BitWeave: Bitcoin smart contracts on Layer 1

Matteo Coppola, Raul Rosa, contact@fluidtokens.com, 2024

Abstract

FluidTokens introduces BitWeave, a revolutionary approach to leverage transactions on the Bitcoin network to create smart contract behavior directly on Bitcoin's main layer.

This innovative protocol eliminates the need for intermediaries and enables permissionless interactions between parties.

BitWeave paves the way for the development of various DeFi protocols on Bitcoin, including the first fully permissionless lending protocol. This whitepaper elucidates the architecture, mechanics, and potential applications of BitWeave, highlighting its transformative impact on decentralized finance (DeFi) and Bitcoin's sovereignty.

Introduction

The integration of decentralized finance (DeFi) protocols with the Bitcoin network has been a longstanding challenge due to Bitcoin's scripting language and lack of native smart contract functionality.

BitWeave heralds a new era of decentralized finance (DeFi) on Bitcoin's main layer, leveraging determinism and PSBT to enable smart contract behavior directly on the blockchain. This innovative approach unlocks the ability to create multiple possible future outcomes within a set of transactions, paving the way for a myriad of DeFi services to be built directly on Bitcoin Layer 1.

Leveraging Determinism and PSBT

At the core of BitWeave lies the concept of determinism, which enables the spending of transactions that do not yet exist on the chain in the Unspent Transaction Output (UTXO) model. This groundbreaking capability allows users to create a set of possible future outcomes within a limited set of transactions, providing unprecedented flexibility and versatility.
Determinism, in the context of transaction and script processing, is a synonym for predictability. This means that a user can predict locally (off-chain) how their transaction will impact the on-chain state of the ledger, in particular the transaction Id.

BitWeave harnesses the power of Partially Signed Bitcoin Transactions (PSBT), which are metatransactions where users sign only their own inputs and all the transaction outputs.
PSBTs are a data format that allows wallets and other tools to exchange information about a Bitcoin transaction and the signatures necessary to complete it.
A PSBT can be created to identify a set of UTXOs to spend and a set of outputs to receive that spent value. Then information about each UTXO that's necessary to generate a signature for it can be added, possibly by a separate tool, such as the UTXO's script or its precise bitcoin value.
PSBTs enable collaborative transaction signing, allowing multiple parties to contribute signatures in any order, as long as each party signs their own inputs. This collaborative signing process enhances security and efficiency while facilitating complex transaction workflows.

On-Chain Enforcement Through Bitcoin Script

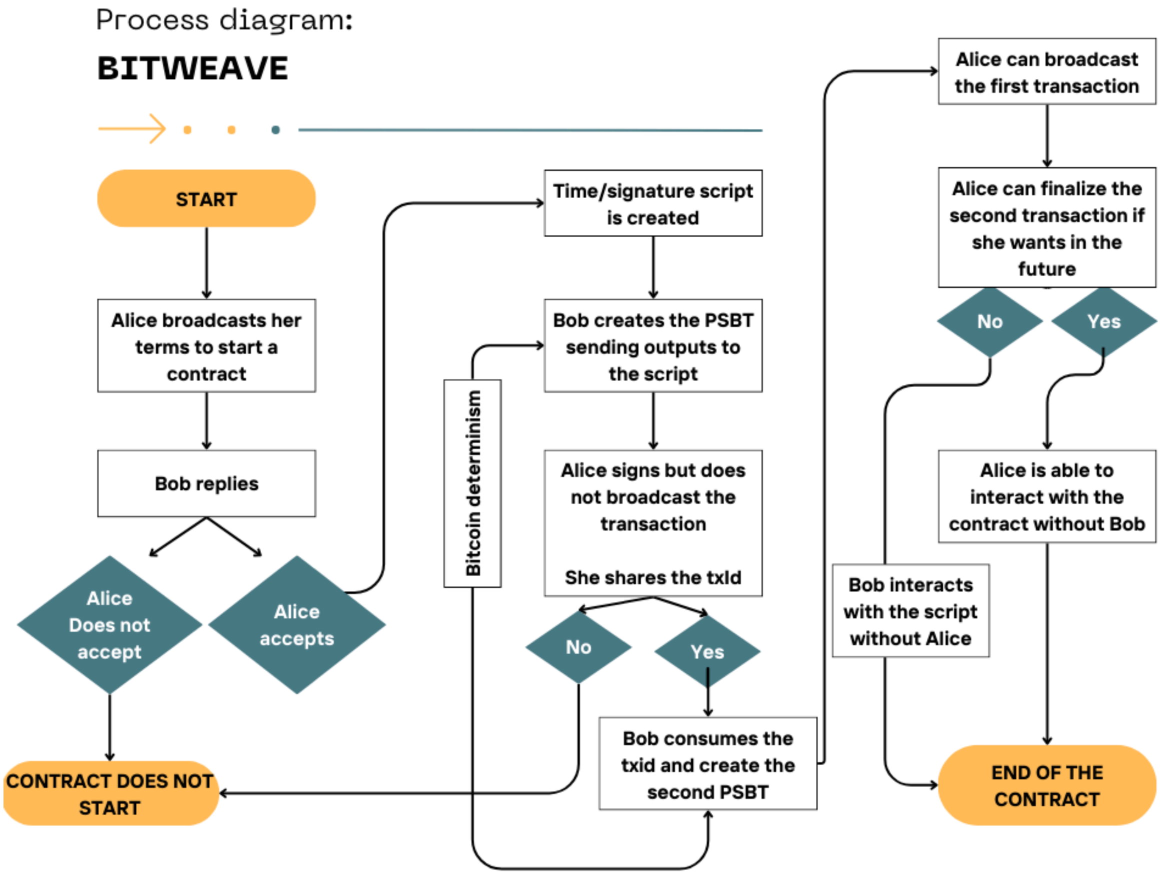
The conditions to spend the possible outcomes generated by BitWeave are explicitly enforced on-chain through the Bitcoin Script language. By embedding conditional logic directly into the transaction outputs, BitWeave ensures trustless execution without the need for intermediaries. This on-chain enforcement mechanism guarantees the integrity and immutability of the transaction outcomes, mitigating the risk of manipulation or fraud.

Expanding DeFi Services on Bitcoin Layer 1

BitWeave opens up a wealth of opportunities for expanding DeFi services directly on Bitcoin Layer 1. Beyond lending protocols, BitWeave can be utilized to create a wide range of decentralized financial products and services, including decentralized exchanges, automated market makers, derivatives platforms, and more. By enabling quasi-smart contract behavior on Bitcoin's main layer, BitWeave empowers users to access a diverse array of DeFi offerings while preserving the security and sovereignty of the Bitcoin network.

BitWeave redefines the possibilities of decentralized finance on Bitcoin by introducing a mechanism for creating multiple possible future outcomes within a finite set of pre-signed transactions. Each future outcome is enforced by conditions written in the Bitcoin blockchain through the Script language, ensuring trustless execution without the need for intermediaries.

Permissionless lending on Bitcoin Main Layer


Process diagram:
BITWEAVE
START
Alice broadcasts her terms to start a contract
Bob replies
Alice Does not accept
Alice accepts
CONTRACT DOES NOT START
Time/signature script is created
Bob creates the PSBT sending outputs to the script
Bitcoin determinism
Alice signs but does not broadcast the transaction
She shares the txId
No
Yes
Bob consumes the txid and create the second PSBT
Alice can broadcast the first transaction
Alice can finalize the second transaction if she wants in the future
No
Yes
Alice is able to interact with the contract without Bob
Bob interacts with the script without Alice
END OF THE CONTRACT

FluidTokens leverages BitWeave to create the first fully permissionless lending protocol on Bitcoin, enabling users to borrow and lend BTC using various collateral assets, including BRC-20, Runes and Ordinals.

The loan process within the FluidTokens ecosystem follows a streamlined approach, ensuring a seamless experience for both lenders and borrowers:

1. **Liquidity Pool Creation**
Lenders initiate the lending process by creating liquidity pools through on-chain transactions, establishing the foundation for borrowing activities.

During this step the following script is used:

```
OP_DUP
OP_HASH160
LENDER_PUBLIC_KEY
OP_EQUALVERIFY
OP_CHECKSIG
```

In this way lenders are the only ones in control of their liquidity

2. **Off-chain Communication**

Borrowers and lenders engage in off-chain communication to negotiate and sign loan and repayment transactions. This off-chain interaction streamlines the loan process while minimizing on-chain congestion and costs.

During this process the borrower is able to sign a loan PSBT without propagating it, in this way the lender is able to create a repayment PSBT and the borrower can propagate the first one only once this is completed.

Collateral during the loan process is sent to the following script and both parties can verify that the collateral is going to it before signing the transaction::

```
OP_IF
    DEADLINE_LOAN
    OP_CHECKLOCKTIMEVERIFY
    OP_DROP
OP_ELSE
    BORROWER_PUBLIC_KEY
    OP_CHECKSIGVERIFY
OP_ENDIF
LENDER_PUBLIC_KEY
OP_CHECKSIG
```

At the end of the offchain signatures we have the first on-chain interaction.

3. **Loan Initiation**

Borrowers initiate loans by submitting on-chain transactions, securing borrowed funds against chosen collateral assets. This triggers the borrowing period and enables borrowers to access the desired liquidity.

At this moment the borrower will pay fees to the protocol using the liquidity from the loan.

4. **Flexible Repayment and Withdrawal**
Borrowers have the flexibility to repay loans and withdraw collateral assets at any time during the loan period, empowering them with autonomy and control over their financial transactions. This is possible thanks to the second PSBT signed by the lender, the repayment.
Borrower is able to sign in any moment the repayment transaction without permission from FluidTokens

5. **Collateral Claim**
Upon the expiration of the loan deadline, lenders have the option to claim collateral assets if borrowers fail to repay loans. This mechanism ensures the security of lenders' investments while incentivizing timely repayments.

At this point the script where the collateral is stored allows the lender to claim the ordinal without need of interactions with the borrower or the protocol itself.

Future Developments

FluidTokens is committed to advancing the capabilities of BitWeave and exploring new opportunities to empower Bitcoin as a sovereign layer 1 blockchain. Key areas of future development include:

1. **Integration of Oracles**: The team is working on integrating Oracles for automatic liquidation, enhancing risk management and efficiency within the lending protocol.

2. **Sovereign Layer 1 Protocols**: FluidTokens aims to develop additional protocols that further empower Bitcoin as a sovereign layer 1 blockchain, unlocking new possibilities for decentralized finance and beyond.

3. **Runes integration**: While ordinal NFTs are hard to price, runes will be the standard that will allow DeFi platforms to interact with fungible tokens, having way more liquidity and therefore an easy tracking of the current price. FluidTokens is going to allow the use of Runes inside the platform.

Conclusion

BitWeave represents a paradigm shift in the realm of decentralized finance, enabling smart contract behavior directly on Bitcoin's main layer. By leveraging innovative transaction mechanisms and the Script language, BitWeave paves the way for the development of fully permissionless lending protocols and other DeFi applications on Bitcoin. With a commitment to decentralization and user empowerment, FluidTokens is poised to revolutionize the DeFi landscape on Bitcoin, ushering in a new era of financial sovereignty and innovation.

Disclaimer

The information presented in this whitepaper is for informational purposes only and does not constitute financial or investment advice. Users are encouraged to conduct their own research and consult with financial professionals before engaging in any DeFi activities. FluidTokens and its team are not liable for any losses incurred as a result of using the protocol.