Biop V1 Whitepaper

Biop V1: Bitcoin L2 Blockchain based on Optimistic Rollup Protocol for Decentralized Computing

July 17, 2023
Biop Team
https://biop.io/

0. Preface

At the beginning of 2023, based on Bitcoin's SegWit and Taproot upgrade, Ordinals theory was released. Ordinal theory concerns itself with Satoshis, giving them individual identities and allowing them to be tracked, transferred, and imbued with meaning. Individual Satoshis can be inscribed with arbitrary content, creating unique Bitcoin-native digital artifacts that can be held in Bitcoin wallets and transferred using Bitcoin transactions. Inscriptions are as durable, immutable, secure, and decentralized as Bitcoin itself. Then based on Ordinals theory, some innovative protocols appeared on Bitcoin network, represented by BRC-20, Bitcoin NFT and ORC-20, the innovation of the protocols finally extended to the Bitcoin network, creating unlimited imagination space for the future development of Bitcoin ecosystem.

However, as we all know, Bitcoin network has some problems, such as: poor scalability, high transaction fee, and no Turing Complete virtual machine, etc. Besides the problems of Bitcoin itself, the biggest problem of BRC-20 and other new Bitcoin protocols is: centralized, relying on the computing and index of centralized servers. The new Bitcoin protocols have the disadvantages of centralized, censorable, private, and unverifiable, etc. It is impossible to build a completely decentralized Web3 application based on them. And it is urgent to expand Bitcoin protocols in a decentralized way and build decentralized infrastructure for a new era of Bitcoin.

At this time, Biop is created. Biop's vision is to build a truly decentralized infrastructure for Bitcoin ecosystem, so that all Bitcoin-based Web3 applications can be running fast, efficiently and safely based on the Biop in a decentralized manner, do not rely on the centralized server.

The goal of Biop is to solve the centralization of the current Bitcoin extension protocols like BRC-20, as well as poor scalability, high transaction fee, and no Turing Complete virtual machine of the Bitcoin network itself. Biop will implement the Optimistic rollup protocol to expand the scalability of Bitcoin, will run Bitcoin L2 in a decentralized, low-cost, efficient, Turing Complete manner, will help Bitcoin build a much larger decentralized ecosystem and attract much more users to participate. Biop will make the current popular Inscriptions, Ordinals, BRC-20, Bitcoin NFT, ORC-20 and other protocols to obtain decentralized support, and no longer require the support of centralized mechanism off the Bitcoin network, which is much safer and more reliable.

Biop is a safe, fast, smart and low-cost Bitcoin L2 blockchain based on Optimistic rollup protocol built by Bitcoin developers, for Bitcoin developers. To establish a large Bitcoin decentralized ecosystem like DeFi, NFT, GameFi, SocialFi... by BVM and smart contract.

Biop will have 3 versions, all of which are Bitcoin L2 Blockchain based on Optimistic rollup protocol. The first version V1 will focus on solving the centralized problem of Bitcoin protocols such as Ordinals and BRC-20, and will build a decentralized computing L2 blockchain for Bitcoin; V2 will implement the interactive operation of BRC-20 and other protocols based on V1, and will become a complete Bitcoin L2 blockchain, with more than 10,000 TPS, second-level block generation time, based on Bitcoin's decentralization, security, and liquidity; V3 will integrate Ethereum L2, become the world's first L2 Blockchain based on both Bitcoin and Ethereum, share the security, decentralization and liquidity of Bitcoin and Ethereum, establish a super-large ecosystem.

This whitepaper focuses on Biop V1, which will complete the computing for various protocols extended from the Bitcoin network in a decentralized, safe, and reliable manner, will parse the computing results into Biop's Merkle Tree and smart contract to provide query and verification service, and will become the decentralized infrastructure for various ecosystem projects based on new Bitcoin protocols.

1. Problems of Bitcoin Network

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

1.1 Poor Scalability

As a Layer 1 blockchain, Bitcoin has high decentralization and security, but high decentralization leads to low scalability, slow block generation, and high latency. A good Bitcoin L2 is needed to solve the scalability problem.

1.2 No Turing Complete Virtual Machine

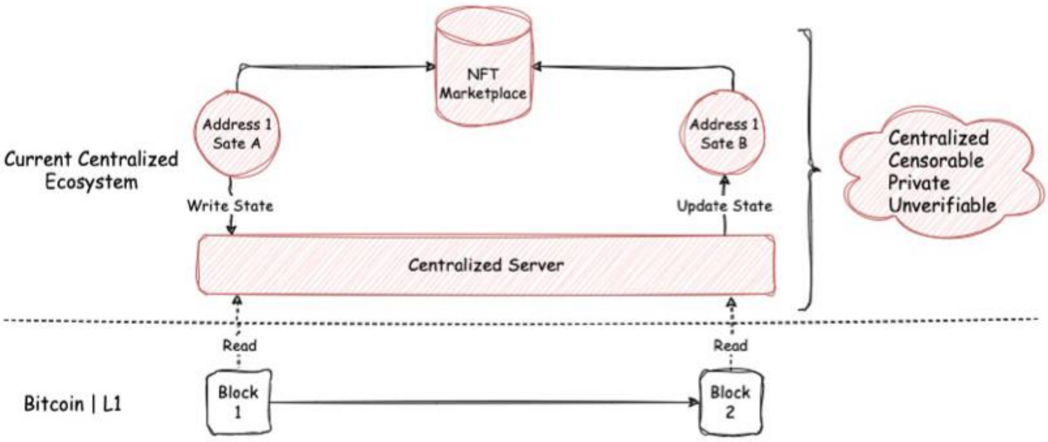
Bitcoin transaction is based on Bitcoin Script, which is a stack-based programming language for locking and unlocking transactions. Bitcoin does not support the Turing Complete virtual machine, which has brought a certain degree of hindrance to the development of Bitcoin ecosystem. The prosperous ecosystem projects on Ethereum are brought by virtual machine and smart contract.

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

The new Bitcoin protocols such as Ordinals and BRC-20 have brought the prosperity of Bitcoin ecosystem and brought unlimited imagination space to Bitcoin ecosystem. However, the Bitcoin network does not do any verification of the new protocols, but only stores them. Also, the centralized server off the Bitcoin network is needed to complete the loop of new protocols. For example, the mechanism of Ordinals theory to number Satoshis is running on a centralized server according to the fixed rules, and the Bitcoin network does not store or even know any relevant information about Ordinals. Although the BRC-20 protocol inscribes the content on Bitcoin network, its correctness has not been verified by Bitcoin network, so it also requires a centralized server off Bitcoin to do the computation and index. The risks brought by centralized server are self-evident. Different application providers use their own logic to compute for protocol services. The possibility of censorship, bugs, delays and other problems is very high, and it also violates the decentralized principles of blockchain and Web3.



2. Biop Design Philosophy

Biop is built according to a strong design philosophy: decentralized, optimistic, sustainability. It's important to understand them fully as they guide the design of Biop.

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. Biop always adheres to the concept of decentralized, provides the decentralized support for the current and future Bitcoin protocols to improve the Bitcoin infrastructure. Biop is the first Bitcoin L2 Blockchain which supports decentralized computing for new Bitcoin protocols, and will become the decentralized infrastructure for all Bitcoin ecosystem protocols.

2.2 Optimistic

Biop is a Bitcoin L2 Blockchain based on the Optimistic rollup protocol, which has been implemented on Ethereum and has achieved very good results. We believe that Biop, as the earliest and most powerful Bitcoin L2 in the world, will definitely establish a bigger ecosystem, and have an even better future.

At the same time, we optimistically believe that the backwardness of Bitcoin ecosystem will inevitably be changed a lot with the development of Biop and various protocols such as BRC-20. Also, the ecosystem of Bitcoin will surpass all existing blockchains including Ethereum. The developers, users, and protocols of Bitcoin will be very prosperous by the development of Biop.

2.3 Sustainability

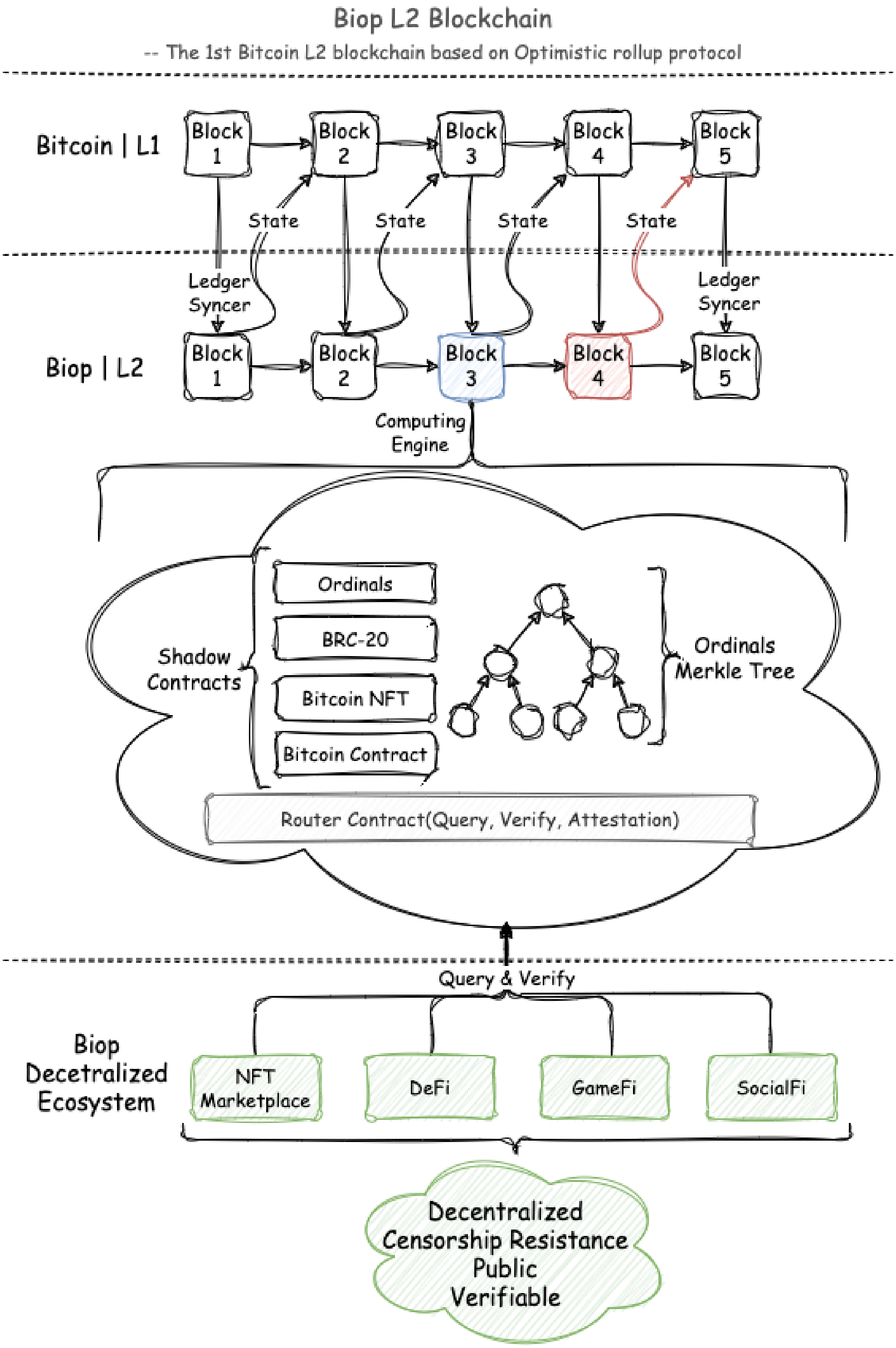
Biop adheres to the principle of sustainability. The initial design of Biop maintains a very open attitude, which can support existing Bitcoin protocols, their extensions, and the future Bitcoin protocols. We will keep the code design as simple as possible so that more developers can contribute code to Biop. We will maintain compatibility with existing protocols and tools, such as geth, to minimize the barriers for developers and users of Biop ecosystem, and let more people focus on the applications itself instead of spending a lot of time to adapt for Biop.

3. Biop L2 Blockchain

Biop L2 Blockchain = Bitcoin + Optimistic Rollup Protocol + PoS + BVM

Biop is a Bitcoin L2 Blockchain based on Optimistic rollup protocol, which moves the computing of new Bitcoin protocols such as BRC-20 to L2, and is Bitcoin's decentralized computing chain. At the same time, as a Bitcoin L2, Biop will be a blockchain, use PoS (Proof of Stake) as consensus algorithm, use the blocks of Bitcoin network as input, use Ledger Syncer to transfer and parse Bitcoin ledger, inscription ledger, BRC ledger, etc. into Biop block, and use Computing Engine to complete the computing of various Bitcoin protocols. Then the computing results are stored as Merkle Trees and smart contracts, and finally the block state is written into Bitcoin block as witness to complete the block generation. The validator is responsible for challenging the correctness of the block, submitting fault proof for problematic blocks, and obtaining challenge rewards.

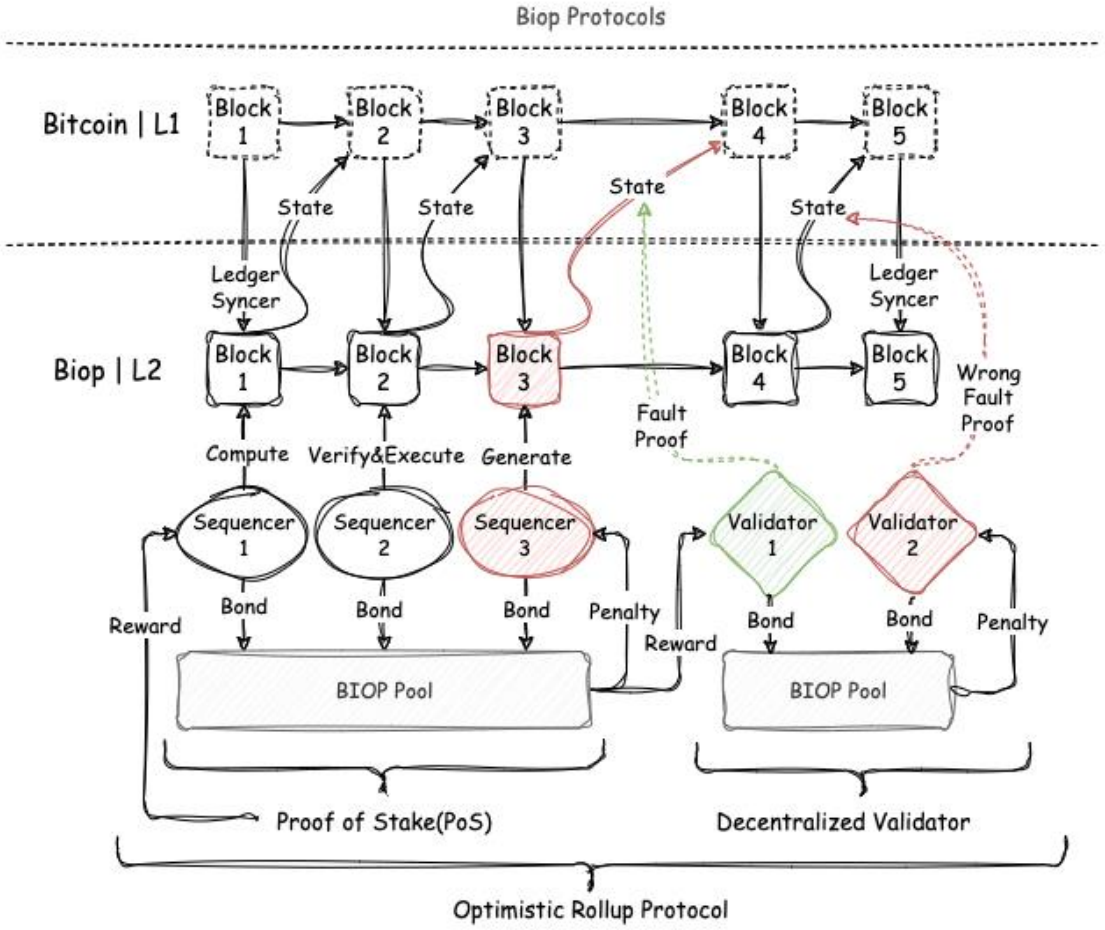
Biop will completely change the centralized dependence of new protocols such as BRC-20, will become the decentralized computing chain for Bitcoin, and will become the decentralized infrastructure for all ecosystem decentralized applications such as NFT marketplace, DeFi, GameFi, and SocialFi on Bitcoin.



This chapter has two parts, one part introduces the protocols of Biop, and the other part introduces the technical components of Biop.

3.1 Protocols

Biop combines Optimistic rollup protocol and PoS (Proof of Stake) consensus algorithm to realize decentralized Bitcoin L2. This chapter will explain the two protocols and the two roles of the protocols: Sequencer and Validator.



3.1.1 Optimistic Rollup Protocol

Optimistic rollup is a type of layer-2 scaling solution that relies on off-chain computation to record transactions in layer-2 trustlessly. Optimistic rollup is basically just a fancy way of describing a blockchain that piggy-backs off of the security of another "parent" blockchain. Specifically, Optimistic rollup takes advantage of the consensus mechanism (like PoW or PoS) of their parent chain instead of providing their own.

Optimistic rollup has been implemented on Ethereum and made a big success. Optimistic rollup on Biop is an approach to scaling Layer 1(Bitcoin) that involves moving computation and state storage off-chain. Biop executes transactions off the Bitcoin network, but post transactions data to Bitcoin as witness.

Optimistic rollup operators bundle multiple off-chain transactions together in large batches before submitting to Bitcoin. This approach enables spreading fixed costs across multiple transactions in each batch, reducing fees for end-users. Optimistic rollup also uses compression techniques to reduce the amount of data posted on Bitcoin.

Optimistic rollup is considered "optimistic" because they assume off-chain transactions are valid and don't publish proofs of validity for transaction batches posted on-chain.

3.1.2 PoS Consensus

Biop is a blockchain which uses the PoS (Proof of Stake) consensus mechanism to ensure decentralization and security. As a decentralized computing chain, Biop V1 will be consistent with the block generation time of Bitcoin. After the block generation of Bitcoin network, Biop uses Bitcoin block as input, computes the BTC’s state and other protocols’ state, and finally save the computing results to Biop's block.

PoS (Proof of Stake) underlies certain consensus mechanisms used by blockchains to achieve distributed consensus. In PoW (Proof of Work), miners prove they have capital at risk by expending energy. Biop uses PoS, where sequencer explicitly stake capital in the form of BIOP token into a smart contract on Biop Chain. This staked BIOP token then acts as collateral that can be destroyed if the sequencer behaves dishonestly or lazily. The sequencer is then responsible for checking that new blocks propagated over the network are valid and occasionally creating and propagating new blocks themselves.

3.1.3 Sequencer

The block generation node of Biop Chain is called Sequencer, who's duty is similar to the Sequencer in Optimistic rollup protocol: packaging, verification and execution of blocks. The difference is that Biop uses multiple Sequencers to generate blocks to ensure the decentralization of Biop Chain. Similar to become a Validator, becoming a Sequencer also requires to stake a certain amount of BIOP token. Generating correct blocks can be rewarded with BIOP token, but generating incorrect blocks will be deducted from the bond as a penalty.

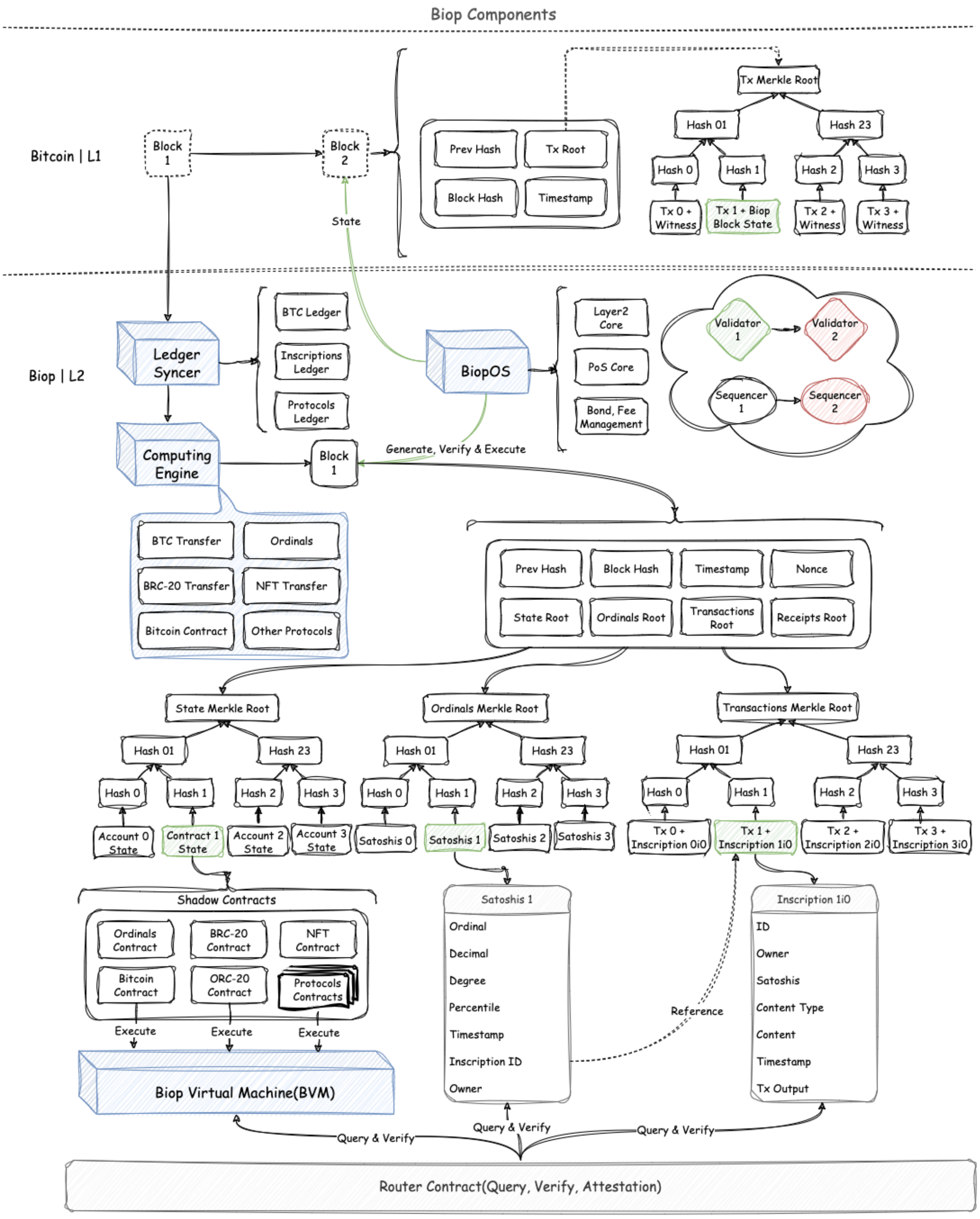
3.1.4 Validator

Optimistic rollup relies on a fault-proving scheme to detect cases where transactions are not executed correctly. The role who generates the fault-proving is called validator. After a rollup batch is submitted on Bitcoin, there's a time window (called a challenge period) during which anyone can challenge the results of a rollup transaction by computing a fault proof.

If the Validator' s fault proof succeeds, the rollup protocol re-executes the transaction(s) and updates the rollup's state accordingly. The other effect of a successful fault proof is that the Sequencer responsible for including the incorrectly executed transaction in a block receives a penalty.

3.2 Components

Biop uses some components to realize the Optimistic rollup protocol, PoS and the interaction between protocols. Biop uses technologies such as BVM, smart contract, and Merkle Tree to complete the computing, state storage, query, and verification of Bitcoin protocols, and to ensure that the state of the protocols can be traceable, verifiable and immutable.



3.2.1 BVM

BVM (Bitcoin Virtual Machine), is the core component of Biop Chain. BVM is responsible for the deployment, execution, query and verification of smart contracts. BVM is an important extension to Bitcoin network by Biop. As a Turing Complete virtual machine, the computing of Bitcoin's BRC-20 and many other protocols will eventually be completed on BVM. BVM is EVM Equivalence — complete alignment with the Ethereum Virtual Machine specification, which means that many developers, decentralized applications, and users of Ethereum ecosystem can seamlessly connect to Biop, laying the foundation for the rapid expansion of Biop ecosystem.

3.2.2 BiopOS

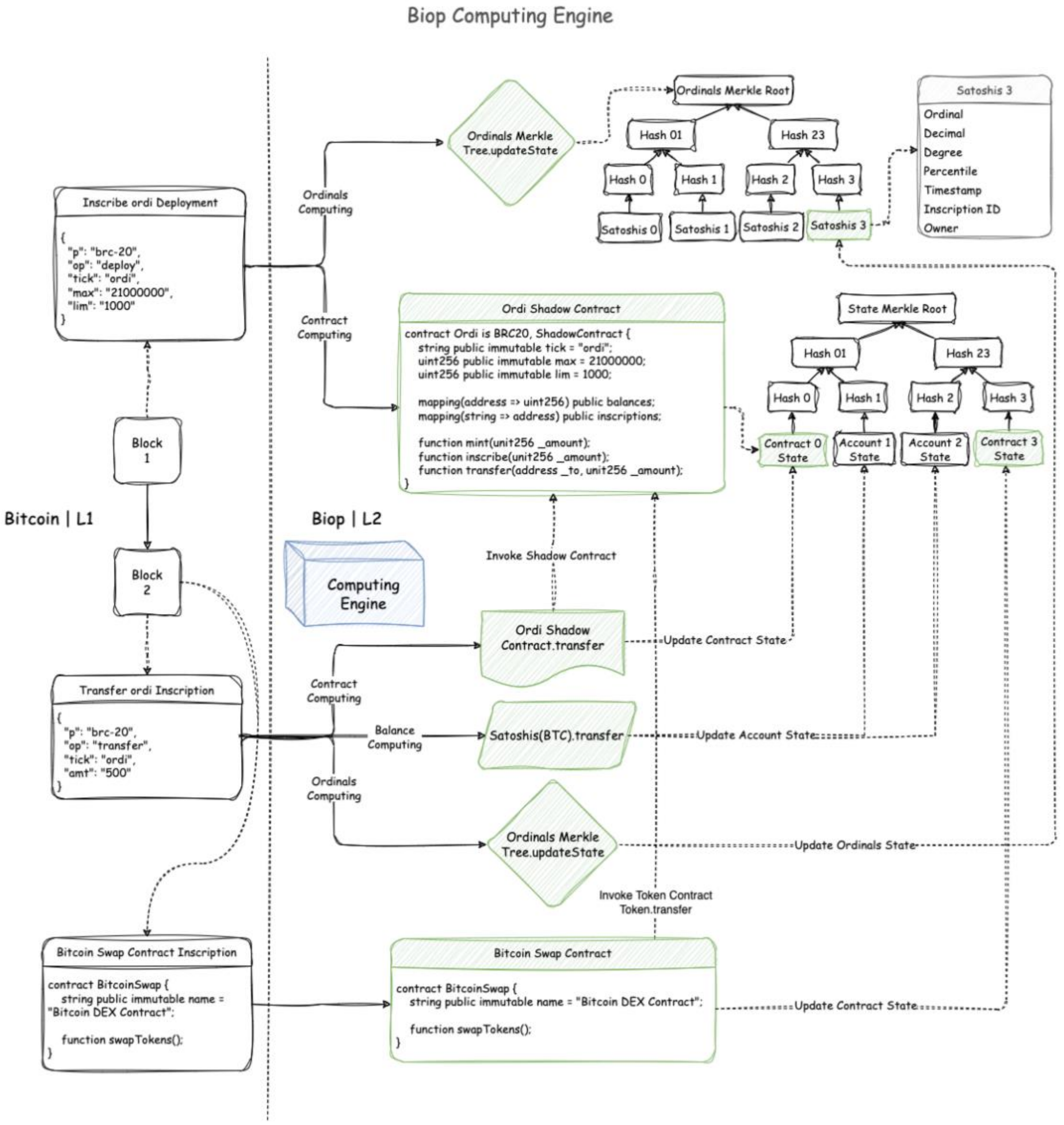
BiopOS is the core implementation of Bitcoin L2, which implements and executes the Optimistic rollup protocol and PoS consensus algorithm, including the generation of Biop block, management of Sequencer and Validator, management of transaction fee, and the interaction with L1(Bitcoin). To save transaction fee, Biop block state data will be stored to Bitcoin as witness.

3.2.3 Ledger Syncer

Ledger Syncer is responsible for interacting with Bitcoin node, parsing various protocol ledgers such as BTC ledgers, inscriptions ledgers, and BRC-20 ledgers from Bitcoin block to Biop Chain, as the input for the computing engine.

3.2.4 Computing Engine

Due to the limitation of Bitcoin's scripting system, Bitcoin does not support Turing Complete virtual machine, the computing of new Bitcoin protocols such as BRC-20 relies on centralized servers off Bitcoin network to complete, and various risks such as censorship are very high. Biop will complete the computing of the new Bitcoin protocols through the Computing Engine, move the computing which cannot be completed by Bitcoin script, and compute: the transfer of inscriptions, Ordinals, the state of BRC-20 and other protocols, etc. Make the new Bitcoin protocols supported by Biop decentralized infrastructure, and be truly decentralized, censorship resistance, trustable, traceable, immutable and verifiable.



Inscribe ordi Deployment

```
{
  "p": "brc-20",
  "op": "deploy",
  "tick": "ordi",
  "max": "21000000",
  "lim": "1000"
}
```

Ordi Shadow Contract

```
contract Ordi is BRC20, ShadowContract {
    string public immutable tick = "ordi";
    uint256 public immutable max = 21000000;
    uint256 public immutable lim = 1000;

    mapping(address => uint256) public balances;
    mapping(string => address) public inscriptions;

    function mint(unit256 _amount);
    function inscribe(unit256 _amount);
    function transfer(address _to, unit256 _amount);
}
```

Transfer ordi Inscription

```
{
  "p": "brc-20",
  "op": "transfer",
  "tick": "ordi",
  "amt": "500"
}
```

Bitcoin Swap Contract Inscription

```
contract BitcoinSwap {
    string public immutable name =
"Bitcoin DEX Contract";

    function swapTokens();
}
```

Bitcoin Swap Contract

```
contract BitcoinSwap {
    string public immutable name = "Bitcoin DEX Contract";

    function swapTokens();
}
```

3.2.4.1 Shadow Contract

Shadow contract is the smart contract corresponding to BRC-20 and other protocols mapped on the Biop Chain. The execution and verification of shadow contract is guaranteed through BVM. With the shadow contract, developers and users can verify the state of the new Bitcoin protocols like invoking the smart contract from Ethereum, which make the new Bitcoin protocols computing, query and verification fully decentralized and trustable.

3.2.4.2 Bitcoin Contract

For Bitcoin have better computing capability, Biop will support smart contract inscribed on Bitcoin by inscriptions or other methods. The smart contract is saved on Bitcoin, executed and verified in Biop's BVM, 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: BVM to build complex decentralized applications like DEX, DeFi, GameFi, etc.

3.2.4.3 Merkle Tree

Bitcoin uses Transactions Merkle Tree to save all the transactions of block. Similar to the Transactions Merkle Tree of Bitcoin, Biop will use more Merkle Trees: State Merkle tree, Ordinals Merkle tree, Transaction Merkle tree, Receipt Merkle tree, to save the computed results from Computing Engine, used for decentralized query and verification.

3.2.5 Router Contract

Router Contract is a smart contract which stores the metadata of all Bitcoin protocols, and provides query and verification services for BRC-20 and other protocols externally. Router Contract matches user's request to the corresponding shadow contract or Merkle Tree to complete the final query or verification. In the future, Biop DAO will decide if charge BIOP token for protocol fee and how to use the fee, such as distribution to Sequencer or burn, etc.

3.2.6 Merkle Proof

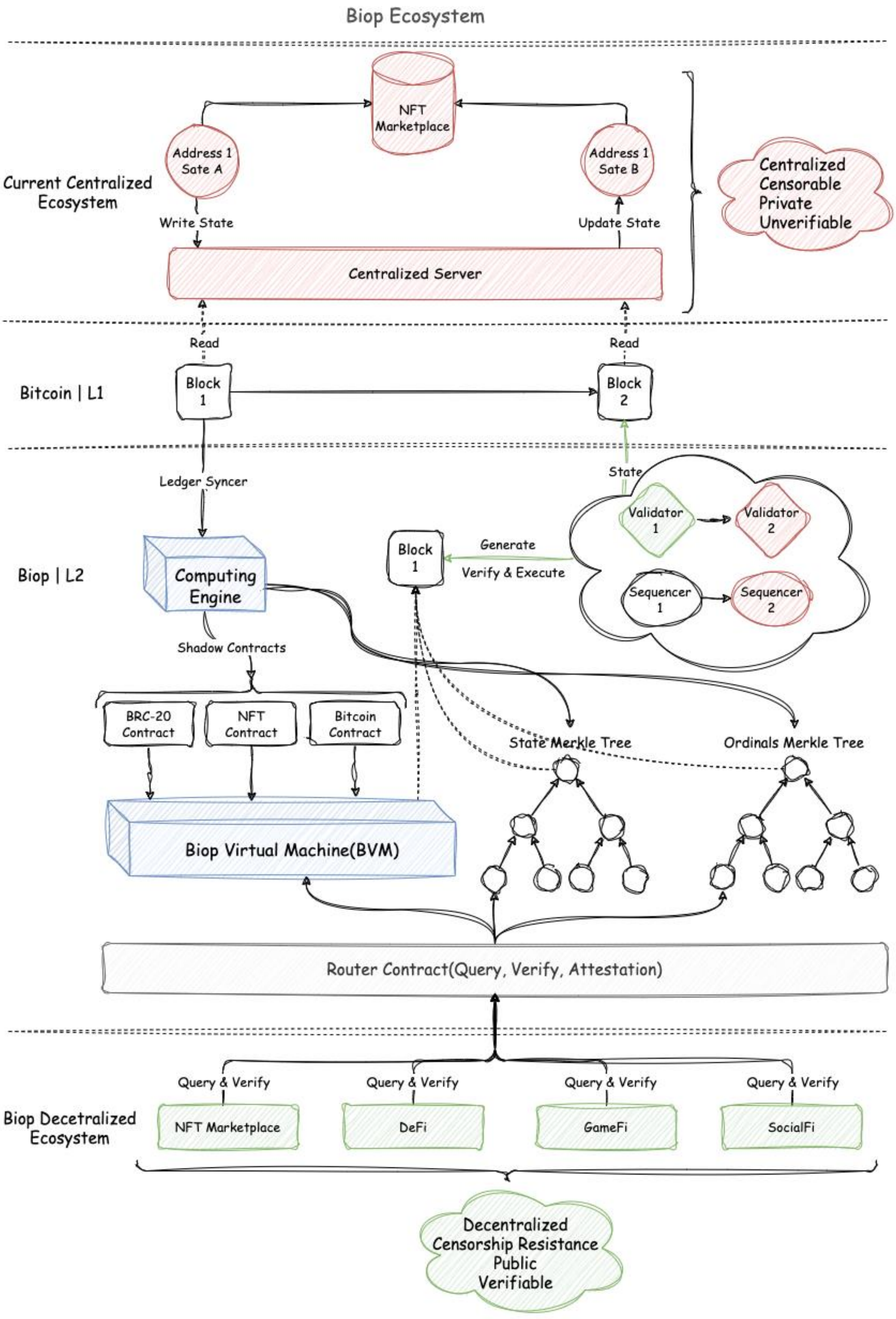
For new Bitcoin protocols such as BRC-20, Biop computing engine will compute and save the Merkle Proof to verify the new protocol state. This is very important, the state of all new protocols is verifiable, and the verification is based on Biop's decentralized nodes, based on immutable Merkle Tree technology.

3.3 Support New Born Protocol

For the new born Bitcoin protocols implemented by Bitcoin Inscriptions, Witness, or other technologies in the future, developers or users can submit a proposal to Biop, so that Biop can support the new protocol. Biop is a sustainable protocol, will continue to support the new born Bitcoin protocols, and develops the Bitcoin ecosystem with an open attitude.

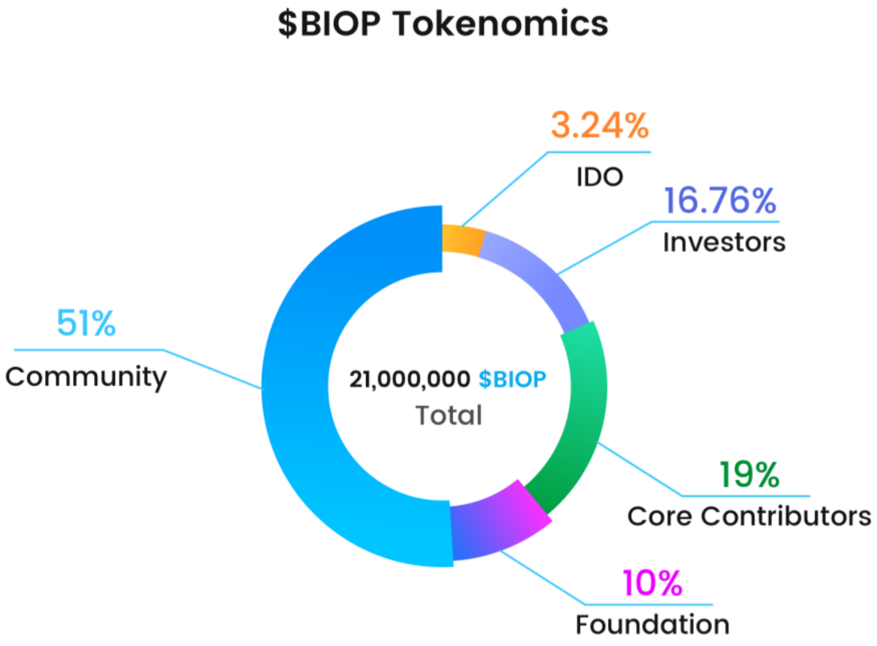
4. Decentralized Ecosystem based on Biop

Biop will establish a strong decentralized ecosystem for Bitcoin, by BVM and smart contract. The current Bitcoin ecosystem projects based on new Bitcoin protocols such as NFT marketplace needs to be supported by centralized server, which has the disadvantages of centralized, censorable, private, and unverifiable. The ecosystem built on Biop, a decentralized infrastructure based on Bitcoin, will be completely decentralized, censorship resistance, open, and verifiable. It is time to participate in the decentralized Web3 ecosystem based on Bitcoin and Biop.


Biop Ecosystem
Current Centralized Ecosystem
NFT Marketplace
Address 1 Sate A
Address 1 Sate B
Write State
Update State
Centralized Server
Centralized Censorable Private Unverifiable
Read
Read
Bitcoin | L1
Block 1
Block 2
Ledger Syncer
State
Validator 1
Validator 2
Sequencer 1
Sequencer 2
Generate
Verify & Execute
Block 1
Biop | L2
Computing Engine
Shadow Contracts
BRC-20 Contract
NFT Contract
Bitcoin Contract
Biop Virtual Machine(BVM)
State Merkle Tree
Ordinals Merkle Tree
Router Contract(Query, Verify, Attestation)
Query & Verify
Query & Verify
Query & Verify
Query & Verify
Biop Decetralized Ecosystem
NFT Marketplace
DeFi
GameFi
SocialFi
Decentralized Censorship Resistance Public Verifiable

5. Biop Tokenomics

As the core of Biop, Biop issued BIOP token based on BRC-20 protocol on Bitcoin network, total supply: 21,000,000, which will be used for Biop decentralized governance. $BIOP token will be distributed to all individuals, teams and institutions that contribute to Biop, including developers, users, ecosystem projects, investors, Sequencers, Validators, Biop Chain participants, etc. At the same time, we have set a reasonable lock period and release period for the allocated tokens.



Category	Percentage	Amount
IDO	3.24%	679,710
Investors	16.76%	3,520,290
Core Contributors	19%	3,990,000
Foundation	10%	2,100,000
Community	51%	10,710,000
Total	**100%**	**21,000,000**

IDO: 3.24%, the fund raised will be used for development and operation, all tokens have been released.

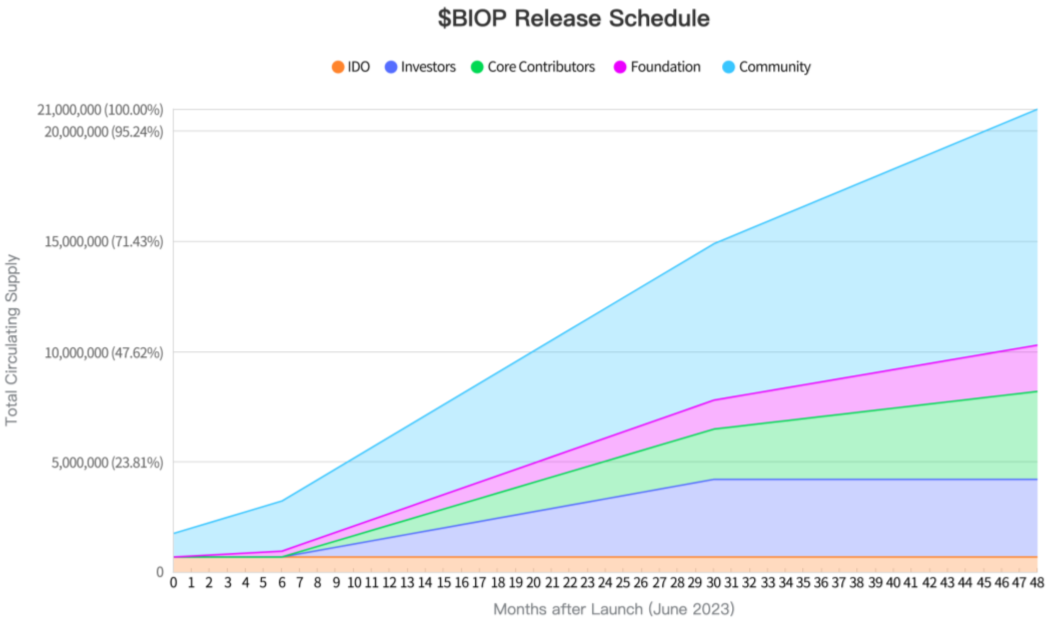
Investors: 16.76%, for investors, so that more institutions can participate in Biop and contribute to the development of Biop. It will be unlocked after 6 months and then will be released linearly in next 24 months.

Core Contributors: 19%, used to reward individuals and teams who have contributed to Biop, unlocked after 6 months, and then released linearly in next 42 months.

Foundation: 10%, used for the operation of Biop Foundation, no lock period, released linearly in 48 months.

Community: 51%, Biop allocated most of the BIOP tokens to community for users, ecosystem projects, Sequencers, Validators, Biop Chain participants, etc. The initial release is 5.1%, and the remaining 45.9% will be released linearly in 48 months.

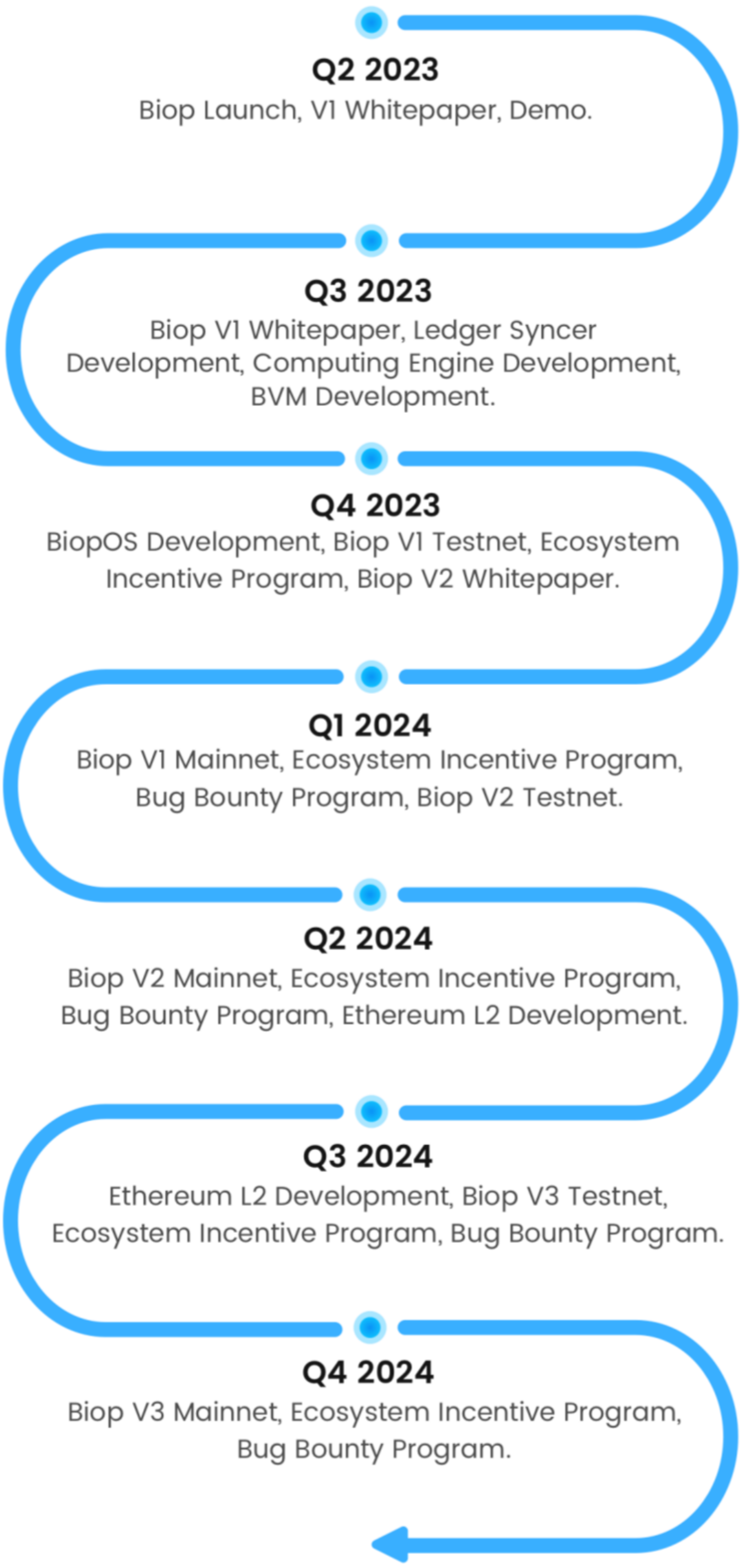
The estimated circulating supply of BIOP Token is shown in the figure below.



6. Biop Roadmap

Biop L2 Blockchain will have 3 versions: V1, V2 and V3. The most important milestones are Biop V1 Mainnet on Q1 2024, Biop V2 Mainnet on Q2 2024, and Biop V3 Mainnet on Q4 2024. All three versions will provide unlimited imagination space for Bitcoin decentralized ecosystem. The details are shown in the figure below.

Biop Roadmap



Q2 2023

Biop Launch, V1 Whitepaper, Demo.

Q3 2023

Biop V1 Whitepaper, Ledger Syncer Development, Computing Engine Development, BVM Development.

Q4 2023

BiopOS Development, Biop V1 Testnet, Ecosystem Incentive Program, Biop V2 Whitepaper.

Q1 2024

Biop V1 Mainnet, Ecosystem Incentive Program, Bug Bounty Program, Biop V2 Testnet.

Q2 2024

Biop V2 Mainnet, Ecosystem Incentive Program, Bug Bounty Program, Ethereum L2 Development.

Q3 2024

Ethereum L2 Development, Biop V3 Testnet, Ecosystem Incentive Program, Bug Bounty Program.

Q4 2024

Biop V3 Mainnet, Ecosystem Incentive Program, Bug Bounty Program.

7. Reference

1. Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf
2. Vitalik Buterin, Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform, https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_Whitepaper_-_Buterin_2014.pdf
3. Ethereum Community, OPTIMISTIC ROLLUPS, https://ethereum.org/en/developers/docs/scaling/optimistic-rollups/
4. Ethereum Community, PROOF-OF-STAKE (POS), https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/
5. Optimism Community, Optimism Bedrock specs, https://github.com/ethereum-optimism/optimism/tree/develop/specs
6. Offchain Labs, Arbitrum Nitro: A Second-Generation Optimistic Rollup, https://github.com/OffchainLabs/nitro/blob/master/docs/Nitro-whitepaper.pdf
7. Casey Rodarmor, BIP: Ordinal Numbers, https://github.com/ordinals/ord/blob/master/bip.mediawiki
8. ordinals.com, Ordinal Theory Handbook, https://docs.ordinals.com/
9. domo, brc-20, https://domo-2.gitbook.io/brc-20-experiment/
10. OKX Web3, BRC20-S, https://www.okx.com/web3/build/docs/bitcoin-ecosystem/brc20-s
11. Binance Academy, ORC-20 Tokens, https://academy.binance.com/en/glossary/orc-20-tokens