BEVM: An EVM-compatible Bitcoin Layer 2 with BTC as gas

29/11/2023, BEVM Foundation

Abstract

BTC commands nearly 50% of the cryptocurrency market share, yet since its inception, Bitcoin has lacked a mature Layer 2 (L2) solution. Following key technological upgrades such as Segwit and Taproot, along with the popularity of the Ordinals protocol and BRC20 tokens, we introduced BEVM, a fully decentralized, EVM-compatible Bitcoin Layer 2 solution using Bitcoin as its gas.

I. Why Does Bitcoin Need Layer 2?

1. Maintain the Security of the Bitcoin Network.

The fundamental purpose of Bitcoin Layer 2 is to maintain the security of the entire Bitcoin network. It is well known that the Bitcoin network would collapse without miner maintenance. Bitcoin's block reward halves every four years, and the next halving is scheduled for April 2024, reducing the reward from ***6.25*** BTC to ***3.125*** BTC per block. If the price of BTC does not double, miners' earnings cannot be guaranteed, providing no incentive for new miners to join or for existing miners to increase their computing power. Additionally, macroeconomic uncertainties and black swan events could lead to a significant drop in Bitcoin prices, further squeezing miners' profits and forcing some mining companies to shut down. Over time, this could weaken the miners' motivation and willingness to maintain the Bitcoin network, thereby compromising its security. Therefore, finding new sources of income for miners to promote their maintenance of Bitcoin network security and consensus has become a crucial issue.

In 2023, with the emergence and popularity of the Ordinals protocol, transaction fees have become the second-largest source of income for miners, accounting for 10-30% of their income. This demonstrates that fee consumption can maintain network security. However, relying solely on inscriptions to boost miners' income is unsustainable. Users need a more durable Bitcoin consumption and usage scenario. We believe that a decentralized Bitcoin Layer 2 network can introduce new narratives and applications, leading to sustainable Bitcoin consumption scenarios from the user's demand side: users will consume BTC to cross assets to Layer 2 and back, and transactions within

Layer 2 will also require BTC consumption. Scenarios in Bitcoin Layer 2 can not only continuously consume users' Bitcoin, thereby increasing miners' income, but also expand the usage scenarios of Bitcoin, thereby attracting more users to hold Bitcoin and helping to increase its price.

2. Inability to Manage On-Chain Assets on Bitcoin Network

The Bitcoin network needs Layer 2 more than Ethereum. Unlike Ethereum, the Bitcoin network cannot independently handle asset settlement issues. Ethereum's Layer 2 primarily addresses issues of expensive Layer 1 Gas and network congestion, while the primary issue that Bitcoin's Layer 2 needs to address is Turing incompleteness. Bitcoin's non-Turing complete on-chain virtual machine can only register assets, so a Turing complete Bitcoin Layer 2 is needed to settle issues related to assets issued on Bitcoin Layer 1. The continuously emerging Ordinals tokens on the Bitcoin network also lack utility and use cases, but Bitcoin Layer 2 provides sustainable use scenarios for these tokens. Users can enhance the playability and usability of Layer 1 assets through various financial platform tools on Layer 2.

3. Bitcoin Scalability Issues

Since its inception, Bitcoin's scalability has been a major concern due to several limitations in its network design, such as a 1MB block size, an average block generation time of 10 minutes, and bandwidth constraints. These limitations lead to transaction delays and increased costs during peak periods, impacting the efficiency of the entire system and the user experience. The 2017 Segregated Witness (SegWit) technology upgrade, which made more efficient use of block space and increased the network's capacity to a maximum of 4MB, also solved the transaction malleability issue. Additionally, the Lightning Network is considered an effective scalability solution, allowing users to conduct instant transactions off-chain, with transactions only recorded on-chain when channels are opened or closed, significantly improving transaction speed and efficiency.

However, although SegWit improved network scalability by increasing block capacity and resolving transaction malleability issues, these improvements are limited in addressing congestion during peak times. Furthermore, the peer-to-peer payment system and user-unfriendly design of the Lightning Network make it difficult for ordinary users to submit fraudulent proofs, lowering the cost for malicious nodes to act fraudulently. To further address Bitcoin's scalability issues, we believe Layer 2 is the most mature solution compared to others like SegWit and the Lightning Network.

II. Overview of Existing Bitcoin Layer2 Solutions

1. Vitalik's Early Proposals (2014). Back in 2014, developers, including the most notable Vitalik, proposed solutions to Bitcoin's Turing incompleteness and scalability issues. Vitalik initially aimed to build a Turing-complete VM for the Bitcoin network to enable it to execute more complex operations, especially smart contracts. However, due to concerns about network security and stability, the Bitcoin community was conservative about major changes to the core protocol, leading Vitalik to establish Ethereum.

2. Lightning Network. Following VB, the most famous Bitcoin Layer2 solution is the Lightning Network. Its goal is to enable "global payments" with Bitcoin, primarily facilitating rapid and convenient micropayments on this Layer2 network. However, the Lightning Network doesn't support smart contracts, hindering the development of Bitcoin-related ecosystem applications on it. Currently, about 4,000 BTC are staked on the Lightning Network. Also, the educational cost of submitting fraud proofs is high for non-developers, making it challenging to maintain asset security, thus limiting its widespread adoption.

3. Stacks. Positioned as Bitcoin's smart contract layer, Stacks mainnet launched in 2018. It uses a "pegging" approach for BTC cross-chain, essentially a centralized mapping method by issuing sBTC on the Stacks network. Its network gas is powered by its mainnet token STX, not BTC. Miners participating in Stacks network mining consume staked BTC to mine its network token, a design not conducive to winning support from the Bitcoin community. Its ecosystem has been developed for five years, but most projects are lackluster or stagnant, with the entire ecosystem's TVL currently under $25 million.

4. Rootstock (RSK). Positioned as a Bitcoin Layer2 supporting smart contracts, RSK uses Hashlock for BTC cross-chain, which is still a centralized method, making it challenging to earn trust from Bitcoin users. Consequently, the BTC quantity used for cross-chaining through RSK is minimal. Also, RSK's consensus algorithm is still POW, an inefficient consensus mechanism for a Layer2 network, hampering its ecosystem development. Despite launching in 2018, the Rootstock ecosystem has seen little to no growth.

5. Liquid. Launched by Blockstream, Liquid is essentially a Bitcoin sidechain serving mainly institutions and asset issuers. It provides asset issuance and circulation services based on the Bitcoin sidechain, targeting business clients. Therefore, Liquid's Bitcoin cross-chain solution is relatively centralized, using 11 certified multisig nodes for Bitcoin custody, similar to a consortium permissioned chain solution.

6. RGB. RGB aims to build a BTC Layer2 based on BTC UTXO and the Lightning Network. RGB’s core design involves UTXO state encapsulation, client-side validation, and bridging the Lightning Network to run non-shared smart contracts. Its most touted feature is encapsulating the core data running on RGB into every Bitcoin UTXO, leveraging the Bitcoin blockchain for asset security. However, this feature has not yet been realized, and even if implemented, RGB faces challenges in asset verification complexity and smart contract non-interactivity.

7. ChainX. The first Bitcoin Layer2 based on Substrate and WASM-compatible, ChainX once had over 100,000 BTC cross-chained. However, it uses an 11-person multisig scheme for Bitcoin asset custody, posing certain centralization risks.

8. BitVM (Proposed in 2023). BitVM, a BTC Layer2 solution, is still in the theoretical stage. BitVM's core logic involves running fraud proofs similar to optimistic rollups on BTC scripts. The smart contract layer operates off-chain, and each contract does not share state. BTC cross-chain uses traditional Hashlock for asset anchoring, not achieving truly decentralized BTC cross-chaining.

These existing Bitcoin Layer2 solutions have not adequately addressed three key issues: **a**. How to realize decentralized cross-chain from Bitcoin Layer 1 to Layer 2; **b.** Whether BTC Layer2 can gain consensus and support from Layer1 users; **c.** Whether BTC Layer2 is friendly enough for developers and users.

Hence, we created BEVM, an EVM-compatible, BTC-as-Gas, fully decentralized Bitcoin Layer2 solution. BEVM has made significant contributions to maintaining the BTC network's security, including increasing BTC consumption scenarios, providing new revenue sources for miners, and using Taproot technology for decentralized custody of user assets, enabling decentralized Bitcoin financial business scenarios.

III. Positioning of BEVM

BEVM is a decentralized and EVM-compatible Bitcoin Layer2 using BTC as Gas.

BEVM is based on technologies such as the Schnorr's signature algorithm and MAST contracts, brought about by the Taproot upgrade, allowing BTC to cross-chain from Bitcoin mainnet to Layer 2 in a decentralized approach. Since BEVM is EVM-compatible, it allows all DApps which can run in the Ethereum ecosystem to operate on BTC Layer 2. In this process, BTC can not only be used as Gas to run a Layer 2, but can also circulate to other EVM chains and new public chains via BEVM.

IV. Background of BEVM’s Inception

1. The SegWit Upgrade and Taproot Upgrade

The birth of BEVM is entirely based on Bitcoin's SegWit upgrade in 2017 and the Taproot upgrade in 2021. The SegWit upgrade allowed Bitcoin blocks to accommodate more data, while the Taproot upgrade not only enabled expanded spaces to hold more complex data but also introduced the Schnorr's signature algorithm. This made decentralized Bitcoin multi-signature a reality, thereby enabling decentralized Bitcoin cross-chain transactions. Ultimately, a decentralized BTC Layer2 became a reality, and BEVM is the prime example of such a decentralized BTC Layer2.

The SegWit and Taproot upgrades have made Bitcoin great again, evolving Bitcoin from the 1.0 era to the 2.0 era and allowing us to witness a more abundant Bitcoin ecosystem.

2. Explosion of Bitcoin Issuance Protocols like Ordinals in 2023

The surge of protocols like Ordinals in 2023, following the SegWit and Taproot upgrades, demonstrated the potential of issuing assets based on Bitcoin, necessitating a Layer2 for more extensive and richer ecosystem applications. Hence, we created BEVM.

3. Six Years of BTC Layer 2 Exploration by BEVM Team

Since 2017, the BEVM team has been exploring Bitcoin Layer2 solutions. Although ChainX, launched in 2018 by the BEVM team, achieved over 100,000 BTC cross-chain, it didn’t fully take off due to industry constraints. Post-Taproot upgrade in 2021, the team initiated the construction of BTC Layer2 based on these advancements. The explosion of Bitcoin issuance protocols like Ordinals in 2023 signaled a new era for the Bitcoin ecosystem, leading to the launch of the BEVM Canary network and plans for the mainnet release in Q1 2024.

V. Technical Framework and Solutions of BEVM

BEVM aims to break through two significant challenges: How to achieve decentralized BTC Layer 2; How to be compatible with EVM and its peripheral ecosystem using BTC as Gas.

1. How to achieve decentralized BTC Layer 2?

The biggest challenge with current existing Bitcoin Layer2 solutions is their inability to achieve decentralization. That is, they can't guarantee that users' Bitcoin can be decentralized bridged to Layer2; nor can they ensure that users' assets and data can be decentralized bridged back to the Bitcoin network.

1.1 How to Decentralized Bridge BTC and BTC-based Assets (such as #BRC20) to BTC Layer 2?

BEVM ensures the security and decentralization of assets from the Bitcoin network to Layer 2 by implementing a Bitcoin light node on BEVM.

1.1.1 Synchronizing the complete Bitcoin block headers to verify the certainty of BTC network data.

1.1.2 Synchronizing cross-chain related transactions and transaction Merkle proofs on BEVM to verify data accuracy.

The entire BTC light node data is implemented on BEVM and is confirmed by BEVM consensus. The data of the BTC light node is synchronized to the underlying account system of EVM, facilitating a decentralized interaction of data and assets from BTC to BEVM.

1.2 How to Decentralize Cross-Chain Assets and Data from BEVM to the Bitcoin Network?

Current Bitcoin Layer2 solutions mostly use private key sharding and multi-signature schemes, where the number of custodians in a multi-signature scheme doesn't exceed 15 people, and the amount of data required to be uploaded is vast and costly. Private key sharding might require a trusted central entity to coordinate the sharding process or provide initial security settings, with the risk of key leakage in a centralized server setup.

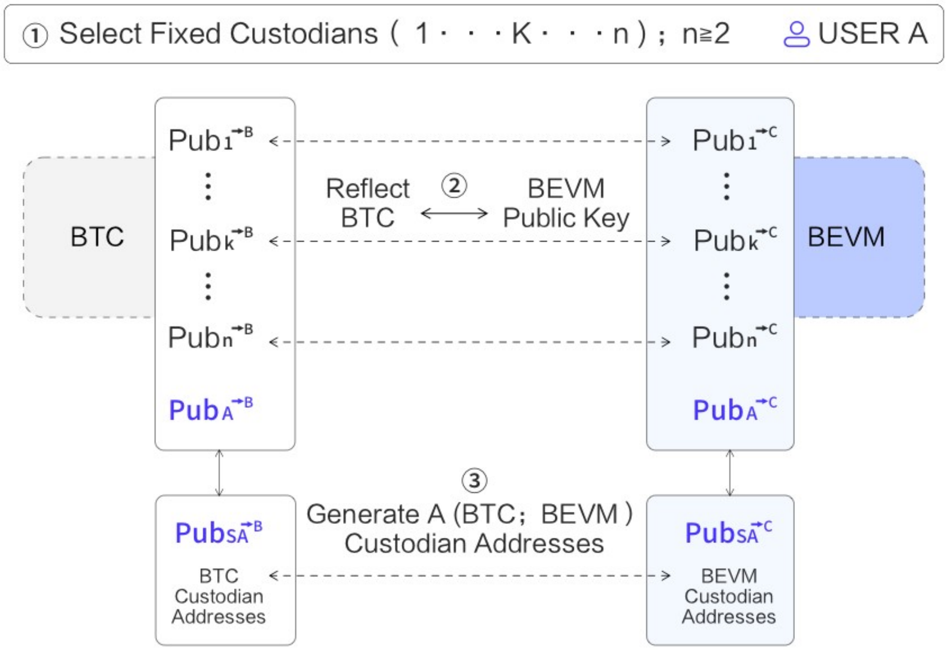
BEVM, however, utilizes Taproot technology and POS consensus nodes to achieve decentralized cross-chain of Layer 2 data and assets back to the Bitcoin mainnet.

1.2.1 POS consensus nodes on BEVM. Each POS consensus node on BEVM comes with three types of private keys: POS block generation key, POS management key, and BTC threshold signature key.

POS Block Generation Key: An online private key responsible for block generation and maintaining BFT consensus on BEVM's PoS network.

POS Management Key: An offline private key responsible for updating and replacing each of the three keys.

BTC Threshold Signature Key: Generated through Taproot technology (Schnorr + MAST contract), it comprises N threshold contract private keys responsible for managing assets and data interaction on the BTC network. These are selected through POS staking logic, with a maximum support of up to 1,000 nodes. Then, each POS consensus node sets its BTC Taproot threshold public key through a chain transaction, mapping their three public keys. Finally, the n consensus nodes form a ⅔ threshold custody contract, similar to the BFT consensus of the POS network.



1.2.2 How are transactions interacting on BEVM returned to the BTC network at layer1 for settlement?

Initially, users submit transactions on BEVM's EVM platform to cross back to the BTC network. Then, BEVM's n PoS consensus nodes use the BTC threshold custody contract for a more than 2/3 BFT vote. After passing the vote, a BTC Taproot transaction is generated and then submitted to the BTC network, completing the on-chain asset interaction.

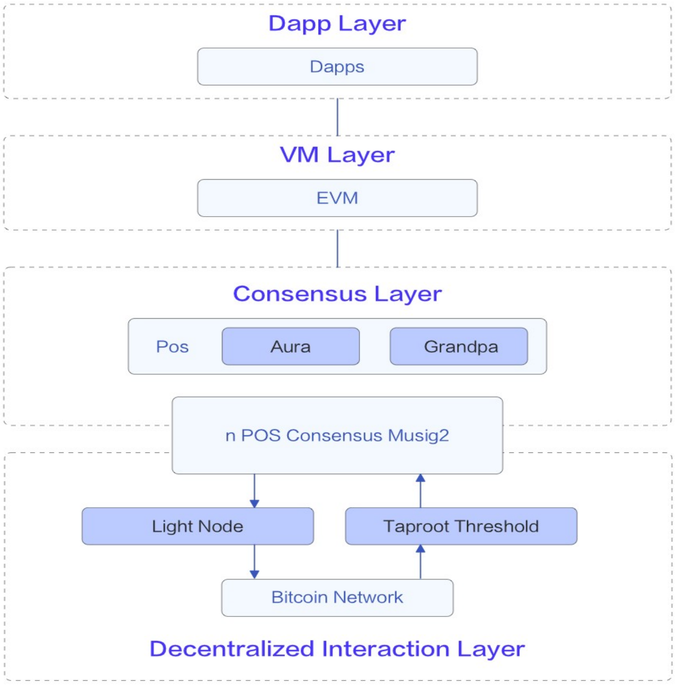
The cross-chain scheme of assets and data from BEVM back to the BTC mainnet combines BEVM's PoS consensus nodes and BTC's threshold signature custody contract. This ensures the security of BTC custody in a fully decentralized and secure manner, similar to BFT POS.

2. How to be compatible with EVM and its peripheral ecosystem using BTC as Gas?

2.1 Achieved through the use of the Substrate framework for EVM compatibility.

2.2 Hard-coding the logic of BTC as gas into the underlying bytecode of EVM.

BEVM Architecture



3. Overall Framework

Cross-Chain Interaction Layer: Through Bitcoin light nodes and a combined POS consensus of Taproot threshold contracts to realize decentralized interaction between Bitcoin and BEVM.

Consensus Layer: Through Aura consensus for round-robin block generation, and Grandpa for BFT consensus confirmation.

VM Layer: A fully EVM-compatible smart contract platform layer.

Dapp Layer: Supports various decentralized Dapp applications written in the Solidity language.

4. Future Technical Expansion

4.1 BTC deposited on BEVM will participate in BEVM's POS consensus staking to ensure that BEVM is securely controlled by the BTC mainnet.

Currently, BEVM forms its consensus layer through threshold contracts generated by nearly 1000 BTC Taproot accounts. We can further enhance this by increasing BTC's participation in Layer2 PoS staking to ensure the security of the Layer2 consensus layer is controlled by the BTC mainnet.

4.1.1 Parameter Settings

BEVM Capacity: Total market value of tokens participating in BEVM's POS governance.
BTC Capacity: Total value of Bitcoin hosted on BEVM.
BEVM Weights: Share weight of tokens participating in BEVM's POS governance in Staking.
BTC Weights: Share weight of Bitcoin hosted on BEVM in Staking.

4.1.2 Formula Algorithm

$BEVM\ Weights + BTC\ Weights = 1$

i) If $btc\ capacity = 0,\ bevm\ weights = 1$

ii) If $btc\ capacity/bevm\ capacity = \infty,\ bevm\ weights = 0$

iii) $btc\ weights = K * (btc\ capacity/bevm\ capacity) * bevm\ weights$

$btc\ weights = \alpha$

$bevm\ weights = \beta$

$btc\ capacity = a$

$bevm\ capacity = b.$

Hence:

If $a = 0, \beta = 1$

If $a/b = \infty, \beta = 0$

$\alpha + \beta = 1\ and\ \alpha/\beta = k * a/b$

4.1.3 Corresponding BTC Hosting Principles

According to this formula, the principle of corresponding BTC hosting is:

When the custodian BTC amount is much larger than the market value of BEVM governance tokens deposited in Validators, the network's security is guaranteed by the staked BTC.

When the market value of BEVM's governance tokens is significantly larger than the custodian BTC amount, the network's governance weight is secured by BEVM governance tokens.

Or, both BEVM governance tokens and BTC will be staked to maintain network security.

4.2 Compatibility and Future of zkSTARK Version Rollup

The zkSTARK rollup version is limited by BIPs, meaning the BTC core team needs to agree to integrate zkSTARK opcodes into the BTC core code. Then, PoW miners' machines, while compatible with BTC hash algorithm mining to ensure BTC consensus network security, can also perform complex zero-knowledge calculations. This allows BTC mining machines to achieve two goals at once: mining to ensure BTC network security and performing complex zero-knowledge calculations.

BEVM has already considered future compatibility with zkSTARK rollup, leaving an interface from the PoS consensus layer for future Bitcoin network upgrades. When new zero-knowledge BIPs are added, BEVM can upgrade immediately to remain the most secure and reliable BTC Layer 2.

VI. Design Philosophy of BEVM

BEVM's design philosophy focuses on essence, practicality, and implementation. The BEVM team believes that the essence of BTC Layer2 is a decentralized BTC cross-chain protocol plus a high-performance smart contract network. The goal of BTC Layer2's birth is to expand complex application scenarios that BTC Layer1 cannot achieve, enabling more developers and users to enter the Bitcoin ecosystem.

Therefore, the BEVM team believes that a practical Bitcoin Layer2 must meet the following three principles:

Whether BTC Layer2 can achieve decentralized BTC cross-chain.

Whether BTC Layer2 can gain support from the Bitcoin Layer1 community.

Whether BTC Layer2 can maximize the attraction of developers and users to the ecosystem.

Firstly, the first step for users to use BTC Layer2 is to cross BTC from the mainnet to Layer2. Therefore, whether the BTC cross-chain scheme can be decentralized becomes the most important standard. This determines the ecological scale and development ceiling of BTC Layer2, and even its life and death.

Secondly, if Bitcoin Layer2 wants to gain support from the Bitcoin Layer1 community, the core point is whether BTC Layer2 uses BTC as GAS. This means that the development of Bitcoin Layer2 can enhance the value of Bitcoin and bring benefits to various stakeholders in the Bitcoin community. Undoubtedly, with BTC as Gas in Bitcoin Layer2, its development is deeply linked to Bitcoin Layer1, naturally gaining support from the Bitcoin community.

Thirdly, the natural mission of Bitcoin Layer2 is to help expand the Bitcoin ecosystem. Therefore, to achieve this expansion, the first principle for Bitcoin Layer2 is to maximize the attraction of developers and users to the Bitcoin Layer2 ecosystem, enriching the Bitcoin ecosystem as much as possible. Thus, minimizing the entry barriers for developers and users is a fundamental principle BTC Layer2 should follow. If the design of Bitcoin Layer2 is too complex or sets high entry barriers for developers and users, it contradicts this principle, greatly increasing the difficulty of Bitcoin Layer2's success. It is well known that smart contract developers in the entire Crypto field have grown and strengthened in the EVM ecosystem. According to public data, in 2022, there were about 400,000 smart contract developers worldwide, with over 80% being EVM developers. Therefore, Bitcoin Layer2 should actively embrace EVM to attract excellent developers to build applications on Bitcoin Layer2, which is also a principle followed by BEVM.

Thus, BEVM's positioning is a decentralized Bitcoin Layer2 that uses BTC as Gas and is compatible with EVM.

VII. Vision and Market Space of BEVM

1. BTC EVM

BTC EVM is the primary vision of BEVM, building a decentralized BTC Layer2 compatible with EVM allows seamless deployment of various EVM ecosystem applications on BEVM, increasing Bitcoin usage and consumption scenarios. To better maintain Bitcoin network security, BEVM plans to launch “BEVM - Stack” to assist developers and Bitcoin projects with high throughput requirements in building their own BTC Layer 2.

2. BTC to VM

BEVM is planning to construct a Decentralized Bitcoin FX Protocol, a decentralized Bitcoin "foreign exchange system", introducing Bitcoin - the digital gold into any chain and ecosystem, enhancing the monetary credit of these public chains. Contrary to WBTC, which enables Bitcoin circulation within the EVM ecosystem but is backed by fully centralized institutions, ***DBFX*** Protocol allows native BTC to circulate across any chain, granting users true ownership of their Bitcoin assets across various blockchains.

Based on these visions, BEVM's future market space is estimated to be over $150 billion with 20% of BTC introduced into Layer2, and over $300 billion with 40% of BTC integrated into other chains.

VIII. The Competitive Barriers of BEVM

1. Six Years of Technical Accumulation in the BTC Layer2 Track by the BEVM Team

Since 2017, the BEVM team has been pioneering in the BTC Layer2 direction. The ChainX launched six years ago achieved a cross-chain of 100,000+ BTC. Over the past six years, they have focused on every major upgrade of BTC, integrating a series of Bitcoin technological innovations into the practice of BTC Layer2. They have combined technological innovations like the Musig2 signature and Mast contracts from the Taproot upgrade with Bitcoin light node technology, ultimately launching the truly decentralized BTC Layer2 — BEVM. The BEVM team has six years of practical experience and technical accumulation in the BTC Layer2 track, which is not merely theoretical but has created a significant recognition and technical barrier in the global BTC Layer2 track.

2. BEVM's Canary Network is Already Online, with a Nascent Ecosystem

Unlike many projects that are still in the white paper stage, BEVM has already launched its Canary Network, and the mainnet is ready to be launched at an opportune time. During the 10-month Canary Network phase, various types of projects will gradually emerge in the BEVM ecosystem, including but not limited to: BTC-based stablecoins, lending, DEX, cross-chain bridges, BTC derivative protocols, NTF, GameFi, LaunchPad, etc.

3. BEVM - Stack and DBFX Protocol

BEVM - Stack is an advanced and highly customizable blockchain technology architecture planned by the BEVM project for future implementation. It aims to provide developers with an efficient, cost - effective way to deploy Bitcoin Layer 2 solutions. This framework will allow a broader range of projects to fully benefit from the security of the Bitcoin network consensus and the convenience of deploying applications on the EVM, thereby increasing Bitcoin's usage and consumption scenarios and better maintaining Bitcoin network security. Additionally, Bitcoin ecosystem projects can also build specialized Layer 2 solutions with their project tokens as Gas, such as creating Layer 2 with $SATS or $ORDI as Gas. They can even develop Layer 2 solutions using Taproot Assets or Lightning Network assets as Gas. The key features of BEVM - Stack include.

- **Modular Architecture.** The core characteristic of BEVM - Stack is its modular design, allowing each component to be independently upgraded and optimized without compromising network security.
- C**ross-Chain Interoperability.** By integrating a variety of blockchain technologies, BEVM - Stack facilitates interconnectivity and data sharing between different blockchains. It also promotes the free circulation of native BTC and BTC-based assets across various chains built on BEVM - Stack.
- **Shared Consensus Mechanism**. The shared consensus mechanism of BEVM - Stack ensures decentralization and security of the network, while also providing atomic-level cross-chain operation capabilities. This enhances collaborative work between different chains.

- **Future Adaptability**. BEVM - Stack is designed to accommodate future blockchain technology developments, such as the integration of zkSTARKs, ensuring it remains competitive in an evolving technological landscape.

The DBFX Protocol is a decentralized Bitcoin foreign exchange protocol designed to enhance the application and circulation of Bitcoin across various blockchain environments. Its main features include,

- **Decentralized Bitcoin 'Foreign Exchange System'**. The DBFX Protocol creates a decentralized Bitcoin trading platform, enabling Bitcoin to freely circulate across different blockchains.
- **Native Bitcoin Assets.** The DBFX Protocol allows the native BTC to circulate freely across various chains, eliminating the need for Wrapped BTC backed by centralized institutions.
- **Enhancing Bitcoin's Value and Application Scenarios.** The DBFX Protocol not only improves the practicality of Bitcoin but also expands its application range and value within the blockchain ecosystem.

IX. Conclusion

BEVM, as the first Layer2 platform fully compatible with EVM and utilizing Bitcoin as gas, represents not only a technological breakthrough but also a redefinition of Bitcoin's value. Combining Taproot, Bitcoin light nodes, Aura + Grandpa consensus, and EVM, BEVM has significantly broadened Bitcoin's application and consumption scenarios. It brings unparalleled opportunities to Bitcoin miners and developers while injecting new vigor into the entire cryptocurrency field.