bitcoinOS：A Digital Sovereign Network for AI Era

@BitcoinOS Labs

1. Introduction

Bitcoin is a peer-to-peer electronic cash system designed to create a decentralized financial ecosystem, providing individuals with sovereignty over their identities and digital assets. bitcoinOS builds upon Bitcoin as its core, adding sovereignty protection for data assets. bitcoinOS is a modular blockchain network with Bitcoin L1 as the settlement layer, constructing Bitcoin L2, known as Fastnet, based on RGB smart contracts and ICP network technology. While the Bitcoin network primarily focuses on asset platforms and payment applications, bitcoinOS integrates Bitcoin L1 assets comprehensively and, through the SmartWallet combined with the ICP network, brings broader application scenarios and superior user experiences to the Bitcoin ecosystem. bitcoinOS maintains the sovereignty of identity and assets, while also supporting and protecting data sovereignty, enhancing privacy and scalability, thereby facilitating fast payments and transactions for all Bitcoin assets.

In the era of artificial intelligence, data is considered the most critical production factor. By providing data ownership through bitcoinOS, it offers the first step guarantee for the legitimate owners of data. Similar to Bitcoin's ownership of identity and currency, data ownership on bitcoinOS will enables everyone to innovate using massive data with Large Language Models (LLM) or Large World Model (LWM). This not only promotes the rapid integration of Web2 and Web3 but also drives the widespread application of Bitcoin and blockchain technology.

If Bitcoin can be likened to the encrypted asset kernel similar to the Linux computing resource kernel, and ICP to the encrypted network protocol similar to the TCP/IP communication protocol, then bitcoinOS is akin to the encrypted asset operating system similar to the Android mobile operating system. Just as Android was born for the mobile internet, bitcoinOS is born for the value internet.

2. Vision

Digital Sovereign Network: While Bitcoin L1 has successfully established sovereignty over identity and assets, bitcoinOS takes this concept to new heights. bitcoinOS builds on Bitcoin

L1 as its core and utilizes the RGB smart contract protocol on the ICP network to construct Bitcoin L2: Fastnet. Fastnet provides comprehensive Bitcoin smart contract functionality and unlimited scalability while strengthening support for data sovereignty. On the bitcoinOS platform, ownership and rights to data assets belong entirely to individuals, making data assets first-class assets.

One-stop platform: bitcoinOS serves as a comprehensive platform for managing Bitcoin L1 assets, including but not limited to BTC transfers, as well as issuing and trading Ordinals, Atomicals, and RGB assets. As the Bitcoin L2 layer within bitcoinOS, Fastnet facilitates the issuance and trading of RGB assets, providing financial function support and fast payments for dApps and ecosystems. Additionally, Fastnet features Turing-complete smart contract functionality, meeting the needs of various application scenarios and empowering Bitcoin assets in areas such as DEX, social networks, staking, gaming, and more.

Gateway to AGI: Data assets are considered one of the most important digital assets. Just as Bitcoin is digital gold, data is digital oil, and bitcoinOS serves as the catalyst for the digital oil revolution. As the first Bitcoin network to grant data ownership, bitcoinOS is positioned as the gateway to the age of artificial intelligence. In the era of artificial intelligence, data becomes the most critical production factor, and having bitcoinOS and data assets becomes the ticket for every individual to enter the age of artificial intelligence. You may not have your own large-scale model, but you must have your own unique intelligent entity.

Foundation for Bitcoin mass adoption: As the cornerstone of driving Bitcoin mass adoption, bitcoinOS combines the transparency of Bitcoin assets with the versatility of the Fastnet universal network. Fastnet not only facilitates fast payments but also ensures the privacy of content and services while almost infinitely scalable to meet diverse application needs. bitcoinOS positions Bitcoin assets as the universal tokens of the digital world in the age of artificial intelligence.

Copilot of Developers & Creators: Runtime of bitcoinOS is based on WebAssembly, standing at the forefront of IT industry standards, benefiting from research achievements across the industry. The core functionality of bitcoinOS smart contract containers simplifies the complexity of developers' smart contract development. They can develop using various programming languages that support WebAssembly, such as Golang, JavaScript, Python, Java, and Rust. Additionally, the built-in dApp store in bitcoinOS greatly facilitates developers and users in accessing Bitcoin ecosystem resources, as well as enabling Bitcoin developers and users to use resources and services from Web2, integrating Web2 and Web3.

3. Technology

bitcoinOS is an enhancement and extension of Bitcoin, aimed at addressing some of the key challenges Bitcoin faces in its mass adoption process. Here are some of the main challenges Bitcoin currently faces:

Challenges	Solutions
Scalable	Lightning, ICP, Layer2···
Smart contract	EVM, RGB, Canister, Move, ···
Token economy	Ordinals, Atomicals, RGB, ···
Data economy	RGB, Canister, Taproot asset, ···

The reasons behind these challenges facing Bitcoin can be traced back to its core values. Bitcoin's design purpose is to safeguard individual sovereignty, ensuring the sovereignty of personal identity and assets, similar to a constitution, which forms its foundation. Therefore, Bitcoin's technical choices and features are all made to maintain these core values in the long term. Decisions such as Proof of Work (PoW), small blocks, block time, block space, etc., are all trade-offs made to ensure individual sovereignty, and these choices are the foundation of consensus within the Bitcoin community.

While Bitcoin L1 is committed to ensuring the highest security, Bitcoin L2 addresses challenges faced in other aspects. When considering various solutions, RGB and ICP are seen as ideal choices. RGB, as a native technology of the Bitcoin community, and ICP, as a universal version of the Lightning Network, both ensure individual sovereignty and provide a solid foundation for the long-term development of Bitcoin.

3.1 RGB

RGB is an extensible and confidential smart contract protocol, similar to zero-knowledge proofs (ZK) in general technology, and it also incorporates features of ZK itself. Unrelated to the blockchain field, RGB is a completely off-chain smart contract, where all computations are performed off-chain and finally validated on-chain, a process known as client-side validation. Through client applications such as wallets, users can verify the legitimacy and correctness of transactions and data without being limited by on-chain smart contracts, theoretically enabling unlimited scalability.

At the core of RGB are UTXOs (Unspent Transaction Outputs) and Single-use seals. The concept of single-use seals was first proposed by Bitcoin Core developer Peter Todd in 2016, allowing a message to be sealed with an electronic seal, ensuring that the message can only be used once, similar to the concept of UTXOs. Specifically, RGB utilizes Bitcoin's UTXOs as the carrier of messages, with Bitcoin's consensus mechanism ensuring that these UTXOs can only be spent once, thereby guaranteeing the nature of single-use seals.

The RGB protocol associates RGB state changes with the ownership of Bitcoin UTXOs based on single-use seals. Therefore, Bitcoin not only ensures the ownership of RGB states but also traces all state changes through the history of UTXOs. Single-use seals and UTXOs provide RGB protocol with a solution to double-spending issues and transaction traceability, both secured by Bitcoin's consensus mechanism.

The RGB protocol employs client-side validation technology, where the states and original transaction data in smart contracts are maintained and verified by all parties involved. The data of RGB smart contracts is only visible among participants, and the exchange of original data can be done through various means, such as email, file sharing, USB drives, etc., but the optimal way is through P2P encrypted network transmission. Data does not need to be verified by Bitcoin nodes but rather the proof (Hash) or commitment (Commitment) of transaction data is written into Bitcoin UTXOs, serving as a proof-of-ownership record system for RGB assets.

Client-side validation technology enables users to only verify UTXO historical data relevant to themselves, without concerning themselves with transaction histories unrelated to them, thereby enhancing privacy and making it more confidential than Bitcoin.

The Bitcoin community has long anticipated the application of RGB to both Bitcoin L1 and the Lightning Network, but before achieving this goal, several challenges need to be addressed:

1. Data Exchange: On Bitcoin L1, only the commitment of RGB transaction data is propagated, rather than the raw transaction data itself. Therefore, the original RGB data needs to be disseminated through another P2P network, which is a critical issue that needs to be resolved.

2. Data Availability: The client-side validation method of RGB requires smart contract data to be stored locally on the client. Therefore, data synchronization among multiple clients and the reliability of data become crucial, as data represents assets. Ensuring high data availability is essential for the successful application of RGB.

3. Interaction Experience: When transferring RGB assets, the recipient needs to generate an invoice using UTXOs and addresses, then send the invoice information to the payer. Subsequently, the payer makes the payment using the invoice, and finally, the recipient verifies and confirms. The entire process is relatively lengthy and requires both parties to be online, resulting in inconvenience for users in terms of interaction experience.

4. The Lightning Network is based on channel technology, supporting only payment messages and not general messages.

Therefore, significant upgrades are needed for the Lightning Network to better support the functionality of RGB smart contracts. Addressing this issue is crucial for integrating RGB into the Lightning Network to achieve broader functionality and applications.

3.2 ICP

ICP (Internet Computer Protocol) is a cryptographic consensus protocol that comprises core layers including the P2P network layer, consensus layer, message routing layer, and execution layer. Networks that implement the ICP protocol are known as Internet Computers, serving as a blockchain cloud and foundational infrastructure at Layer 0 for building blockchains.

ICP leverages robust cryptographic technologies such as Chain-Key Cryptography and Threshold Cryptography. The network consists of multiple subnets, demonstrating excellent interoperability between these subnets and with the external Internet. Through built-in cryptographic oracles, ICP achieves a complete Bitcoin full node on Canister containers.

The smart contract container Canister of ICP utilizes WebAssembly as its runtime, aligning with cutting-edge technological standards and benefiting from research outcomes across various industries and general computing. It boasts extremely fast execution speeds, with each Canister capable of storing over 400GB of data.

In summary, ICP stands as an excellent choice for constructing modular blockchains, offering superior privacy with robust execution and data availability layers (DA), and serving as a general-purpose version of the Lightning Network on-chain.

4. Product features

Fastnet, as the Bitcoin Layer 2 solution within bitcoinOS, adopts a technological approach combining RGB and ICP, leveraging the strengths of both to complement and enhance each other, demonstrating a typical modular blockchain architecture. RGB is responsible for smart contracts, while ICP provides the network, execution, and data availability layers.

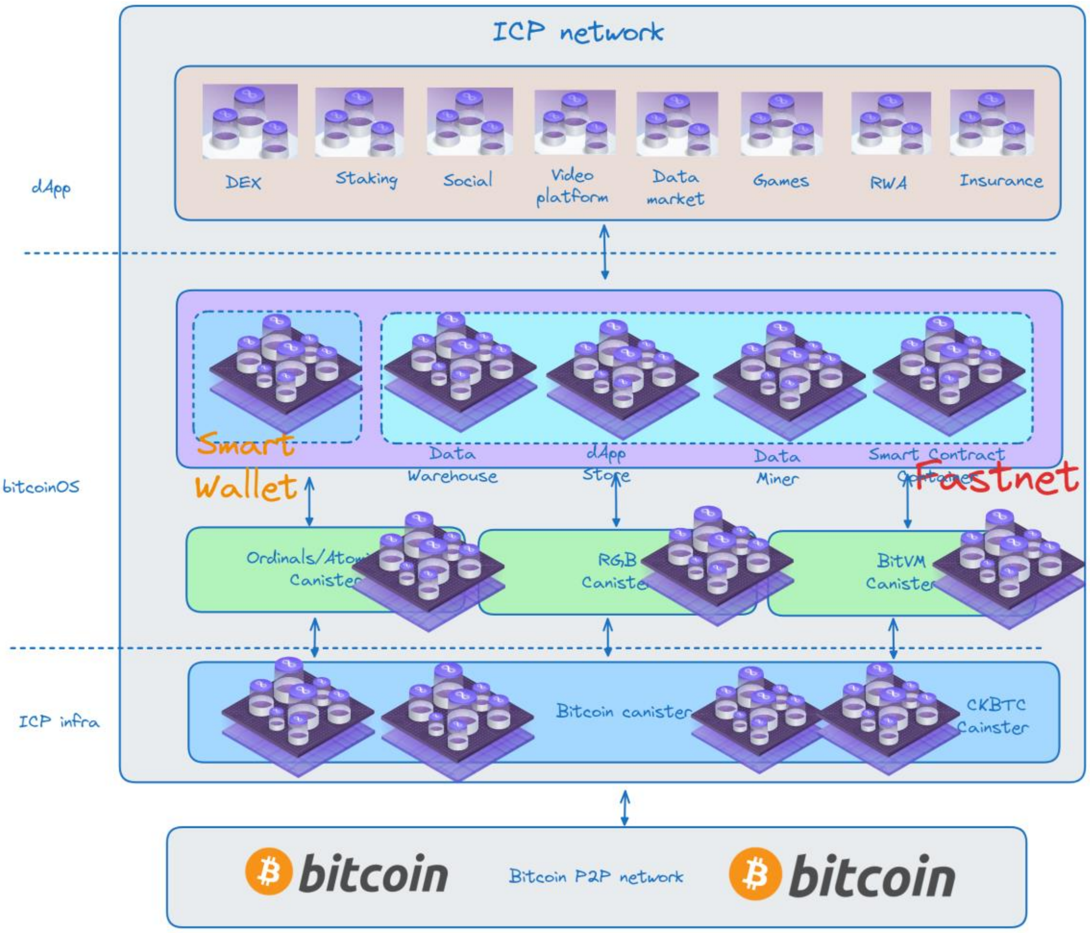
bitcoinOS utilizes WebAssembly as its runtime, supporting general-purpose computing and providing excellent support for applications such as Artificial General Intelligence (AGI) and Large Language Models (LLM). Users can leverage Bitcoin ecosystem assets on bitcoinOS to empower AI applications.

ICP effectively addresses the challenges mentioned earlier with RGB. ICP itself serves as a high-speed on-chain network supporting general message protocols, not limited to payment channels like the Lightning Network, thus resolving the issue of RGB data exchange.

ICP's Canister offers significant data storage capacity, addressing the data availability issue of RGB. RGB data can be securely stored on Canister while maintaining privacy, aligning with RGB's emphasis on privacy protection philosophy, and serving as the foundation for individual data sovereignty.

The smart wallet in bitcoinOS benefits from both RGB and ICP technologies, as they are both compatible with WebAssembly. By running the RGB client (such as the wallet) within the smart contract container Canister, the functionality of the wallet running in Canister is much more powerful than simple account abstractions. It enhances the programmability and automatic interaction capabilities of the wallet, enabling it to automatically guide through non-critical steps of RGB transactions.

For example, when Alice wants to make a payment to Bob, she can send a payment request to Bob's smart wallet through her own smart wallet. Bob's smart wallet will automatically generate an invoice and send it back to Alice's smart wallet. Then, Alice's smart wallet will make the payment against the invoice and send the raw transaction data via ICP to Bob's smart wallet, while also writing the commitment of the transaction data into Bitcoin UTXO. Upon receiving Alice's payment message and transaction data, Bob's smart wallet will validate the payment transaction against the commitment data in Bitcoin UTXO. Once validated, Bob's smart wallet will confirm the transaction. The entire transaction process only requires Alice to send the payment request and enter the amount, without Bob's direct involvement. This interaction experience is similar to current Bitcoin transactions.



bitcoinOS is a comprehensive system that fully supports Bitcoin L1 while also having its own L2 implementation. Leveraging the fast on-chain network of ICP's universal version and utilizing ICP's built-in Sequencer, bitcoinOS ensures the security of all messages through verification and consensus mechanisms such as Chain-key and Threshold Cryptography. Smart contracts on the RGB Canister are responsible for maintaining the Checkpoint state and proofs of RGB on ICP, and periodically commit the state to Bitcoin UTXO, achieving a level of security comparable to that of the Lightning Network.

In addition to utilizing RGB as the smart contract protocol for L2 Fastnet, bitcoinOS also supports various protocol assets such as btc, Ordinals, and Atomicals through SmartWallet. By implementing corresponding Indexers on ICP Canister, bitcoinOS has built a decentralized network of Bitcoin assets.

bitcoinOS is an open and powerful system and platform that can integrate various Bitcoin technologies and assets, not limited to specific technologies and protocols. In the future, it can also integrate cutting-edge technologies including BitVM to provide users with a wider range of services and features.

Fastnet serves as not only a solution for Bitcoin L2 but also the primary carrier of data assets network in bitcoinOS. bitcoinOS has developed various types of Data Warehouse smart contract containers for various data assets, designed and optimized for different application scenarios, such as personal digital assistants, personal gaming assistants, and personal agents. Each type of data asset has corresponding evaluation criteria and protocols. By combining with Data Miner contract containers, bitcoinOS successfully bridges the channel and connection between individual users and data consumers (including AI institutions, enterprises, or individuals). Developers can fully utilize various data containers to develop dApp, achieving the separation of data and applications. In this system, each user can act as a data miner by generating data for mining. When individual users are rewarded for mining through dApp, dApp developers also receive rewards simultaneously.

Data is considered the most important production material and element in the AI era, much like digital oil. Therefore, data ownership becomes the first step in the AI era. With the continuous development of artificial intelligence, up to 80% of personal work may be replaced by AI, and the biggest work for individuals may be to contribute data to AI. Consequently, the importance of data assets is increasingly highlighted. Through data ownership, we can activate everyone to innovate with massive data and large language models (LLMs) or large world models (LWMs), and emerge collective wisdom from them. This will help break the limitation of blockchain having only financial functions, enabling blockchain with better data privacy to be as colorful as Web2 and seamlessly integrate with Web3. Through such efforts, we can move towards the mass adoption of Bitcoin and blockchain, entering the Web5 era.

bitcoinOS is a Layer 2 project built on top of Bitcoin, utilizing RGB smart contract technology and running on the ICP network. Its main components include:

1) Fastnet (Bitcoin L2): Fastnet is a Bitcoin Layer 2 solution based on RGB and ICP, introducing Turing-complete smart contract

functionality to Bitcoin. It establishes a fast P2P communication network through ICP, granting users not only personal identity sovereignty and monetary sovereignty but also data sovereignty, giving users complete control over their data.

2) SmartWallet: SmartWallet is a non-custodial smart wallet that can access various assets on the Bitcoin Layer1 as well as Bitcoin Layer 2 assets on Fastnet. It also serves as a cloud wallet, allowing users to flexibly enable online features based on personal preferences.

The main advantages of bitcoinOS are as follows:
a) Excellent scalability: bitcoinOS leverages multi-subnet technology to achieve a transaction processing capacity of over 100,000 transactions per second. By continuously adding subnets, the network's scalability is linearly enhanced, opening up broad prospects for future development.

b) Outstanding privacy protection: bitcoinOS adopts RGB and ICP network, ensuring complete confidentiality and non-disclosure of data, safeguarding transaction information. Only participants and smart contracts can access raw transaction data, achieving efficient and secure transaction privacy protection, comparable to zero-knowledge proof (ZK) technology.

c) Seamless integration of Web2 and Web3: bitcoinOS achieves seamless integration of Web3 applications with Web2 through cryptographic oracles on ICP, cleverly introducing Bitcoin's financial attributes into the Web2 field. For example, using Bitcoin assets for fast payments and transactions. In addition, bitcoinOS rapidly introduces a large number of Web2 users and developers into the Web3 ecosystem through built-in smart contract containers, promoting the organic integration and common development of the two.

d) Enhancement of data sovereignty: bitcoinOS upgrades data to a first-class asset, empowering users with complete data sovereignty and asset control. Data is stored in dedicated smart contract containers, no longer dispersed across various dApp smart contracts, enabling users to fully control their data and generate revenue through data transactions and collaborations.

e) Innovative data mining mechanism: Users in bitcoinOS incentivized through the use of dApps developed by developers, combined with staking tokens and generating data, achieving mutual incentives for users and developers. This innovative data mining mechanism disrupts traditional dApp development models, benefiting both users and developers. Data mining complements data sovereignty, truly changing the relationship between users and means of production, making users not only users of dApps but also partners of dApp developers, jointly promoting the development and prosperity of the network.

f) Friendly support for Artificial General Intelligence (AGI): The WebAssembly runtime in bitcoinOS efficiently supports running AGI large language models, combined with massive unique data in bitcoinOS and powerful AI computing power support provided by the ICP network, providing an innovative exploration platform for AI institutions and individuals. This comprehensive technical support provides a solid foundation for the development and application of AI applications.

5. Development Roadmap

The feature of bitcoinOS design will be developed and implemented in stages, with the initial plan as follows:

1) Genesis Era (Q3 2024):

- Focus on establishing the core infrastructure of bitcoinOS, including the development of SmartWallet and the construction of Bitcoin L2 Fastnet, which includes key components such as Data Warehouse and Data Miner.
- Launch Testnet and Mainnet, and initiate stablecoin integration and basic DEX.
- Collaborate with ecosystem partners to promote the launch of over 100 dApps.

2) AppStore (Q1 2025):

- Launch the application store and smart contract containers on Bitcoin L2 Fastnet to expand bitcoinOS's functionality.
- Developers can easily develop various dApp and earn revenue from the application store through built-in token settlements.
- Users and developers can earn rewards from data mining by staking tokens for data mining, fundamentally changing the relationship between developers and users to achieve a win-win cooperation.

3) Sovereign Era (Q3 2025):

- Achieve the status of data assets as first-class assets on bitcoinOS through data sovereignty.
- Treat data assets as first-class assets similar to tokens, allowing users to trade their data or collaborate with AI institutions or individuals to earn stable long-term income, further enhancing bitcoinOS's value capture capabilities.

4) Smart Era (Q4 2025):
- Launch the GPT Store and collaborate with AGI large model institutions or developers to make bitcoinOS GPT Store the preferred choice for AGI agents.
- Developers can train and deploy their own large models and various agents on bitcoinOS, realizing a fully decentralized AI ecosystem and digital world.

5) Better Era (Q2 2026):
- Design and launch the Bitcoin Phone, a mobile operating system with bitcoinOS embedded, running as a light node of the bitcoinOS network.
- Increase support for satellite communications to further improve personal sovereignty network and metaverse space.