Programmable Zero- knowledge-based Bitcoin HyperLayer

Bring Smart Contract and Dapps to Bitcoin to Unleash $700B

Abstract

Since Bitcoin was launched in 2009, blockchain has led to the rapid development of numerous distributed applications as the next-generation Internet infrastructure. Alongside this, various blockchain infrastructures have emerged, targeting different application scenarios such as smart contracts, lending, trading, and stablecoins. Currently, Bitcoin accounts for around 50% of the total market capitalization in the crypto market. However, due to its non-Turing complete scripting language, the lack of mainnet smart contracts, and slow transaction speeds, its long-term development is severely hindered. In the immensely prosperous Ethereum ecosystem, we recognize its enormous potential for expansion.

Introducing bitsat, we are building a HyperLayer on the Bitcoin network to achieve a scalable network compatible with the EVM. On HyperLayer, different types of protocols and smart contracts can be built using the VM Engine. This means that decentralized applications can be built on the Bitcoin network, and assets from different protocols can circulate within the same network layer.

Operating as a Turing complete blockchain system, HyperLayer utilizes zero-knowledge proofs for off-chain transaction verification and packages transaction states into UTXO. This enables assets to be transferred between HyperLayer and the Bitcoin main network without relying on trust.

We envision building a massively adopted infrastructure for thousands of decentralized applications in the world's largest blockchain ecosystem.

bitsat

Why Unleash Value for Largest Blockchain?

The value of the Bitcoin network will be unleashed infinitely. It will be utilized in Dapp, such as DeFi, DEX, NFT, etc.

$726B +

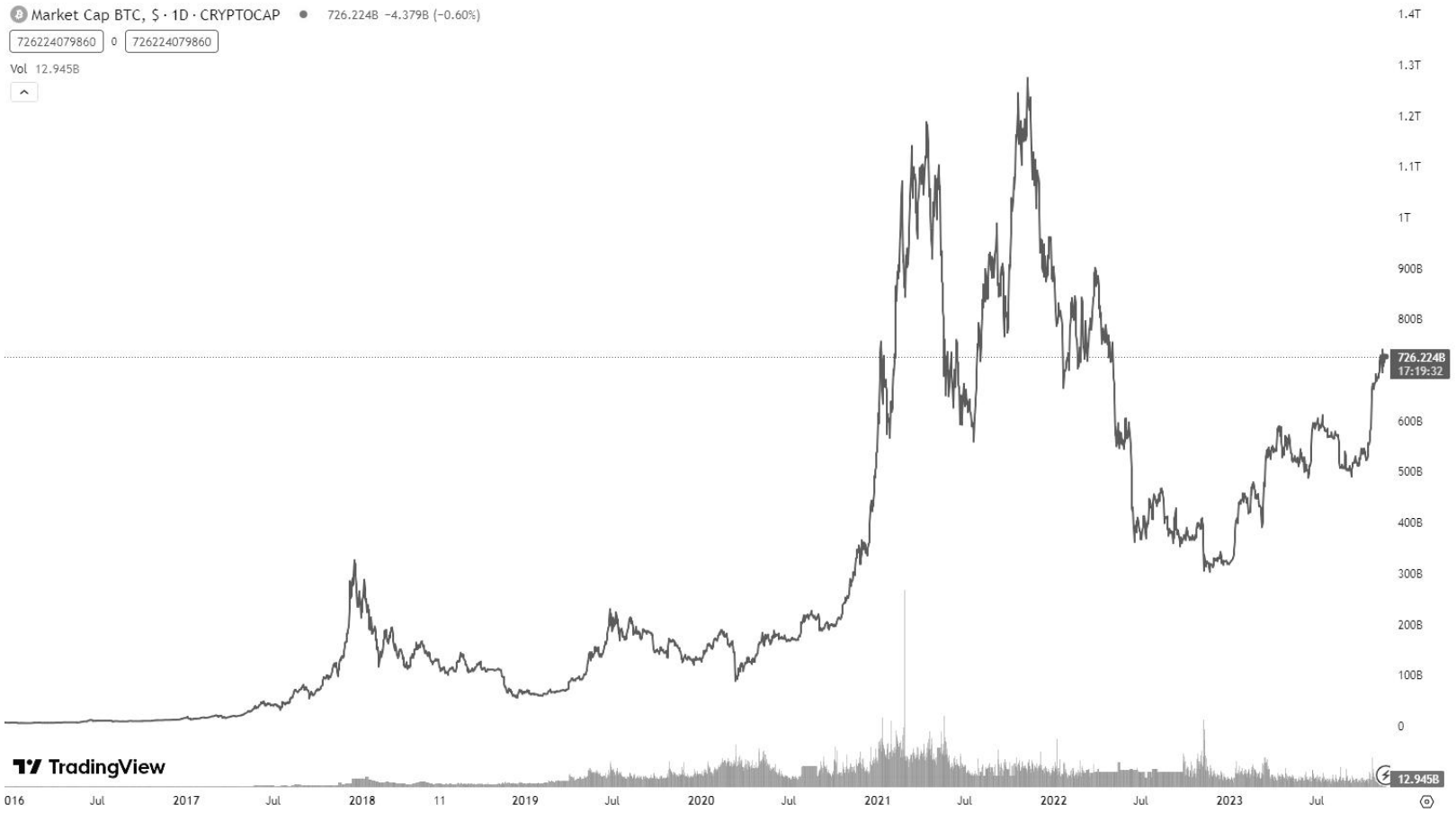
Marketcap

$10B-$70B

Trading volume per day

70B +

TVL prediction (≈10% Marketcap)



*Sources: TradingView, CoinMarketCap | 20,11,2023

bitsat

What Factors Limit Bitcoin?

Scalability Limitation

Bitcoin's block size limit and transaction confirmation time lead to network congestion and longer transaction processing times.

Non-Turing Complete

Scalability limitation is the largest barrier for the wide adoption of Bitcoin network.

Compatibility

Protocols based on Taproot are not mutually compatible and lack bridges to external ecosystems.

Large Fluctuations in Network Fees

As the Bitcoin market price and network status fluctuate, the continuous increase in network fees makes transactions costly.

Extended Security

Bitcoin's Layer 2 scaling and network protocols often sacrifice decentralization or efficiency, making it difficult to effectively inherit the security of the native network.

What Users, Builder, Crypto Investors Needs on Bitcoin?

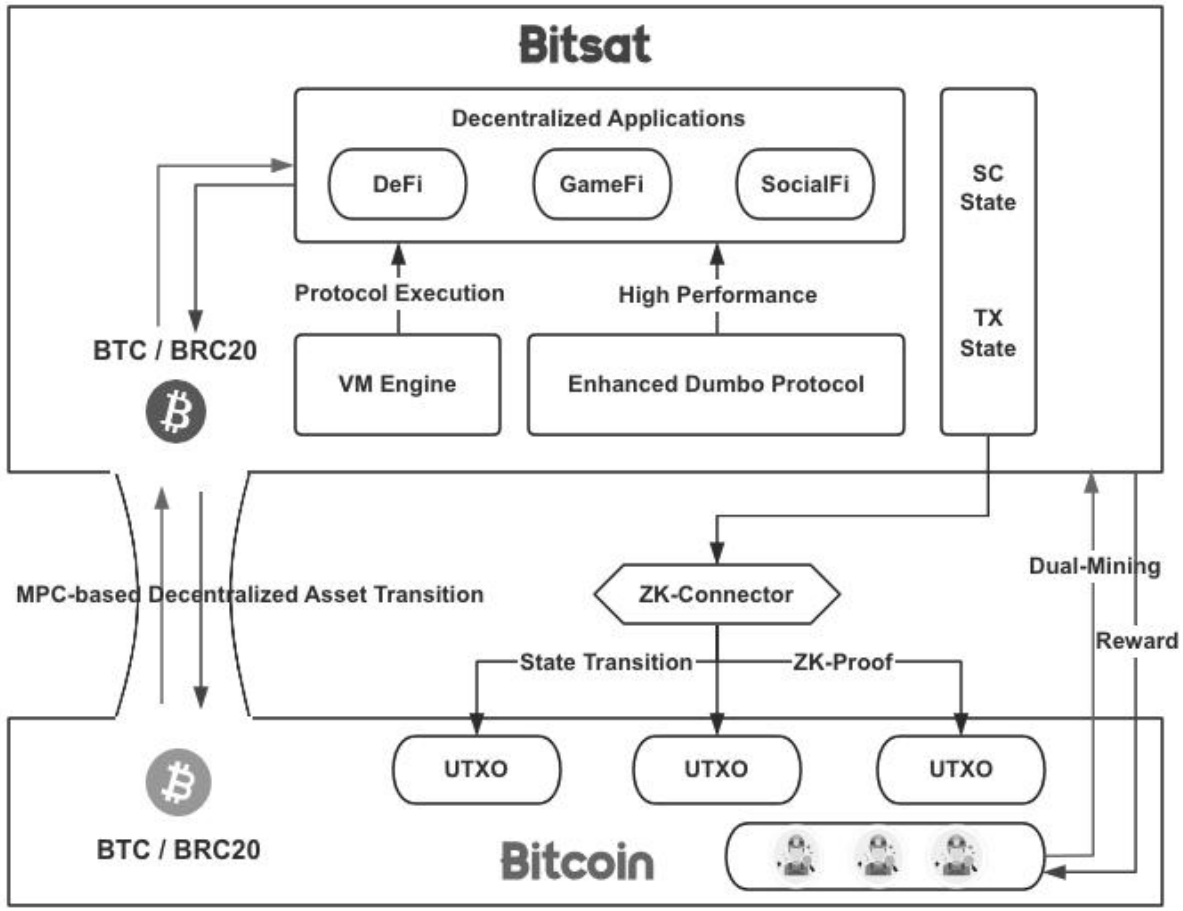
Needs on Bitcoin	Bitsat
Transactions securely and quickly	Enhanced Dumbo Protocol and ZKrollup guarantee faster and more secure
Improve ctyptos liquidity on DeFi	Support build SWAP and DEX on chain
Build DApp on chain quickly and simply	EVM compatibility
Low transaction fees	Processing transaction on Hyperlayer

Build on Bitcoin HyperLayer

Bitsat operates by creating a HyperLayer, with its core design consisting of three elements: the cross-layer communication mechanism established by ZK-Connector, the smart contracts established by the VM Engine, and the asynchronous high-performance consensus mechanism of the Enhanced Dumbo Protocol.

The HyperLayer compresses transaction states and verifies them on the UTXO, which means that when a transaction occurs, it does not need to directly record all information on the Bitcoin main blockchain, while inheriting the security of the Bitcoin network.

This makes near-instant and low-cost Bitcoin transfers between parties possible, making micro-payments and daily transactions more feasible. By offloading most transactions from the main blockchain, the HyperLayer aims to alleviate congestion and improve the overall efficiency and usability of the Bitcoin network.



bitsat system structure

Feature

High Performance

The asynchronous consensus mechanism ensures the high performance and scalability of the HyperLayer, with eventual atomicity, maximizing the efficient throughput of each consensus group

Security

Account asset control and management are implemented based on Secure Multi-Party Computation (SMPC) . It satisfies the optimal threshold property and enables secure asset transfers between the Bitcoin network and the HyperLayer in a fully decentralized manner

Scalability

Compatibility with EVM. Bitsat encapsulates the execution abstraction of the virtual machine, introducing smart contracts to Bitcoin, allowing DApps to migrate at a low cost

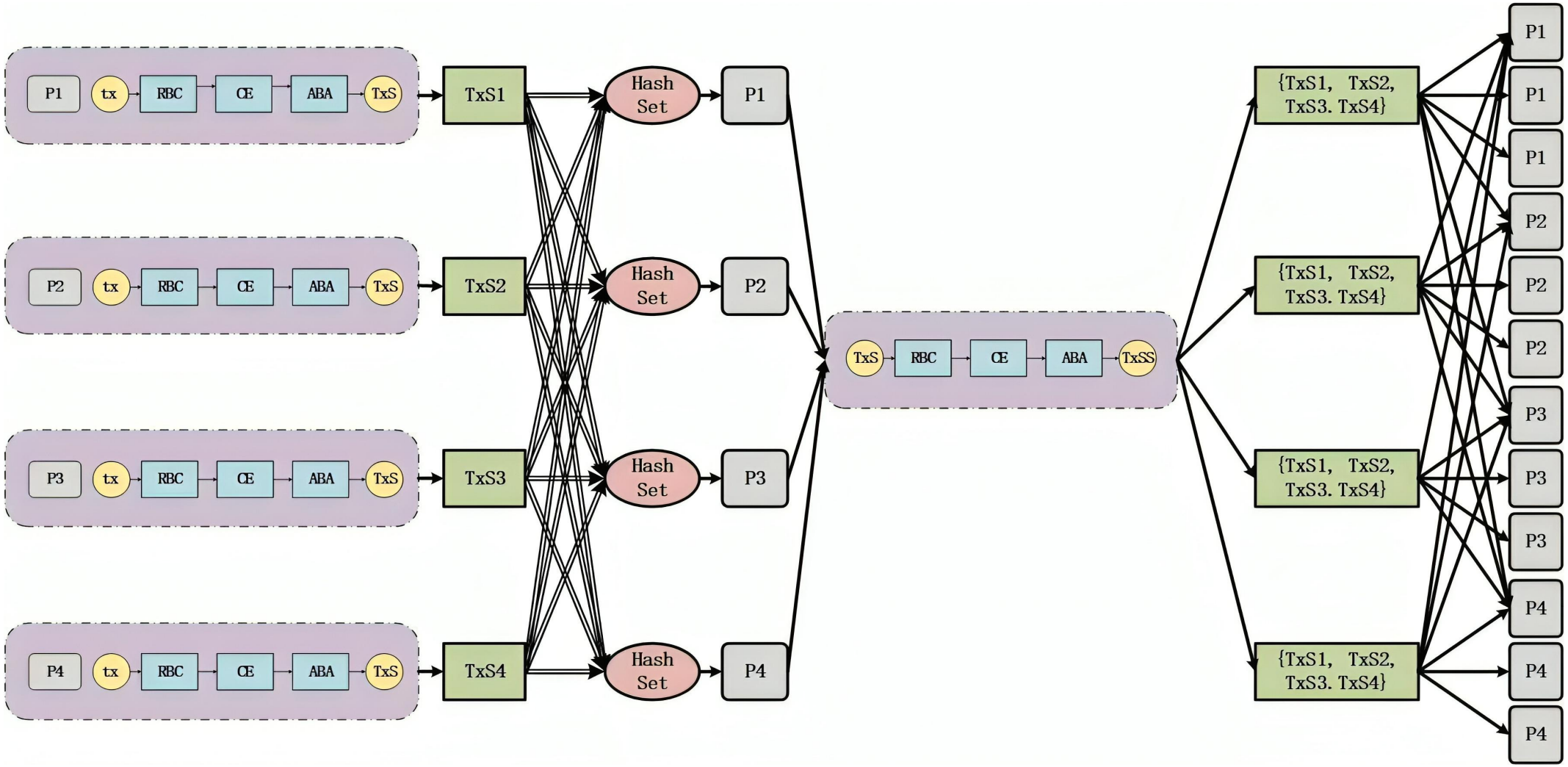
Inherited Layer1

Transactions on the HyperLayer are packaged into UTXO verification through zk-proof, inheriting the security of the Bitcoin network

bitsat

High Performance Consensus

The asynchronous Byzantine fault tolerance ensures security and maintains liveness even under extreme network conditions. Based on the Enhanced Dumbo Protocol, it can be widely adopted on a large scale. It has also led to a sharp reduction in transaction costs.



bitsat

Enhanced Dumbo Protocol Performance

Best Security & Performance

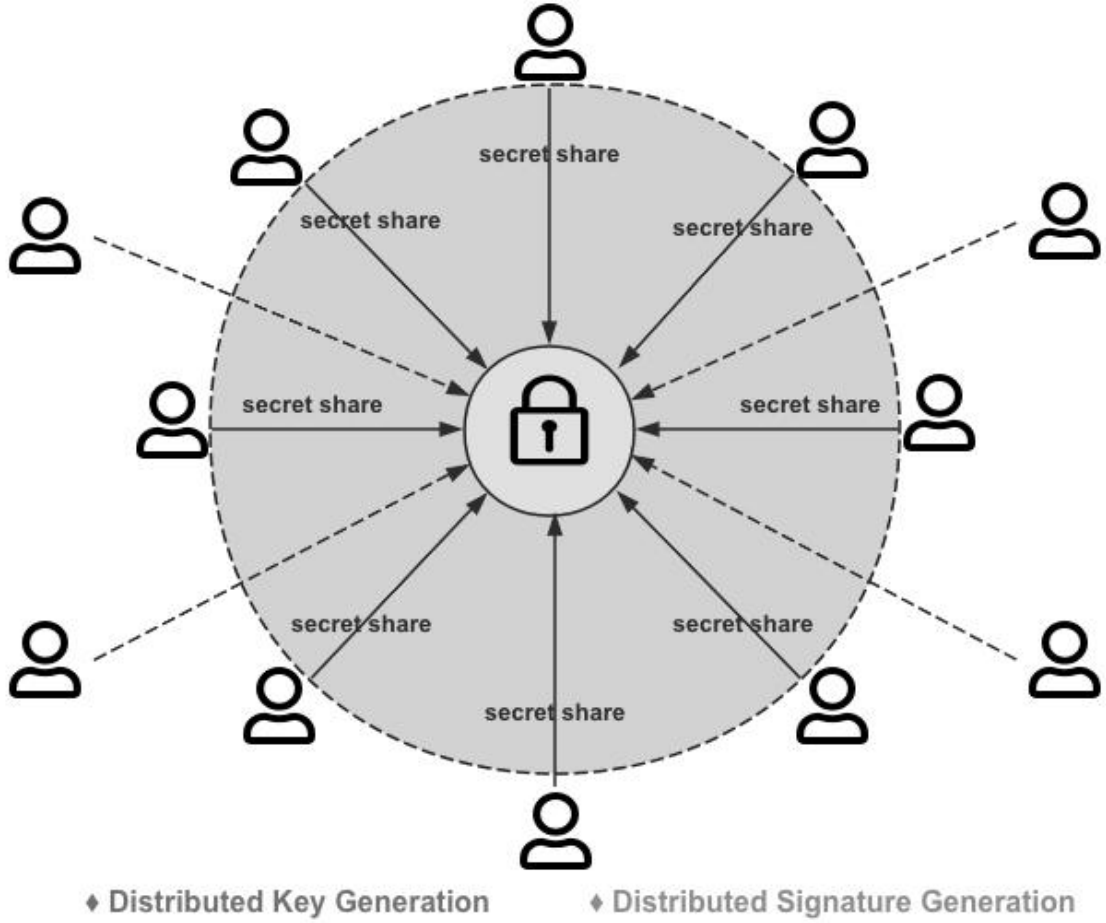
100,000 Tx+ /s

bitsat

How to Implement Cross-layer Assets Securely?

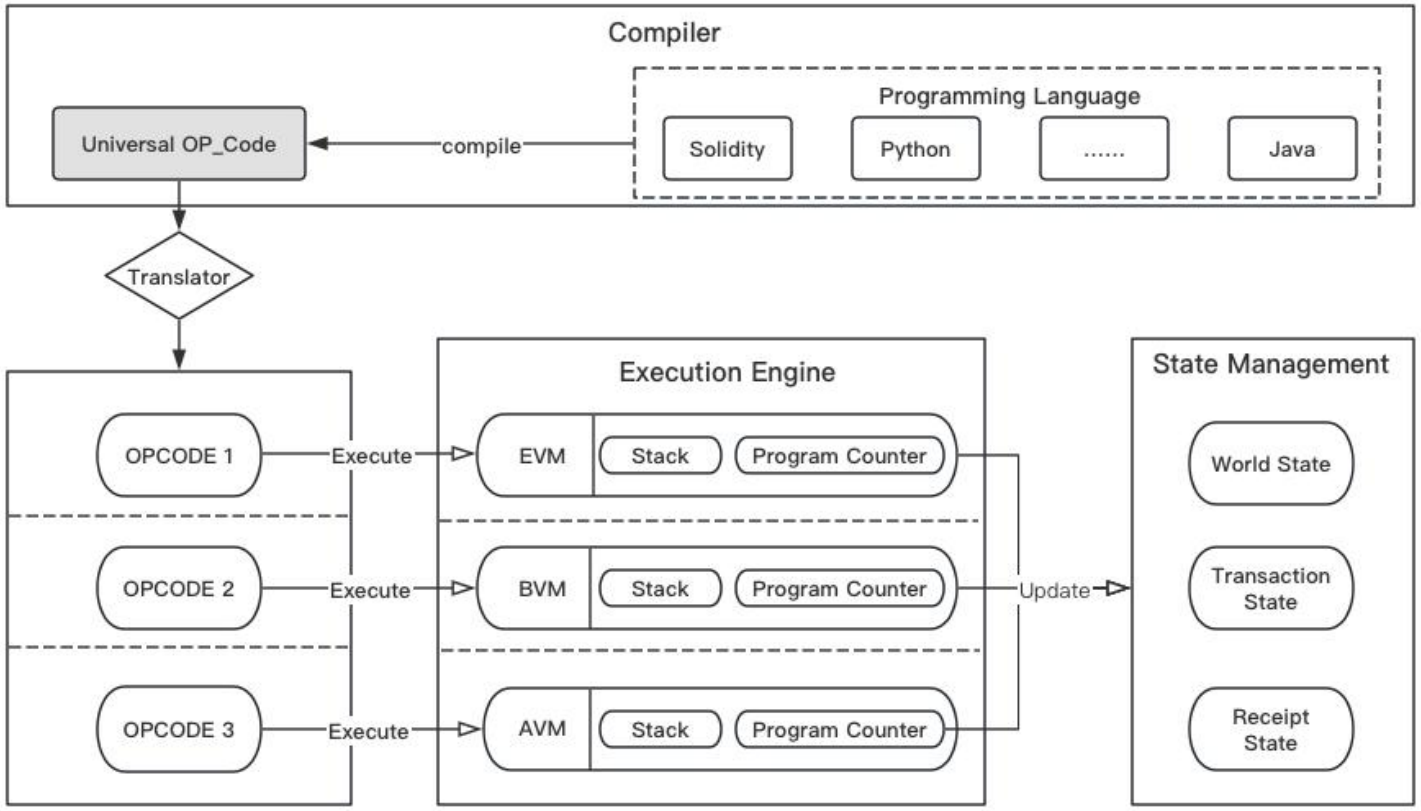
Trustless Custody of Assets

The Decentralized Custody Node (DCN) is a decentralized custody node deployed on Layer 1, enabling multi-party management of accounts through threshold signatures. Users can transfer assets to the DCN, facilitating the transfer of assets from Layer 1 to HyperLayer. Upon receiving a user's withdrawal request, the asset management node constructs a transaction, generates the corresponding valid signature, and broadcasts the transaction on Layer 1, smoothly transferring the user's funds from HyperLayer to the Layer 1 account.



bitsat

VM Engine: Compatibility with EVM



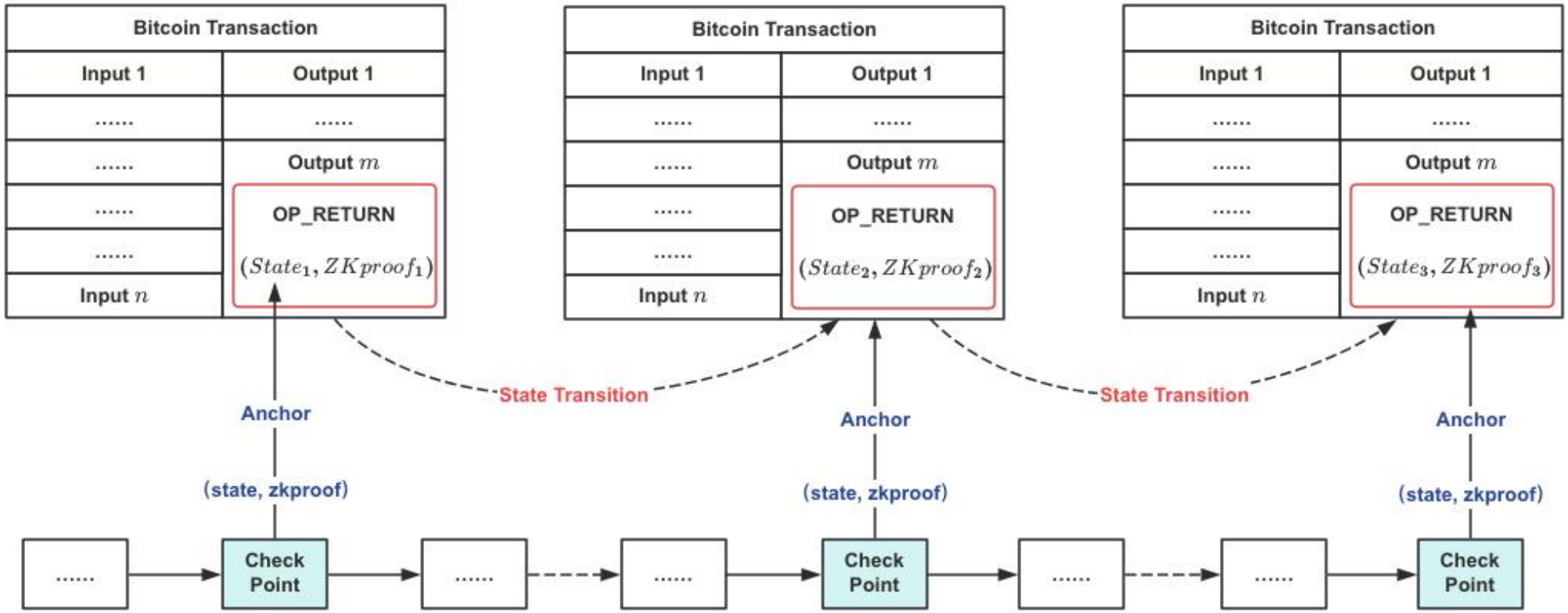
bitsat VM Engine

It is possible to build different types of protocols and smart contracts using the VM Engine on HyperLayer. This means that Dapp can be built on the Bitcoin network, and assets from different protocols can circulate within the same network layer.

bitsat

Synchronization with UTXO

The transactions on HyperLayer are packaged and verified through zk-proof, inheriting the security of the Bitcoin network.



bitsat ZK-Connector

bitsat

Why HyperLayer?

Bitcoin Layer 1

Economic Incentives

Consensus

P2P Network

Blocks

Bitcoin Layer 2

Lightning

Sidechain

Plasma

HyperLayer

Economic Incentives

High Performance Consensus

P2P Network

Blocks

Smart-contract

ZK-Rollup

EVM

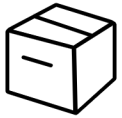
Why Bitsat?

	UTXO	Sidechain	Lightning	Protocal Layer	HyperLayer
Project	Bitcoin	Stacks	RGB	Ordinals	bitsat
Consensus	Proof of Work	Proof of Transfer	/	/	Enhanced Dumbo Protocol
Tx Processing	UTXO	UTXO	Client-Side Verification	UTXO	ZK rollup+UTXO
Security	High	Middling	Middling	High	High
Decentralization	High	Low	Low	Low	High
Performance	Low	High	Middling	Low	High
Smart-contract	×	√	×	√	√
Account	×	√	√	×	√
Language	×	Clarity	×	×	Solidity
DApp	×	√	×	×	√
Network Fee	High	Low	Low	High	Low

Technical Innovations

Decentralized Assets Mint

Management of assets are achieved using secure multi-party computation (SMPC) , supporting ECDSA and Schnorr threshold signature algorithms, and enabling secure asset transfers between the Bitcoin network and HyperLayer in a fully decentralized manner.



ZK rollup

The data of HyperLayer (including account state and contract state) is anchored in UTXO after being aggregated and compressed based on ZK. UTXO carry HyperLayer data, including validity and other relevant information.

Enhanced Dumbo Protocol

The asynchronous consensus mechanism ensures high performance and scalability of HyperLayer, achieving eventual atomicity and maximizing the efficient throughput of consensus groups.

VM Engine

The virtual machine execution abstraction encapsulates compatibility with mainstream virtual machines, introducing smart contracts to Bitcoin, and supporting costless migration of other DApps.

Dual-Mining

Bitcoin blocks carry transactions containing HyperLayer's state data and zk-proof. Block miners receive additional incentives.

Beneficial for Builders, Traders, Users

Real-time Confirmation of Transcations

Enhanced Dumbo Protocol enables high-speed processing of transaction throughput, meeting the needs of large-scale adoption by decentralized applications.

Assets Circulation of Trustless

Secured Asset transfer ensured by Zero- knowledge.

Low Network Fee

Tenmendously lower the network fee based on HyperLayer processing.

EVM Compatibility

Developers can quickly build decentralized applications on HyperLayer.

Additional Incentives for Bitcoin Miners

Bitcoin miners receive economic incentives for verifying transactions that include HyperLayer-packaged state on HyperLayer.

Inheritance of UTXO Security

Transactions on HyperLayer are packaged into UTXO verification through zk-proof, inheriting the security of the Bitcoin network.

bitsat

Bitcoin Ecosystem is Coming

2023

Feasibility Analysis

Technical Research

Product Development

2024 Q2

Testnet Launch

VM Egine
EVM compatibility

Incentive Plan

WhitePaper Issurance

2024 Q4

Mainnet 1.0

Enhanced Dumbo Protocol

2025

Mainnet Launch

Mainnet

ZK-Connector
Compress and verify transactions in zk-proof

2026

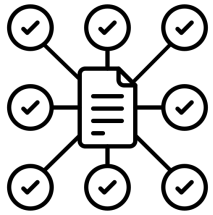
Protocal Compatibility

VM Egine
WASM compatibility

Cross Layer protocal
ERC on HyperLayer

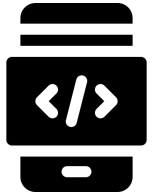
bitsat

What We Can Do on Bitcoin HyperLayer?

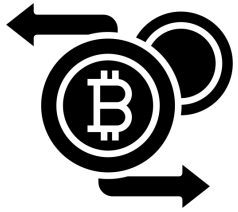


DeFi

Crypto/NFT/BRC Issuance



Dapp



DEX / Swap

Staking

Stablecoin

bitsat

Contact US

support@bitsat.ai

@Bitsat_Official

https://t.me/Bitsat_Official