Midl whitepaper

Table of contents

Abstract

The Midl introduces a Bitcoin execution layer designed to enable the native execution of decentralized applications (dApps) directly on the Bitcoin network. Midl allows users to interact with robust EVM-level smart contracts using their own Bitcoin wallets without bridging assets or leaving the Bitcoin network by providing an additional abstraction layer. This seamless integration enhances the user experience, offering fast transaction finality – requiring only one Bitcoin block confirmation – and unlocking new capabilities for Bitcoin, such as supporting advanced dApps like staking platforms, AMMs, GameFi, and SocialFi applications.

This whitepaper describes the architecture, consensus mechanism, interaction with smart contracts, security considerations, and the roadmap for Midl's development.

Introduction

Since its beginning, Bitcoin has established itself as a secure and decentralized platform for peer-to-peer transactions. However, its limited scripting capabilities have restricted the development of complex decentralized applications (dApps) directly on its network. While alternative platforms like Ethereum have succeeded in the dApp ecosystem, a significant demand remains for native dApps on Bitcoin.

The Midl aims to bridge this gap by introducing a Bitcoin execution layer that enables the native execution of dApps, providing a seamless and efficient user experience comparable to EVM-compatible platforms. By allowing users to utilize powerful smart contracts directly on the Bitcoin network without the need for bridging or leaving the network, Midl enhances scalability, speed, and functionality on Bitcoin.

Vision

Despite Bitcoin's dominance in cryptocurrency, its inability to support complex smart contracts and decentralized applications (dApps) has limited its utility compared to platforms like Ethereum. The Midl team envisions overcoming these limitations by enabling native execution of dApps on the Bitcoin network, enhancing usability, and providing seamless access to advanced functionalities without compromising the user experience.

Existing solutions attempting to bring dApps to Bitcoin often face challenges such as:

- **Native approach**:** **Existing solutions do not provide a native experience to users – those solutions merely commit state into Bitcoin from external systems without seamless integration and direct interaction – introducing complexity and potential security risks. These factors delay user interactions and hinder the development and adoption of decentralized applications on Bitcoin.
- **User experience**: One of the most significant UX challenges of BTC dApps is that existing solutions require users to bridge funds out of the Bitcoin network, necessitating additional time and complicating the overall workflow.
- **Limited functionality**: Bitcoin's scripting language is not Turing-complete, restricting the development of advanced dApps and limiting the network's capabilities.

- **Scalability issues**: High transaction fees and slow confirmation times hinder the deployment of scalable applications, affecting developers and users.

Our mission

The Midl aims to address these challenges by introducing an execution layer that allows users to natively utilize Bitcoin network assets in robust EVM-level smart contracts without bridging funds or waiting additional time. By doing so, Midl enhances the user experience while enabling users to remain within the Bitcoin network and employ their preferred wallets.

Solution

Midl is a Bitcoin execution layer that enables the native execution of decentralized applications (dApps) on the Bitcoin network. Essentially, Midl acts as an abstraction layer – an intermediary between Bitcoin and Layer 2 solutions.

By offering full compatibility with the Ethereum Virtual Machine (EVM), Midl brings the rich functionality of Ethereum dApps to Bitcoin users.

Key features

- **No bridging required**:** **Midl eliminates the need for users to bridge funds, enabling fast and native execution of smart contract transactions on the Bitcoin network. Transactions require** only one Bitcoin block confirmation instead of the usual six**, significantly accelerating the process and allowing users to perform smart contract transactions natively. Midl offers more than just a Layer 2 solution; it provides an additional layer of abstraction where everything happens seamlessly and instantly in one step, without any prior actions required from the user.
- **Native dApps on Bitcoin**: Midl offers a genuinely native dApps experience by enabling the execution of decentralized applications directly on the Bitcoin network. As users don't have to bridge their funds, change wallets, or perform transactions on any network other than Bitcoin, Midl provides a seamless and familiar environment. By offering an EVM-like experience, Midl brings advanced dApps – such as staking platforms, Automated Market Makers (AMMs), GameFi, and SocialFi applications – to operate natively on Bitcoin, a capability previously only possible on platforms like Ethereum.
- **Cross-chain transactions**: Supports interoperability with EVM-compatible chains, enabling asset transfers and dApp interactions.
- **User-friendly experience**: Enables users to utilize their own Bitcoin wallets, integrating with popular wallets to provide a seamless and familiar interface for dApp interaction.
- **Efficient scaling**: Enhances user experience by allowing multiple EVM transactions within a single BTC transaction, reducing fees and improving transaction throughput.

Technical architecture

Consensus mechanism

Midl utilizes a Delegated Proof-of-Stake (DPoS) consensus mechanism to achieve faster transaction finality than relying exclusively on Bitcoin's proof-of-work consensus. Validators are selected based on their stake – the Midl tokens/BTC ratio – and are responsible for processing transactions, maintaining the network, and ensuring security.

- **Validator selection**: Top N validators are chosen weekly based on their total stake.
- **Validator groups**: Validators are divided into groups, each managing TSS Vaults for transaction processing.
- **Rotation**: Validator sets are rotated periodically to ensure decentralization and security.

Validators and staking

- **Staking requirements**: Validators must stake their BTC and Midl tokens in the System's Staking Contract.
- **Delegation**: Users can delegate their stakes to validators, sharing in network and Native BTC Yield.
- **Infrastructure responsibilities**: Validators must run Midl nodes, manage threshold signature schemes (TSS Vaults), and monitor Midl and Bitcoin networks.

Slashing conditions

Validators face slashing (loss of stake) for malicious activities such as:

- Refusal to execute user transactions.
- Prolonged non-participation in consensus.
- Invalid transaction execution.
- Attempts to attack or destabilize the network.

Network operation

- **Execution layer dependency**: The Midl network relies entirely on Bitcoin's blockchain and security mechanisms.
- **User interaction**:

  - **Creating BTC transactions**: Users create BTC transactions with funds (BTC and Runes) intended for use in dApps and send them to threshold signature schemes (TSS Vaults) controlled by validators. This approach emphasizes decentralization and ensures that no single entity controls the funds, enhancing security and trust in the network.
  - **Signing dApp messages**: Users sign virtual Midl dApp transactions and attach the BTC transaction hash using their BTC private keys.
  - **Result**: The user awaits BTC dApp transactions in the form of receiving desired BTC and Runes due to this interaction.
- **Validators processing**:
  - **Acknowledging BTC blocks**: Validators acknowledge the next Bitcoin block and the transactions sent to the Midl TSS Vault.
  - **Processing Midl transactions**: Validators process the corresponding Midl transactions.
  - **Finish validating user intents as finality reached**: At this point, Validators commit Midl block with Merkle root of Bitcoin transactions sent to Midl TSS Vaults.
  - **Returning BTC transactions**: Validators send corresponding Bitcoin transactions back to users.
- **Scalability**:
  - **Multiple transactions per BTC transaction**: Users can send up to 10 Midl transactions within a single BTC transaction, enhancing scalability.

Interaction with smart contracts

User experience

Midl provides a user experience similar to interacting with EVM-based dApps but leverages Bitcoin wallets for transaction signing. Users can:

- **Use familiar BTC wallets**: Interact with compatible native BTC wallets of choice. No need to change what you are used to.
- **Multiple transactions**: Send up to 10 Midl transactions simultaneously within a single BTC transaction.
- **Sign intents securely**: Users generate and sign intents** – **representing their desired actions within Midl dApps – using their BTC private keys, which remain securely in their wallets. Midl does not have any access to these private keys at any time. The signed intents include attached BTC transaction hashes, ensuring that all transactions are authenticated and controlled exclusively by the user.

Transaction processing

![[MIDL BTC tx flow(TSS VAULT).png]]

- **Transaction creation**: Users generate Midl raw transactions (intents), sign them, and include the corresponding BTC transaction hash.

- **Execution**: Validators work with virtual assets on the Bitcoin network. They acknowledge the Bitcoin transactions and virtually mint the corresponding assets needed to process the dApp transactions within the Midl network.
- **Finalization**: After processing the dApp transactions, the validators burn the virtual balances. They then return actual Bitcoin transactions containing the assets to the users, completing the process.
- **Committing Midl state to BTC**: After execution of all BTC block transactions related to Midl, Midl validators create Midl compact state proofs and commit them to BTC to later be used to verify Midl state against it and for users to verify valid BTC dApps execution.

Wallets support

Midl supports integration with popular wallets to provide users with seamless interaction using their preferred Bitcoin wallets. Currently, Midl supports:

- **Xverse**.
- **MetaMask (via BTC Snap)**.

Requirements for wallet integration:

For wallets to support Midl and be added to our frontend app connectors, they must meet the following requirements in addition to basic Bitcoin network functionalities:

1. **Signature support**:
   - Ability to support **secp256k1** signatures.
2. **Transaction handling**:
   - Capability to read and broadcast transactions on **testnet V3** (support for testnet V4 is a plus).
3. **Runes support**:
   - **Taproot address generation**: Ability to generate Taproot addresses.
   - **Runes balance indexing**: Index the Runes balance of public addresses.
   - **Runes transfer**: Enable the transfer of Runes.
4. **Message signing**:
   - Implement the *signMessage()* function for BTC wallets using the **BIP322** format.

Future support:

- **Ledger**: Integration with Ledger hardware wallets is planned for future updates to expand wallet compatibility.

Bitcoin security reliance

Commitment to the Bitcoin blockchain

Midl relies on Bitcoin's security by:

- **Merkle root commitment**: Storing Midl blockchain data on Bitcoin by committing the Merkle root of Midl blocks between Bitcoin blocks.
- **TSS Vaults**: Validators use threshold signature TSS Vaults to control UTXOs and commit the Midl state to Bitcoin.
- **Data storage**: Validators and the Midl network store the full state of the Midl blockchain internally. To reduce on-chain data and transaction fees on Bitcoin, validators commit compact Midl state proofs directly to the Bitcoin blockchain. This approach ensures that the Midl state can always be verified against Bitcoin later, maintaining data integrity and security while minimizing the amount of data stored on-chain.

Tokenomics

Midl token

- **Staking token**: Validators utilize it to participate in consensus and secure the network.
- **Governance**: Holders can vote on network proposals and future developments.
- **Security**: Crucial for preventing network domination by "whales" (large stakeholders), ensuring decentralization and protection against potential manipulation.

Roadmap Midl bootstrapping

Midl network bootstrapping will slowly expand and build its security in several phases. It will also give time for the initial team to verify that the network runs smoothly and fix potential bugs or add additional security mechanisms for the subsequent network upgrades.

Phases

Midl's development will progress through several phases to ensure security and stability:

1. **Permissioned phase**: A select number of initial validators run a single threshold TSS Vault.
2. **Validator expansion**: Gradual increase in validators and threshold TSS Vaults.
3. **Permissionless DPoS**: Open participation with several threshold TSS Vaults, scaling according to network needs.

Note: Specific parameters like the number of validators and threshold TSS Vaults will be finalized after further analysis and security audits.

Conclusion

The Midl represents a significant advancement in bringing native dApps and enhanced functionality to the Bitcoin network. By providing a user-friendly experience and enabling the execution of robust EVM-level smart contracts directly on Bitcoin – without the need for bridging – Midl addresses the limitations currently faced by Bitcoin users seeking to engage with decentralized applications.

For developers and existing EVM protocols, Midl allows access to BTC network liquidity and Runes without forcing users to bridge assets. Smart contract code remains unchanged, frontend read interactions are the same, and write interactions require minimal adjustments. This dramatically improves the developer experience related to interactions with the Bitcoin network.

Midl employs a Delegated Proof-of-Stake (DPoS) consensus mechanism to secure the network and process transactions efficiently. While DPoS can be critiqued for having a lower number of validators, it is a suitable choice for Midl for several reasons:

1. **Scalability with validator numbers**: TSS Vaults need to scale better with a high number of validators, unlike networks like Ethereum that can support potentially hundreds of thousands of validators. DPoS accommodates a practical number of validators for Midl's needs.
2. **Balanced participation and decentralization**: DPoS allows for multiple options regarding how often each chosen validator validates blocks. Validators can be made equal in participation despite differing stakes, helping to prevent excessive centralization.
3. **Comparative industry practice**: In practice, Bitcoin and Ethereum are controlled by a small number of stakers or mining pools. Therefore, their consensus algorithms are not ideal for decentralization, making DPoS a reasonable choice for Midl.

Through careful planning, robust technical architecture, and a commitment to security, Midl aims to become a cornerstone in the evolution of the Bitcoin ecosystem, promoting innovation and broader adoption of blockchain technology. By addressing key challenges and providing practical solutions, Midl enhances the functionality and accessibility of Bitcoin for both users and developers.

References

- **Bitcoin whitepaper**: Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*.
- **Ethereum whitepaper**: Vitalik Buterin, *A Next-Generation Smart Contract and Decentralized Application Platform*.
- **Delegated Proof-of-Stake (DPoS)**: DPoS Consensus Algorithm
- **BIP322**: *Generic Message Signing in Bitcoin*, BIP322

For more information and updates, please visit the Midl official website and join our community channels.

Disclaimer

This document is provided for informational purposes only and is subject to change. Before using the Midl, conducting your own analysis and staying updated with the latest information from official sources are recommended. Certain parts of this document may undergo significant changes after additional security considerations and deep security audits.

For more information and updates, please visit the official Midl website and join our community channels.