BTC Layer2 Whitepaper

A Blockchain Compatible with EVM for Decentralized Computing

Oct 25, 2023
BTC Layer2 Team

https://ligo.network

0. Preface

Since 2023, with the rise of Ordinals theory, the BTC ecosystem has regained user attention. A large number of users have begun to return to the BTC ecosystem, leading to a sharp increase in transaction volume on the BTC chain. Subsequently, based on the Ordinals theory, some innovative protocols along with relevant products have appeared on the Bitcoin network. These include BRC-20, Bitcoin NFT, BIP300, Brc-20 dex, etc. The innovation of these protocols has ultimately extended to the Bitcoin network, creating unlimited potential for the future development of the Bitcoin ecosystem.

However, as we all know, the Bitcoin network has certain issues, such as poor scalability, high transaction fees, and the absence of a Turing Complete virtual machine, among others. Besides the inherent problems of Bitcoin, the greatest issue with BRC-20 and other new Bitcoin protocols is their centralization. They rely on the computation and indexing of centralized servers. These new Bitcoin protocols exhibit disadvantages such as being centralized, susceptible to censorship, private, and unverifiable, among other issues. It is currently impossible to build a completely decentralized Web3 application based on the present state of the BTC chain. There is an urgent need to expand Bitcoin protocols in a decentralized manner and build a decentralized infrastructure for a new era of Bitcoin.

At this time, BTC Layer2 has been created. BTC Layer2's vision is to build a truly decentralized infrastructure for the Bitcoin ecosystem. This will enable all Bitcoin-based Web3 applications to run quickly, efficiently, and safely on BTC Layer2 in a decentralized manner, without relying on a centralized server. Most importantly, BTC Layer2 is compatible with the EVM and the DeFi ecosystem on Ethereum. This compatibility will afford BTC Layer2 great scalability and impressive liquidity.

The goal of BTC Layer2 is to address the centralization of the current Bitcoin extension protocols, such as BRC-20, as well as the poor scalability, high transaction fees, and the absence of a Turing Complete virtual machine in the Bitcoin network itself. BTC Layer2 will implement the EVM to enhance Bitcoin's scalability. It aims to run Bitcoin L2 in a decentralized, cost-efficient, effective, and Turing Complete manner, which will help Bitcoin build a much larger decentralized ecosystem and attract more users to participate. BTC Layer2 intends to allow the currently popular protocols like Inscriptions, Ordinals, BRC-20, Bitcoin NFT, ORC-20, and others to obtain decentralized support, eliminating the need for the assistance of centralized mechanisms off the Bitcoin network. This approach is much safer and more reliable.

BTC Layer2 is a safe, fast, smart, and low-cost Bitcoin L2 blockchain based on EVM, built by Bitcoin developers for Bitcoin developers. Its goal is to establish a large Bitcoin decentralized ecosystem encompassing DeFi, NFT, GameFi, SocialFi, and more, using EVM and smart contracts, and capable of supporting more than 10,000 transactions per second (TPS).

This whitepaper focuses on BTC Layer2 V1. This version will perform computations for various protocols extended from the Bitcoin network in a decentralized, safe, and reliable manner. It will parse the computational results into

BTC Layer2's Merkle Tree and smart contracts to provide query and verification services. Furthermore, it aims to become the decentralized infrastructure for various ecosystem projects based on new Bitcoin protocols.

This whitepaper focuses on introducing BTC Layer2's technical principles. The following chapters will present BTC Layer2 from the perspectives of Current Problems, Design Philosophy, and Underlying Architecture.

1. Problems of Bitcoin Network

Bitcoin, as the world's first and largest blockchain and cryptocurrency, has very high decentralization and security. However, there are still some problems that make it hard for Bitcoin to accelerate mass adoption.

1.1 Poor Scalability

As a Layer 1 blockchain, Bitcoin has high decentralization and security, but this high level of decentralization leads to low scalability, slow block generation, and high latency. A well-established, effective Bitcoin L2 is needed to solve the scalability problem.

1.2 No Turing Complete Virtual Machine

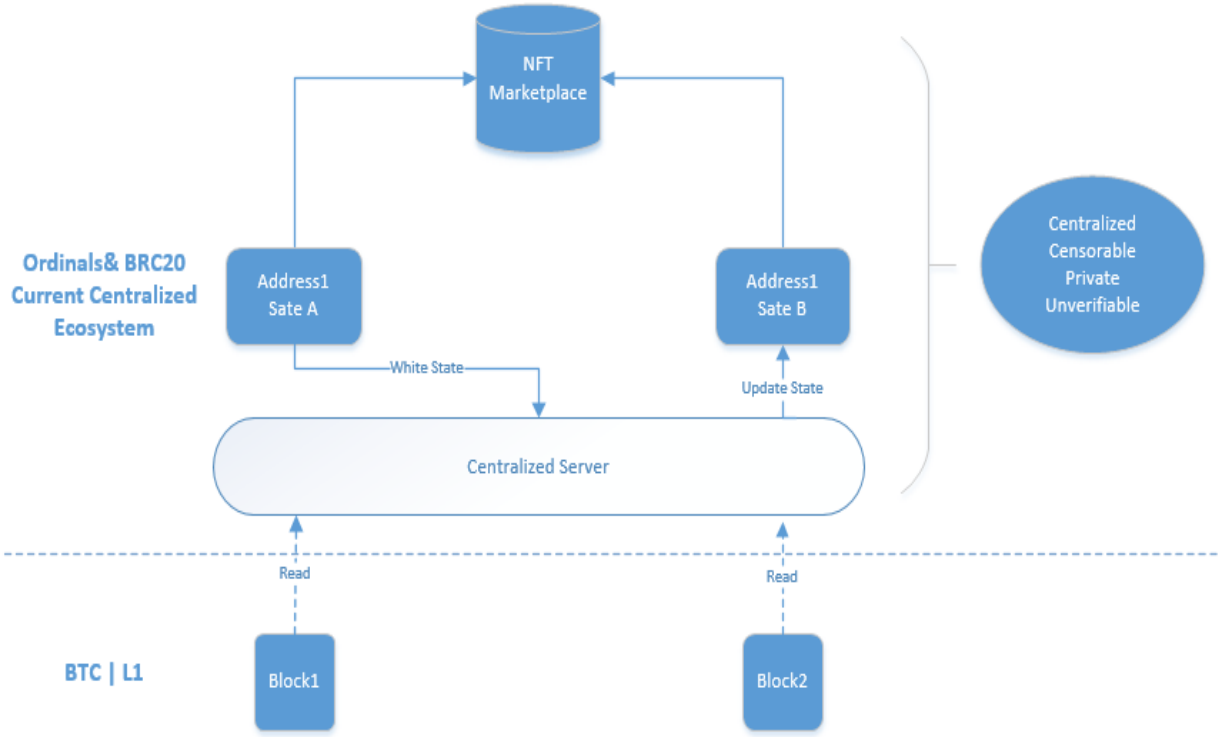
Bitcoin transactions are based on Bitcoin Script, which is a stack-based programming language for locking and unlocking transactions. However, Bitcoin does not support a Turing Complete virtual machine, which has hindered the development of the Bitcoin ecosystem to some extent. The flourishing ecosystem projects on Ethereum are facilitated by the virtual machine and smart contracts.

1.3 High Transaction Fee

The ecosystem prosperity brought by Bitcoin protocols such as BRC-20 and the continuous rising of BTC prices have pushed up the transaction fee on Bitcoin network, and provided resistance to further expansion of Bitcoin ecosystem.

1.4 Centralization Risk of new Bitcoin Protocols

New Bitcoin protocols such as Ordinals and BRC-20 have spurred the prosperity of the Bitcoin ecosystem, opening up limitless potential for its growth. However, the Bitcoin network does not verify these new protocols but merely stores them. In addition, a centralized server outside the Bitcoin network is needed to complete the cycle of these new protocols. For instance, the Ordinals theory's mechanism for numbering Satoshis operates on a centralized server according to fixed rules, and the Bitcoin network neither stores nor knows any relevant information about Ordinals. Although the BRC-20 protocol records its content on the Bitcoin network, its correctness has not been verified by the network. As a result, it also requires a centralized server outside of Bitcoin to carry out computation and indexing. The risks associated with a centralized server are obvious. Different application providers use their own logic to compute for protocol services. The likelihood of censorship, bugs, delays, and other problems is high, which contradicts the decentralized principles of blockchain and Web3.



The Situation of Current BTC Innovations

2. BTC Layer2 Design Philosophy

BTC Layer2 is built according to a strong design philosophy: Decentralization, EVM Compatibility and Sustainability. It's important to fully understand these principles as they guide the design of BTC Layer2.

2.1 Decentralized

Decentralized is the most important factor for blockchain to survive, be recognized and pursued by the whole world, is the foundation of safe and censorship resistance. BTC Layer2 always adheres to the concept of decentralized, provides the decentralized support for the current and future Bitcoin protocols to improve the Bitcoin infrastructure. BTC Layer2 is one of the first Bitcoin L2 Blockchains which supports decentralized computing for new Bitcoin protocols, and will become the decentralized infrastructure for all Bitcoin ecosystem protocols.

2.2 EVM Compatibility

BTC Layer2 is based on the EVM, which has been implemented on Ethereum and has achieved substantial success. We believe that BTC Layer2, as one of the earliest and most potent Bitcoin L2 solutions globally, will definitely establish a larger ecosystem and will have an even brighter future.

Simultaneously, we believe that the limitations of the Bitcoin ecosystem will inevitably undergo significant changes with the development of BTC Layer2 and various protocols such as BRC-20, BIP300. We also believe that the Bitcoin ecosystem will surpass all existing blockchains, including Ethereum. The development of BTC Layer2 will greatly benefit Bitcoin developers, users, and protocols.

2.3 Sustainability

BTC Layer2 adheres to the principle of sustainability. The initial design of BTC Layer2 maintains a very open stance, capable of supporting existing Bitcoin protocols, their extensions, and future Bitcoin protocols. We aim to keep the code design as simple as possible so that more developers can contribute to BTC Layer2. We will maintain compatibility with existing protocols and tools, such as geth, to minimize barriers for developers and users within the BTC Layer2 ecosystem. This approach allows more individuals to focus on the applications themselves rather than spending a substantial amount of time adapting to BTC Layer2.

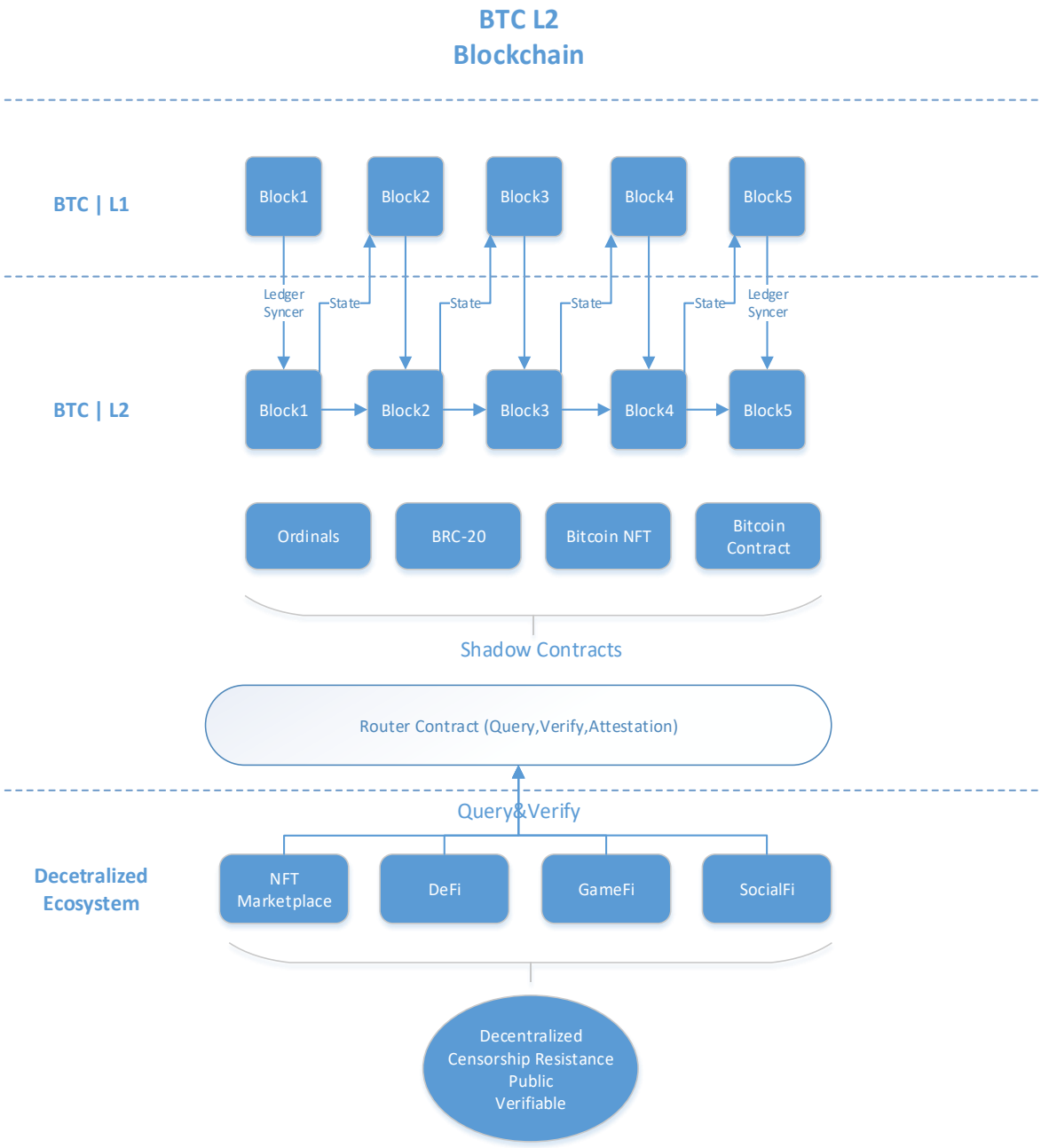
3. BTC Layer2 Architecture

BTC Layer2 Blockchain = Bitcoin + RPPOM Consensus + EVM

BTC Layer2 is a Bitcoin L2 Blockchain based on EVM. It moves the computation of new Bitcoin protocols, such as BRC-20, to L2, making it a decentralized computing chain for Bitcoin. As a Bitcoin L2, BTC Layer2 operates as a blockchain that utilizes the RPPOM (Random Pool Proof of Multi-properties) decentralized consensus algorithm. This stochastic multi-asset equity pledging consensus algorithm allows decentralized mining pools to operate. The computation results are then stored as Merkle Trees and smart contracts, and the block state is finally written into the Bitcoin block as a witness to complete block generation. Validators are responsible for challenging the correctness of the block, submitting fault proofs for problematic blocks, and obtaining challenge rewards.

BTC Layer2 will completely alter the centralized dependence of new protocols such as BRC-20, becoming the decentralized computing chain for Bitcoin and serving

as the decentralized infrastructure for all ecosystem decentralized applications, such as NFT marketplaces, DeFi, GameFi, and SocialFi on Bitcoin.



LIGO BTC Layer2 Diagram

3.1 Consensus

BTC Layer2 combines the EVM and RPPOM consensus algorithm to actualize a decentralized Bitcoin L2. This chapter will explain the RPPOM consensus and the three roles within the ecosystem: Senator, Citizen, and Tourist.

3.1.1 RPPOM Consensus

According to the RPPOM consensus mechanism, the BTC Layer2 network produces a block every 5 seconds, significantly improving transaction confirmation speeds. This efficiency is evident when compared to BTC, which produces a block every 10 minutes. Thus, the performance of a BTC asset transfer or trade on the BTC Layer2 network is approximately 120 times faster than that on the BTC network. RPPOM's theoretical TPS (transactions per second) reaches 10,000, sufficient to handle high-load transactions across multiple chains.

The server and network requirements for BTC Layer2 are less demanding, more adaptable, and can easily interface with other blockchains. Furthermore, the BTC Layer2 generation node is randomly selected from all Candidate Citizens who meet the pledging requirements. This selection process randomizes the generation nodes, making them difficult to target, thereby greatly mitigating the risk of network attacks. Even a complete attack on partial nodes won't affect the stability of the entire network.

There are three roles in BTC Layer2: Senator, Citizen, and Tourist. The system will have 15 fixed Senators, all with identical permissions but different categories. Five of them will form the House of Lords, and the remaining 10 will form the House of Commons. By utilizing BTC's native multiple signatures (16 out of 15), the Senator uses valid 11/15 signatures to ensure the security of incoming assets, thus guaranteeing decentralization and regulation.

We will first outline the details here:

Let R, = Zx]/f(),where f(x)is a polynomial of degree n. The public parameter is A% e R!x(m-1)andis used to commit to a scalar message m C Dom C , where Dom is a domain of that message, asfollows: Com,.(m, S) = A% • S + m. The properties of the homomorphic operations are also defined as:

Coma(my, S) Coma(mz,)= Coma(m, S)+ Coma(mS)mod q=Coma:(mi +m2S +S)mod qComa(mi, S)

Coma;(mz, S)= Coma(m, S)- Coma(m,S) mod q= Coma(m - m2,S-S)modq

wherem;, m, E R, areringelements and S, S e R-xl are (m - 1)-dimensionalvectors ofringelementsThe integers m;, m, E Z are encoded in binary as coeficient vectors m, = (m;o .., m;-0,...0) e (0,l)' (my 2') with m;y e {0,1} and j e{0,1}.

3.1.2 Senator

A Senator is an asset manager and community administrator in the L2 ecosystem. By consensus, the Senator is responsible for managing assets on hot and cold multisignature addresses on different chains. The cross-chain interconnection must ultimately be conducted through the Senators' consensus. To become a Senator, a user must pay a certain amount of $LIGO tokens, ensuring a significant financial stake is placed in the system. This financial stake safeguards the network's integrity and stability by aligning the Senators' interests with that of the network. The change of Senator is determined by Citizen votes. By pledging, Citizens are selected to produce blocks and obtain block rewards. Tourists can also participate in mining and receive mining rewards by pledging assets with Citizens. According to the RPPOM consensus mechanism, after new blocks are generated, the system will automatically follow the underlying protocol and distribute rewards to citizens and their supporters (users who pledged their assets with Citizens), according to their weighting.

3.1.3 Citizen

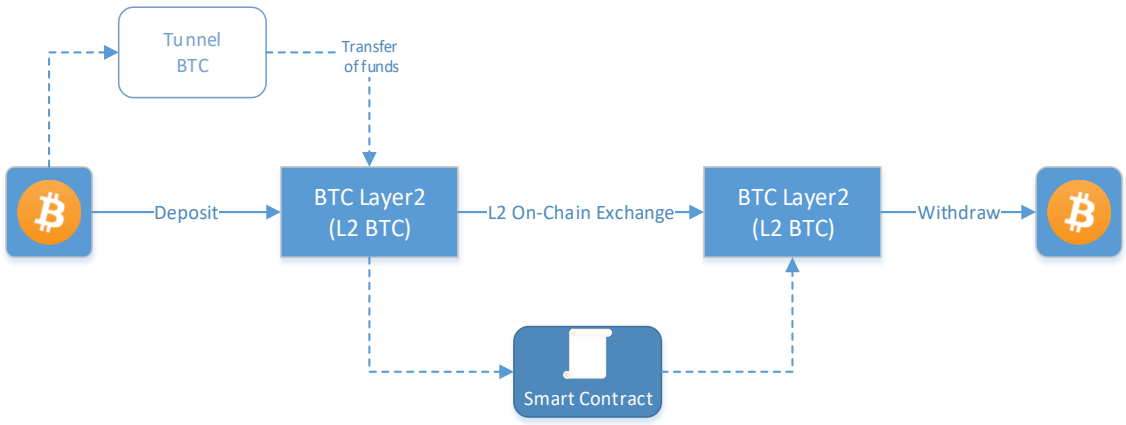
A Citizen can be understood as an on-chain mining pool that requires the installation of full node services to gain relevant weights through asset voting. The higher the weight, the greater the probability of obtaining blocks, and there will be rewards for block generation.

3.1.4 Tourist

A Tourist can pledge transferred assets to a Citizen to obtain relevant rewards. If the pledged Citizen successfully issues a block, profits will be obtained based on the proportion of the pledge, with Citizen's handling fees being deducted.

3.2 Bitcoin L2 Contract

For Bitcoin have better computing capability, BTC Layer2 will support smart contract inscribed on Bitcoin by inscriptions or other methods. The smart contract is saved on Bitcoin, executed and verified in BTC Layer2's EVM, which will make Bitcoin have virtual machine to execute smart contract and computing capability like many chains such as Ethereum. Then finally the Bitcoin will have the technical infrastructure: EVM to build complex decentralized applications like DEX, DeFi, GameFi, etc. Cross-chain process example diagram:



3.3 Merkle Tree

Bitcoin uses a Transactions Merkle Tree to save all the transactions of a block. Similar to Bitcoin's Transactions Merkle Tree, BTC Layer2 will use additional Merkle Trees: the State Merkle Tree, the Ordinals Merkle Tree, the Transaction Merkle Tree, and the Receipt Merkle Tree. These will save the computed results from the Computing Engine, and will be used for decentralized query and verification.

3.4 Router Contract

The Router Contract is a smart contract that stores the metadata of all Bitcoin protocols and provides external query and verification services for BRC-20 and other protocols. The Router Contract matches a user's request to the corresponding shadow contract or Merkle Tree to complete the final query or verification. In the future, the BTC Layer2 DAO will decide whether to charge $LIGO token as a protocol fee and how to use the fee, such as distributing it to the Sequencer or burning it, etc.

3.5 Merkle Proof

For new Bitcoin protocols such as BRC-20, the BTC Layer2 computing engine will compute and save the Merkle Proof to verify the new protocol state. This is very important, as the state of all new protocols is verifiable, and the verification is based on BTC Layer2's decentralized nodes, using immutable Merkle Tree technology.

3.6 Threshold Signature

The team will upgrade to Threshold Signature in the second R&D phase for catering future ecosystem expanding.

4. Decentralized Ecosystem based on BTC Layer2

BTC Layer2 will establish a robust decentralized ecosystem for Bitcoin, using the EVM and smart contracts. The current Bitcoin ecosystem projects based on new Bitcoin protocols, such as NFT marketplaces, need to be supported by centralized servers, which are centralized, censorable, private, and unverifiable. The ecosystem built on BTC Layer2, a decentralized infrastructure based on Bitcoin, will be entirely decentralized, resistant to censorship, open, and verifiable. It's time to participate in the decentralized Web3 ecosystem based on Bitcoin and BTC Layer2.

5. BTC Layer2 Tokenomics

This economic model is an experimental one, aimed at rapidly building community enthusiasm for the project, launching BTC L2, and significantly enhancing the liquidity of Bitcoin ecosystem assets.

Our BTC L2 is based on a dual-token model designed around BRC-20 assets. The plan is as follows: We use $LIGO and $SATS as our tokens:

1. $LIGO for governance (a governance token that gives holders voting rights, incentives, and staking rewards);
2. $SATS for utility (a utility token that pays for gas fees and enables fast and cheap transactions on the layer2 network. $SATS will be abundant, inexpensive, and sufficiently circulated). The value of our tokens is backed by Bitcoin as an asset.

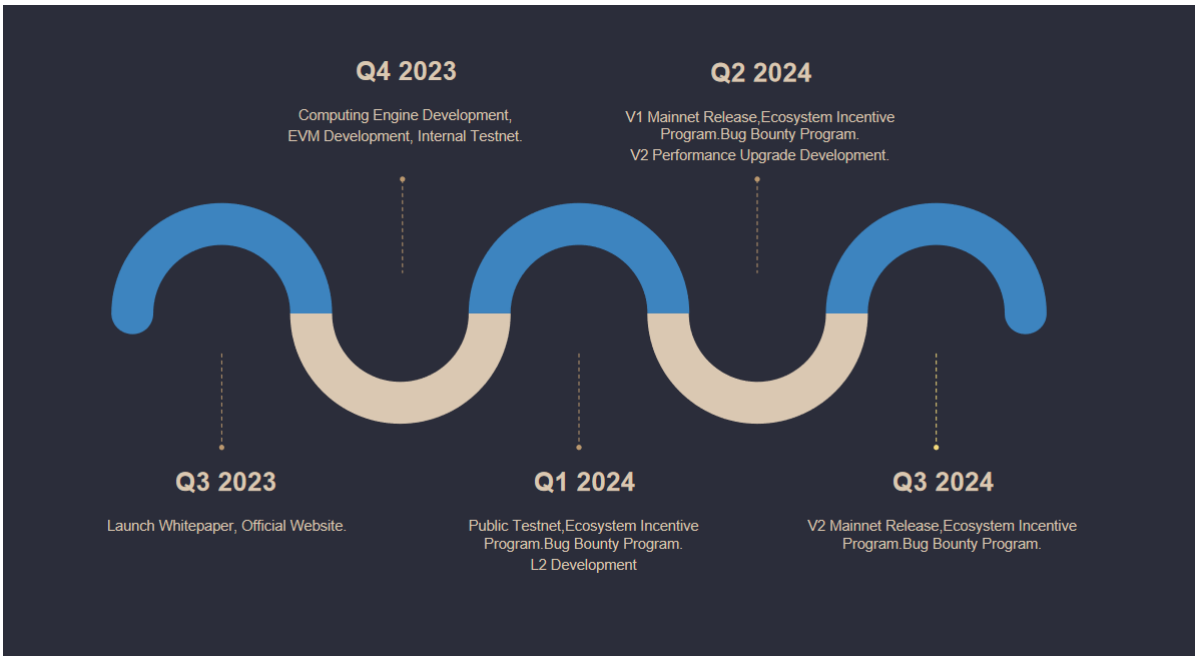
1) The success of BTC L2 is a success of consensus, which correspondingly enhances asset liquidity. We leverage the advantages of the existing BRC-20 token $SATS, which already has nearly 46,000 holders and a quantity advantage of 2100 trillion, to build a leading, truly decentralized ecological project for BTC layer2.

2) $LIGO already issued 1Trillion tokens on BRC-20, distributed to community for free mint, to gain community operational resources and enthusiasm. **Ligo is expected to be listed in 2-3 months' time following its release. With over 10,000 organic Web3 users, the future of the BTC ecosystem looks promising and potentially fruitful.**

We set $LIGO to be fixed and deflationary, creating scarcity and value growth, and set $SATS to be dynamic and inflationary, adapting to the network's needs and usage. We also incentivize our users and supporters to participate in our project through the distribution and rewarding mechanisms of $LIGO

6. BTC Layer2 Roadmap

BTC Layer2 Blockchain will have 5 main phases, The Roadmap details are shown in the figure below.



7. Reference

[1] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/ bitcoin.pdf. Oct 2008

[2] Vitalik Buterin. Ethereum White Paper : A Next-Generation Smart Contract and Decentralised Application Platform. https://github.com/ethereum/wiki/ wiki/White-Paper.

[3] Bonneau, J., Clark, J., Felten, E., Kroll, J., Miller, A. and Narayanan, A. 2014. Mixcoin: Anonymity for Bitcoin with Accountable Mixes. In Financial Cryptography.

[4] Maxwell, G. 2013. Coinjoin: Bitcoin privacy for the real world. Bitcoin forum thread. https://bitcointalk. org/index.php?topic=279249.0.

[5] Chiesa, A., Garman, C., Miers, I., Virza, M., Ben-Sasson, E., Green, M., and Tromer, E.2014. Zerocash: Practical decentralised anonymous e-cash from bitcoin. In IEEE Symposium on Security and Privacy (S&P).

[6] Miers I., Garman C., Green M., and Rubin A. 2013. Zerocoin: Anonymous distributed e-cash from bitcoin. In IEEE Security and Privacy (S&P), pages 397{411, 2013.

[7] Torres, W. A. A., et al. Post-Quantum One-Time Linkable Ring Signature and Application to Ring Confidential Transactions in Blockchain (Lattice RingCT v1. 0). Cryptography ePrint Archive Version. 61

[8] Noether, S. (2015). Ring SIgnature Confidential Transactions for Monero. IACR Cryptology ePrint Archive, 2015, 1098.

[9] Bünz, B., Bootle, J., Boneh, D., Poelstra, A., Wuille, P., & Maxwell, G. (2017) Bulletproofs: Short Proofs for Confidential Transactions and More. IACR Cryptology ePrint Archive, 2017, 1066.

[10] HOFFSTEIN J, PIPHER J, SILVER MAN J H. NTRU: A ring - based public key cryptosystem.

[11] LYUBASHEVSHY V, PEIKERT C, REGEV O. On ideal lattice and learning with errors over rings

[12] Ordinals.com, Ordinal Theory Handbook,https://docs.ordinals.com/

[13] Domo, Brc-20,https://domo-2.gitbook.io/brc-20-experiment

Note: Before the system was upgraded to BTC Layer2, the consensus algorithm ran live and was 100% secure with a TVL of 130M USD.

RPPOM possesses an extremely high level of system security, sufficient to defend against various malicious attacks and unexpected situations, ensuring the safety of the network and assets. We can also guard against the following extreme scenarios:

1. The Citizen plays a crucial role in maintaining system stability. Suppose a randomly selected portion of Citizens doesn't work; as long as not all of the selected 25 Citizens are inactive, it won't affect the chain's stability. As long as one of the 25 selected Citizens is online, it can produce 25 consecutive blocks. In such an extreme abnormal situation, relying on the chain's incentives can still transition to the next adjustment round. Under normal circumstances, if a Citizen fails to produce a block consecutively 5 times, their participation rate will be reduced. The participation rate will decrease the Citizen's staked asset amount in a coefficient manner, with the formula being: Final Staked HX Amount by Citizen = User Staked HX Amount x Participation Rate (0~100%). Therefore, all Citizens will eventually be high-quality nodes, and the above extreme scenario is unlikely to occur in real-world settings.

2. Suppose a Citizen maliciously produces two different blocks at the same time. Subsequent Citizens will continue to produce blocks based on the order they received. When the block production round ends, HyperExchange will automatically switch based on the length of the two chains, choosing the longer one. In such a scenario, ensuring a confirmation count of 17 blocks can prevent double-spending attacks.

3. Suppose a mining pool occupies many resources on the chain but less than 51%. In this scenario, even if the mining pool's asset allocation is perfect, it cannot guarantee that it will have more than 50% of the block producers in each round. Therefore, based on a confirmation count of more than 17 blocks, it's challenging to execute a double-spending attack.

4. Suppose mining pools collectively occupy more than 51% of the resources. In this extreme scenario, the mining pools could potentially cause a data rollback on the chain. However, the assets of the mining pools are not just HX but also many HIOUs, which are managed by Senator consensus. If mining pools collude maliciously, they will face the following situations:

(1) The participation rate of all mining pools involved in the malicious act will be reduced to 0% (meaning no matter how much they stake, it's equivalent to zero).

(2) The HIOUs staked by the mining pool will be frozen and restricted. Whether they are unfrozen depends on the impact caused.

Malicious actions mean that mining pools will face the loss of registration fees and their HIOUs staked in the pool. Users supporting that mining pool will need to enter an appeal process, with the Senator consensus deciding whether to unfreeze the user's assets.

In conclusion, under the protection of the RPPOM consensus mechanism, the potential benefits and risks faced by Citizens acting maliciously are not advantageous.