efficient routing and increased liquidity.

The relay system enables the Lightning channels to function as a network, where users can send payments to any other user connected to the network, even without a direct channel. When a user is allowed to send funds in a channel to more than one recipient off-chain, there is a risk of double spending. Double spending occurs when a user tries to spend the same funds more than once. This is a serious issue in any payment/transfer system, as it can undermine the security and reliability of the system.

To address this problem, the Lightning Network employs a mechanism called "multi-signature transactions" to ensure channel security. In a multi-signature transaction, both the sender and recipient must sign the transaction before it is executed. If the two parties do not agree on the terms of the

transaction, the channel is reverted to its previous state, ensuring that the funds are not spent more than once and that the transaction is secure.

In addition, the Lightning Network leverages the blockchain's feature to prevent double spending by ensuring that the funds are not spent until a certain amount of time has passed. This prevents the sender from spending the funds before the recipient has had a chance to claim them.

One of the key requirements for the relay system to function effectively is that relay users must be online at regular intervals. This ensures that payments can be routed through them efficiently and that the network remains connected. If a relay user is offline for an extended period, it can disrupt the flow of payments and impact the overall performance of the network.

In the event that a relay user fails to function as expected, the end recipient may not receive the intended funds. This can occur due to various reasons such as:

- **Offline Relay Node**: If a relay node is offline, it cannot forward the payment, causing the transaction to fail.
- **Insufficient Funds**: If a relay node does not have sufficient funds to forward the payment, the transaction will not be completed.
- **Technical Issues**: Technical problems with the relay node, such as software or hardware failures, can prevent the node from processing transactions.

To mitigate these risks, the Lightning Network employs mechanisms such as:

- **Multiple Path Routing**: Payments can be routed through multiple paths to increase the likelihood of successful delivery.
- **Node Redundancy**: Implementing redundant nodes can ensure that if one node fails, another can take over the transaction.
- **Timeout Mechanisms**: Implementing timeouts can help detect and respond to failed transactions, allowing for retries or alternative routing.

These measures aim to minimize the impact of relay user failures and ensure that funds are delivered to the intended recipient.

3.3 Double Spending Problem

The blockchain consensus algorithm is designed to address the double spending problem by ensuring that all transactions are verified and agreed upon by the network. In the context of the Lightning Network, the one-to-one channel setup is effective in preventing double spending because the recipient is fixed and both parties must agree on the transaction terms.

However, the one-to-N lightning theory, which involves relay users, cannot solve the double spending problem if the relay users cannot stay online. This is because the fundamental requirement of the one-to-one lightning rule is broken, allowing for the possibility of double spending. The reliance on relay users introduces a point of failure, which can compromise the security of the system. Meanwhile, the payment would be delayed when relay users are not online, which can hardly fit for instance confirmation.

The best design of the Lightning Network is the concept of channel. However, it is hard for the users to practice. Many limitations in the usage while ensuring the prevention of the double spending problem.

3.4 Limitations of Lightning Channels

While the Lightning Network offers significant improvements in transaction speed and cost, it comes with certain limitations, particularly in the context of fund locking:

- **Locked Liquidity**: In traditional Lightning channels, especially one-to-one channels, funds are locked for the duration the channel remains open. This can tie up significant capital, reducing overall network liquidity.

- **Channel Capacity Constraints**: The amount that can be transacted is limited by the initial funding of the channel. This can be problematic for larger transactions or when the channel balance becomes skewed to one side.
- **Rebalancing Challenges**: When channel balances become uneven, users may need to close and reopen channels or perform complex rebalancing operations, which can be time-consuming and costly.
- **Network Topology Dependence**: The efficiency of payments depends heavily on the network's topology and the availability of well-funded channels, which can lead to routing difficulties.

These limitations highlight the need for more flexible protocols that can maintain the benefits of Lightning-style networks while reducing the constraints associated with locked funds. The following section will introduce a novel protocol designed to address these challenges.

4 Objective of Payment

The objective of the payment system is to ensure fast and secure transactions. While decentralization is important for the security of assets on the blockchain, it is not necessary for every aspect of the payment system. In fact, it is ideal to facilitate faster confirmations and improve the overall efficiency of the payment system while keeping all assets on-chain.

4.1 Payment with Fast Confirmation

To address the limitations of blockchain transfer delay, we propose a novel approach that enables fast confirmation of transactions. The payment service would help the merchant confirm the transaction as soon as possible, ensuring a smoother and more efficient transaction process.

4.2 Transparent Transaction Processing

The payment protocol ensures that user funds are never directly accessed or used for any purpose other than the intended transaction, maintaining the principle of user sovereignty over their assets.

5 Design of Bullet Pay

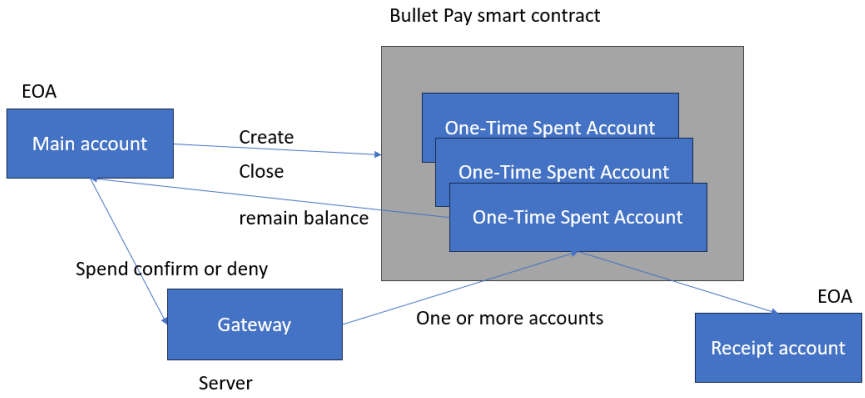

Figure 1: Bullet Pay System Diagram

5.1 One-Time Spend Account: A Novel Approach

To address the limitations of Lightning channels, we propose a novel concept: One-Time Spend Account. This approach offers a more flexible and efficient way to manage funds within the network. Here's how it works:

- **Sub-Account Creation**: Users can create multiple sub-accounts from their main account. Each sub-account is designated for a single transaction.
- **One-Time Use**: As the name suggests, each sub-account can only be used once for spending. This feature ensures better control and security of funds.
- **Automatic Balance Return**: After the transaction is completed, any remaining balance in the sub-account is automatically returned to the main account. This eliminates the need for manual rebalancing.
- **Reduced Lock-in**: Unlike channel design where funds might be locked for extended periods, this approach allows for more dynamic fund allocation.
- **Improved Liquidity**: By allowing users to allocate only the necessary funds for each transaction, this approach keeps more funds available in the main account, improving overall network liquidity.
- **Simplified Routing**: With sub-accounts created for specific transactions, payment becomes more straightforward to any existing blockchain address.

This One-Time Spend Account model offers several advantages over traditional Lightning channels:

- **Enhanced Flexibility**: Users can create sub-accounts for any recipients, without long-term lock of funds.
- **Improved Security**: The one-time use nature of sub-accounts reduces the risk associated with channel over payment.
- **Efficient Fund Management**: Automatic return of unused funds ensures that capital is always available for new transactions.
- **Scalability**: This approach can potentially handle a larger number of transactions with batch blockchain submition or a better infurstructure in future.

By implementing this novel protocol, we can maintain the speed and cost benefits of Lightning-style networks while addressing many of the limitations associated with traditional channel-based systems. The One-Time Spend Account is central to Bullet Pay's design. Users can create sub-accounts for single transactions, ensuring that funds are allocated only as needed. After the transaction, any unused funds are automatically returned to the main account, improving liquidity and simplifying fund management.

Advantages:

- **No Long-Term Fund Lock-in**: Funds are only allocated for the duration of the transaction.
- **Enhanced Security**: Single-use accounts reduce risks associated with prolonged fund exposure.
- **Dynamic Fund Allocation**: Improves overall network liquidity and user control.

5.2 Transparent Payment Gateway: Enhancing Speed and Security

To further improve the efficiency and security of our proposed system, we introduce a transparent payment gateway that acts as an intermediary between the main account and the One-Time Spend Account. This gateway offers several key benefits:

- **Accelerated Confirmation**: The gateway can implement optimized confirmation protocols, significantly reducing the time required to verify and process transactions.

- **Transparency**: The payment gateway provides a clear, auditable trail of all transactions, enhancing trust in the system.
- **Enhanced Security**: By acting as a buffer between the main account and sub-accounts, the gateway adds an extra layer of security to prevent double spending.
- **Fund Isolation**: The gateway never directly touches or controls user funds, maintaining the principle of user sovereignty over their assets.

The Transparent Payment Gateway acts as an intermediary between the main account and sub-accounts, facilitating fast and secure transactions. It ensures that user funds are never directly controlled by the gateway, maintaining the principle of user sovereignty over their assets. It serves as a crucial component in our protocol, bridging the gap between online payment system and the blockchain assets holding.

6 Bullet Pay Protocol

6.1 Topup: Pre-loading Sub-accounts

To further improve the user/merchant experience and secure the payment progress, we introduce a pre-loading mechanism for sub-accounts. This allows users to allocate funds to sub-accounts in advance, without locking these funds to specific merchants. This approach offers several advantages:

- **Faster Payment**: By pre-loading sub-accounts, users can initiate payment more quickly, as the funds are sent with a signature instead of sending via chain block processing.
- **Better Fund Management**: Users can allocate funds to sub-accounts on mobile phone payment app for daily usage, without the risk of carrying large assets.

This pre-loading feature combines the benefits of our One-Time Spend Account model with the convenience of having readily available funds for quick payments. It maintains the security and flexibility of our original design while offering users more control over their funds and the ability to send to arbitrary merchants.

6.2 Spend

When a user initiates a payment, they may choose to use one or more sub-accounts. To facilitate this, the list of sub-account IDs and amounts to be used, and the recipient's address are signed with the private key of user's payment wallet. This signed information is then sent to the payment gateway for processing.

The payment gateway operates as follows:

1. When a user initiates a payment, the gateway accepts the payment from the one or more One-Time Spend Accounts.
2. The gateway verifies the sub-account ids and make sure it is never been used before.
3. Once verified, the gateway facilitates the payment from the sub-account to the recipient onchain, and notify the merchant.
4. The gateway then oversees the transaction from the sub-account to the recipient, ensuring its successful completion, monitoring the process for any anomalies.
5. After the onchain transaction, any unused funds from the sub-accounts has returned to the main account.

6.3 Simplified User Experience

One of the key advantages of the Bullet Pay system is its focus on simplifying the recipient's experience. Unlike blockchain-based transfer systems, where the recipient may need to wait for seconds or minutes to confirm the funds, Bullet Pay confirms that the funds are directly paid to the recipient with instant notification.

This approach not only enhances the recipient experience but also increases the adoption rate of the blockchain system. By making the process seamless and hassle-free for chain users, Bullet Pay encourages more widespread use of blockchain technology for everyday payment. The sender is required for creating the One-Time Payment Account before initiating the payment. This action is as simple as the topup to the sender. Both end-user and recipient are familiar with the process.

In future, it is possible to have payment hardware whose secret key in the chip can never be exported. The payment hardware can be topup from the crypto wallet on mobile phone or PC.

7 Limitations of Existing Infrastructure

Despite the advancements made by Bullet Pay in enabling offline payments, the current infrastructure of Layer 1 (L1) and Layer 2 (L2) solutions still falls short of achieving the payment capacity of traditional payment systems like Visa or Alipay. This highlights the need for further infrastructure upgrades to support the growing demands of blockchain-based payments.

To overcome these limitations, it is essential to invest in the development of more advanced infrastructure that can support the high demands of blockchain-based payments. This includes the creation of more scalable, efficient blockchain networks that can facilitate high capacity, secure, and reliable transactions.

7.1 Wider Sharding System for Scalability

To address the limitations of traditional blockchain-based payment systems in terms of transaction per second (TPS), we have developed a novel sharding system called Wider. This innovative solution enables the payment gateway to process a virtually unlimited number of transactions within the blockchain's block interval, significantly enhancing the overall scalability of the system.

Wider achieves this by horizontally partitioning the blockchain into smaller, parallel chains, each capable of processing a huge of transactions. This approach allows for a substantial increase in the total TPS, making it suitable for high-demand payment systems. The Wider sharding system ensures that each shard operates independently, yet in harmony, to facilitate seamless and efficient transaction processing.

By leveraging Wider, our payment system can handle a large volume of transactions in limited-time, making it an ideal solution for applications that require high throughput and low latency. This technology breakthrough enables us to overcome the blockchain scalability limitations in payment, providing a fast, secure, and reliable payment experience for users.

7.2 Unlocking Smart Contract Computation Capacity

In addition to the Wider sharding system, our technology also addresses the performance limitations imposed by the Virtual Machine (VM) execution limitations on blockchain transactions. Minus Theory innovation unlocks the full capacity of smart contracts by removing the constraints of on-chain computational resources on VM execution.

By decoupling the VM execution from the blockchain's on-chain resources, we enable smart contracts to execute without being limited by the blockchain's computational power. This breakthrough allows for more complex and computationally intensive smart contracts to be executed efficiently, further enhancing the overall performance and capabilities of our payment system.

The Minus Theory's impact on VM execution enables a significant increase in the complexity and sophistication of smart contracts, making it possible to support a wider range of use cases and applications. This, in turn, expands the potential of blockchain technology in various industries, including finance, supply chain management, and more.

8 Conclusion

This whitepaper addresses the misconception that transfers and payments are interchangeable by emphasizing the significance of a gateway for payment pre-consensus. Our approach leverages the unique properties of One-Time Payment Account to facilitate efficient and secure payments. The Payment Gateway plays a crucial role in ensuring the integrity and speed of the payment process. By consolidating payment consensus, it enables the system to verify and validate transactions in a timely manner, thereby ensuring that payments are processed quickly and securely.

The use of One-Time Payment Account is particularly well-suited for this design. These sub-accounts are created for a single payment and are then discarded, providing an additional layer of security and minimizing the risk of double spending. This approach also simplifies the management of funds, as each sub-account is dedicated to a specific transaction, making it easier to track and reconcile payments. Moreover, the One-Time Payment Account mechanism inherently minimizes the risk of double-spending, as each sub-account can only be used once. This eliminates the possibility of an attacker attempting to spend the same funds multiple times, thereby ensuring the integrity of the payment process.

Bullet Pay redefines blockchain payment systems by addressing the limitations of channel-based solutions like the Lightning Network. With its innovative One-Time Spend Account and Transparent Payment Gateway, Bullet Pay offers a robust, user-friendly, and scalable solution for fast and secure payments. By simplifying the user experience and leveraging cutting-edge technologies like Wider Sharding and Minus Theory, Bullet Pay sets a new standard for blockchain payments, making it a powerful tool for the future of digital finance.