



BENFEN WHITE PAPER

BenFen

Version Date 06/08/2026

『New Generation of Real-World
Payment Public Chain』

君子务本
本立而道生

Benfen.org

Table of Contents

1. Vision and Mission of BenFen	01
2. Definition of Key Term	04
3. BenFen Blockchain	05
3.1 Security	05
3.2 High Performance and Consensus Mechanism	05
3.3 High Availability	07
3.3.1 Verifiability	07
3.3.2 Flexibility	08
3.3.3 Standard Library	08
3.4 zkLogin	09
3.4.1 Address Generation Flow	10
3.4.2 Signature Inspection Transaction Flow	10
3.5 Gas Fee	11
4. Native Stablecoin	13
4.1 Stablecoin Ecosystem	13
4.1.1 Stablecoin Circulation within BenFen Ecosystem	13
4.1.1.1 Paying Gas Fees with Stablecoins	13
4.1.2 Stablecoin Applications in the PayFi Ecosystem	14
4.1.2.1 Core Advantages of PayFi	15
4.1.2.2 The Role of BenFen Chain Stablecoins	15
4.1.2.3 Use Cases of PayFi	16
5. One-Click Token Issuance	18
5.1 Token Issuance Mechanism	18
5.2 Specific Process of Token Issuance	18
5.3 Types of Tokenized Assets	19

5.3.1	Stablecoins	19
5.3.2	One-Click RWA Issuance	21
5.4	Paying Gas Fees with Project Tokens	23
5.5	Using Sponsored Transactions for Gas Payment	24
6.	Privacy Accounts and Privacy Payments	26
6.1	Core Technology	26
6.2	Detailed Process of Privacy Transactions	27
6.2.1	Creation of Privacy Assets: One-Step Privacy Starting from Recharge	27
6.2.2	Privacy Payment	28
6.2.3	Viewing or Redeeming Assets	29
6.3	Core Features and Differentiated Advantages	29
6.3.1	Dual-Layer Compliance Design	29
6.3.2	Ultimate User Experience and Zero Gas Fee Model	30
6.3.3	High Performance and Ecological Scalability	30
7.	BenPay DEX	31
7.1	BenPay DEX Features	31
7.2	BenPay DEX Built-In Oracle System	31
8.	BenFen Bridge	33
8.1	Native BenFen Bridge	33
8.1.1	BenFen Bridge Key Components	33
8.1.2	Cross-Chain Process	35
8.1.3	Risk Prevention Measures	35
8.2	Cross-Chain Based on Node Network	36
8.2.1	Cross-Chain Process	38
9.	BenFen Ecosystem	39
9.1	BenPay: Web3 Stablecoin Financial Super App	39
9.1.1	BenPay Earn	39
9.1.2	BenPay Card: On-Chain Stablecoin Payment Card	40
9.1.3	BenPay Lending: Decentralized Lending Protocol	41

9.1.4	BenPay Merchant Services	42
9.1.5	BenPay On-Chain Red Packets	42
9.2	Technical Foundation and Ecosystem Support	42
9.3	Compliance and Security Assurance	43
9.4	Summary	43
10.	BenFen ID: An On-Chain KYC and Privacy-Preserving Identity Layer	44
10.1	Core Mechanism	45
10.1.1	Credential Model and Privacy Principles	45
10.1.2	Identity Verification and Credential Issuance	47
10.1.3	Verification Rules and Execution Mechanism	48
10.2	Key Features	49
10.2	Application Scenarios	50
11.	Governance	52
11.1	BenFen DAO and On-Chain Governance	52
11.2	Working Mechanism and Proposal Status	52
11.3	DAO System Design Description	53
12.	Roadmap	55
12.1	Layered Network	55
12.2	BenFen Layer-2 Solution Overview	55
12.2.1	State Channels	56
12.2.2	RollupChain	56
13.	Prospects	57
14.	Reference	58

Disclaimer: Nothing in this White Paper constitutes an offer to sell or an invitation to purchase any tokens. BenFen is releasing this White Paper solely for the purpose of receiving feedback and comments from the public. If BenFen decides to sell any tokens (or Simple Agreements for Future Tokens), it will do so through definitive offering documents, including disclosure documents and risk factors. These definitive documents are expected to include an updated version of this White Paper, which may differ significantly from the current version.

Nothing in this White Paper should be construed or read as a guarantee or promise as to how BenFen or the tokens will develop or as to the utility or value of the tokens. This White Paper outlines current plans, which may change at its discretion. Their success will depend on many factors outside BenFen's control, including market-based factors and factors within the data and cryptocurrency industry. Any statements about future events are based solely on BenFen's analysis of the issues described in this White Paper. This analysis might prove to be incorrect.

1. Vision and Mission of BenFen

Since it appears, Bitcoin has been defined as a Peer-to-Peer Digital Cash System. Blockchain distributed ledger technology, built upon Bitcoin, has undergone remarkable evolution and profoundly impacted multiple fields. As the first and most well-known cryptocurrency, Bitcoin offers advantages such as decentralization, security, and transparency. However, its extreme price volatility severely limits its potential as a medium of exchange and a store of value.

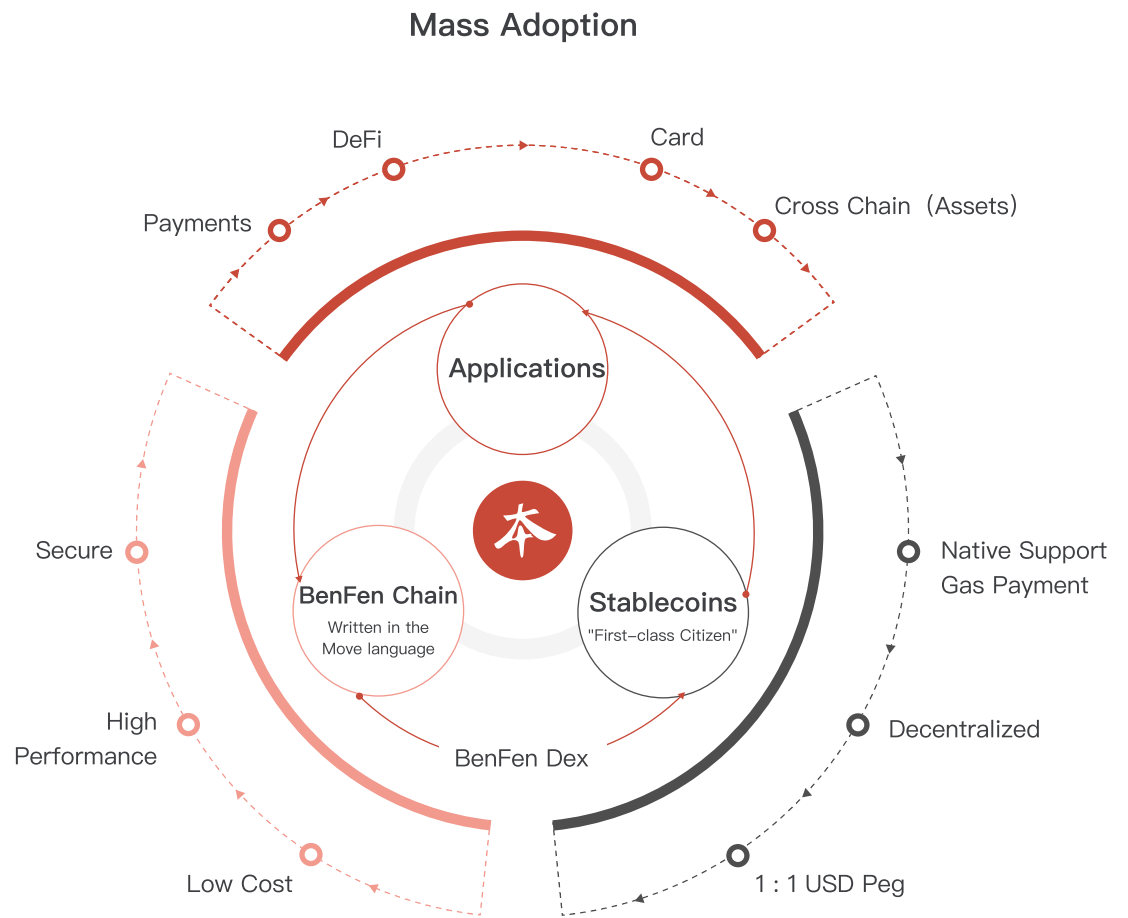
Stablecoins, one of the most important applications in Web 3.0, address this issue to a certain extent. Their relatively stable prices make them the primary means of payment in the Blockchain space. They are also known as **PayFi** (Payment Finance), an innovative technology and application model that combines payment functions with financial services in the Blockchain and Cryptocurrency space, serving as an indispensable backbone of the wave. However, issues such as centralization, lack of transparency and native support from public chains limit their broader adoption and application in a certain way.

Therefore, we have decided to build **BenFen — a next-generation public chain for real-world payment. Based on the Move programming language, BenFen offers technical advantages such as security, low cost, and scalability.**

It has a native pegged coin BUSD, enabling users to pay gas fees directly with stablecoins, significantly lowering the barrier to entry. BUSD, as the core asset of the BenFen public chain ecosystem, is pegged 1:1 to the US dollar and is minted on-chain from bridged USDT/USDC. The chain natively supports cross-chain functions and covers real payment scenarios through various ecosystem applications. BenFen is committed to building an open payment network that connects cross-border payments, e-commerce platforms, and offline merchants, and promotes the development of a diverse application ecosystem.

As the first public chain to natively support the use of stablecoins for gas fee payments, BenFen has built a complete, closed-loop ecosystem centered around stablecoins to meet market demand. This ecosystem includes, but is not limited to, decentralized finance (DeFi), cross-chain asset services, payment solutions, lending, and Real World Asset (RWA) tokenization. Furthermore, developers can leverage BenFen's powerful decentralized technology and rich underlying financial services to rapidly build a wide range of applications using the secure Move language.

BenFen's architectural design ensures that BenFen Chain, DEX, Stablecoins, and ecosystem applications can mutually reinforce each other, forming a layered driving flywheel. This enhances the efficiency and reliability of the entire network and provides a solid foundation for the widespread adoption of On-Chain Applications, thereby promoting the application and development of Blockchain technology in broader scenarios. BenFen aims to become a leading blockchain ecosystem through such a comprehensive design, providing users and developers with a comprehensive, efficient, and secure Blockchain Service Platform.



2. Definition of Key Term

In order to help readers understand the whole article better and more conveniently, we would like to list the key terms as follows:

- **BUSD:** BUSD is a USD-pegged stablecoin minted 1:1 through cross-chain USDT/USDC. Users can cross-chain transfer USDT or USDC into BenFen Chain, where the assets are automatically converted into BUSD at a 1:1 ratio. Conversely, users can redeem their BUSD for USDT or USDC at the same 1:1 ratio and withdraw the assets across chains.
- **BFC:** BenFen Coin (BFC) is the native token of the BenFen Chain, ensuring the security of the entire network through the equity staking mechanism. At the same time, it can also be used to pay the gas fees for on-chain transactions and provide continuous economic incentives for nodes.
- **BenFen DEX:** BenPay DEX is a native automated market maker model decentralized exchange (AMM DEX) built into the BenFen blockchain.

3. BenFen Blockchain

BenFen is built on the Move language to create a secure, high-performance, and highly available underlying Blockchain. It achieves sub-second latency and high throughput of tens of thousands of transactions per second while significantly reducing the average transaction cost and ensuring security.

3.1 Security

The Move Programming Language first debuted in Facebook's Diem Blockchain project. As a smart contract programming language focused on digital assets, Move has many security advantages:

- **Type Safety:** Move features a strict type system that can catch many common errors at compile-time, such as type mismatches and null pointer references, thereby enhancing code security.
- **Resource Lifecycle Management:** Through the concept of resources, assets are managed with strict lifecycle control, ensuring resources can only be used and transferred in expected ways, avoiding many security vulnerabilities such as reentrancy attacks and resource leaks.
- **Permission Control:** Developers can define permissions and constraints for accessing resources in the code. They can also achieve fine-grained control over resources and prevent unauthorized access and potential security risks.
- **Immutability:** Move encourages the use of immutable data structures and functional programming paradigms, reducing code complexity and minimizing many security vulnerabilities, such as state tampering and unintended side effects.
- **Formal Verification:** Move provides formal verification tools for static analysis and verification of smart contracts, helping developers discover and fix potential security issues, thereby improving code reliability and security.

3.2 High Performance and Consensus Mechanism

The Blockchain industry currently faces two core challenges: achieving high throughput while maintaining low latency and ensuring the long-term stability of the consensus protocol. To overcome these challenges, BenFen adopts an innovative approach that combines DAG-Based Consensus with Non-Consensus. This approach successfully achieves sub-second latency, sustaining a high throughput of tens of thousands of transactions per second and maintaining support for complex contracts, checkpoint generation, and reconfiguration of Validator Sets across epochs.

BenFen employs a sophisticated method to handle different types of transaction objects to achieve these goals. When a user with a private key creates and signs a transaction, the transaction is sent to each validator of BenFen Chain. These validators perform a series of validity and security checks before returning the signed transaction to the client. The client collects responses from the majority of validators to form a transaction certificate. Once the certificate is assembled, the user returns it to all validators. The validators check the certificate's validity and send receipts to the client. Transaction certificates can be processed directly without waiting for consensus engine intervention (processed via the fast path) for transactions involving only User-Owned Objects. All certificates are processed with a DAG-Based Consensus protocol executed by BenFen's validators. The consensus protocol determines the total order of certificates, and validators check and execute certificates involving shared objects. The client can collect responses from the majority of validators and assemble them into valid certificates used as proof of transaction settlement. Finally, each consensus submission forms a checkpoint, ensuring the network's long-term stability. The specific process is illustrated in the following diagram:

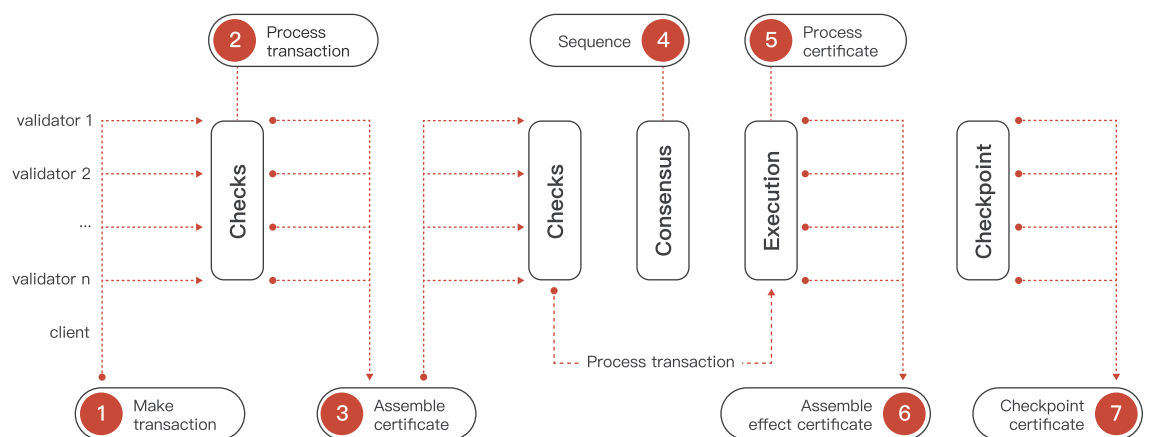


Figure 2: BenFen Flowchart

Through the optimized process described above, BenFen ensures extremely low transaction latency, maintaining processing times below 0.5 seconds per transaction and achieving high throughput with tens of thousands of transactions per second. This means users can expect rapid transaction confirmation and efficient blockchain operations.

Moreover, BenFen demonstrates exceptional robustness. Even in the event of some validation nodes failing or ceasing operation, the system can continue to run stably. This fault tolerance is one of the key factors ensuring the reliability of blockchain networks. It effectively mitigates the impact of single points of failure on the entire system, thereby enhancing its availability and stability. This ensures that BenFen can maintain high performance and reliability under various circumstances, providing users with an outstanding Blockchain experience.

3.3 High Performance and Consensus Mechanism

BenFen's high availability is reflected in the verifiability of contracts written in the Move language, which supports modular design and development, significantly reducing the difficulty of on-chain development.

3.3.1 Verifiability

To reduce on-chain computational overhead and improve security, Move defines a specification language called the Move Specification Language. This language describes how programs operate correctly, with specifications such as preconditions, postconditions, and invariants to define program behavior. The design of this specification language aims to reduce on-chain computational overhead and enhance security.

Once a program is described with the Move Specification Language and the specifications are defined, the next step is to convert the Move program and specifications into Boogie programs, an intermediate verification language with formal semantics. This conversion process is completed by the Move-to-Boogie compiler, transforming the program and specifications into a representation in the Boogie language.

Finally, automated theorem provers from the formal verification domain are used to verify whether the program meets the specifications. These solvers can analyze Boogie programs, check for violations of the specifications, and thus verify the correctness and security of the program. The program's behavior can be comprehensively checked by conducting formal

verification, providing a higher level of assurance.

3.3.2 Flexibility

BenFen's high flexibility stems from its modular design, advanced abstraction capabilities, custom data structures, flexible permission control, and cross-platform compatibility, which can meet the needs of the development of various Blockchain applications, providing more options and possibilities.

- **Modular Design:** Supporting modular design, allowing developers to modularize code into reusable components, thereby improving code maintainability and extensibility.
- **Advanced Abstraction Capabilities:** Offering rich advanced abstraction capabilities, such as Resources and Transactions, making it easier for developers to express complex logic and business requirements.
- **Custom Data Structures:** Allows developers to define custom data structures and types, better adapting to different application scenarios and needs, and enhancing flexibility and customizability.
- **Flexible Permission Control:** Supports flexible permission control mechanisms, enabling developers to control resource access permissions granularly as needed, achieving more secure and trusted smart contracts.
- **Cross-Platform Compatibility:** The Move language is designed with cross-platform compatibility in mind, enabling it to run on different blockchain platforms, providing developers with broader choices and flexibility.

3.3.3 Standard Library

As a general-purpose and secure smart contract platform, BenFen provides a formally verified smart contract Standard Library. The Standard Library contains over 40 commonly used functional modules, including accounts, transfers, transactions, events, error handling, mathematical calculations, vector operations, and more.

3.4 zkLogin

The innovative design of zkLogin provides users with a way to generate addresses and sign transactions based on Third-Party Authorization.

It can better help users meet the following six demands:

- **Convenient Transactions:** zkLogin enables users to generate addresses and conduct transactions on the chain with Third-Party OAuth login.
- **Security and Autonomy:** The OAuth provider only generates JWTs with temporary public keys, and does not have access to the user's temporary private key, i.e., no one other than the user, no other person or organization can get the complete information of the address's public and private keys.
- **Dual Authentication:** zkLogin is a two-factor authentication method that uses a JWT provided by the OAuth provider and a salt provided by the user or another salt provider. Stealing a user's OAuth account alone does not allow one to control the user's address.
- **Privacy Assurance:** The identity of the user's OAuth account is not known through the data on the chain.
- **Flexible Choice:** Users can choose any variety of OAuth.
- **Native Signature:** zkLogin is a feature natively supported by BenFen. Transaction verification occurs on the public chain layer instead of the contract layer, which maximizes the satisfaction of high-performance and low-cost transactions.

3.4.1 Address Generation Flow

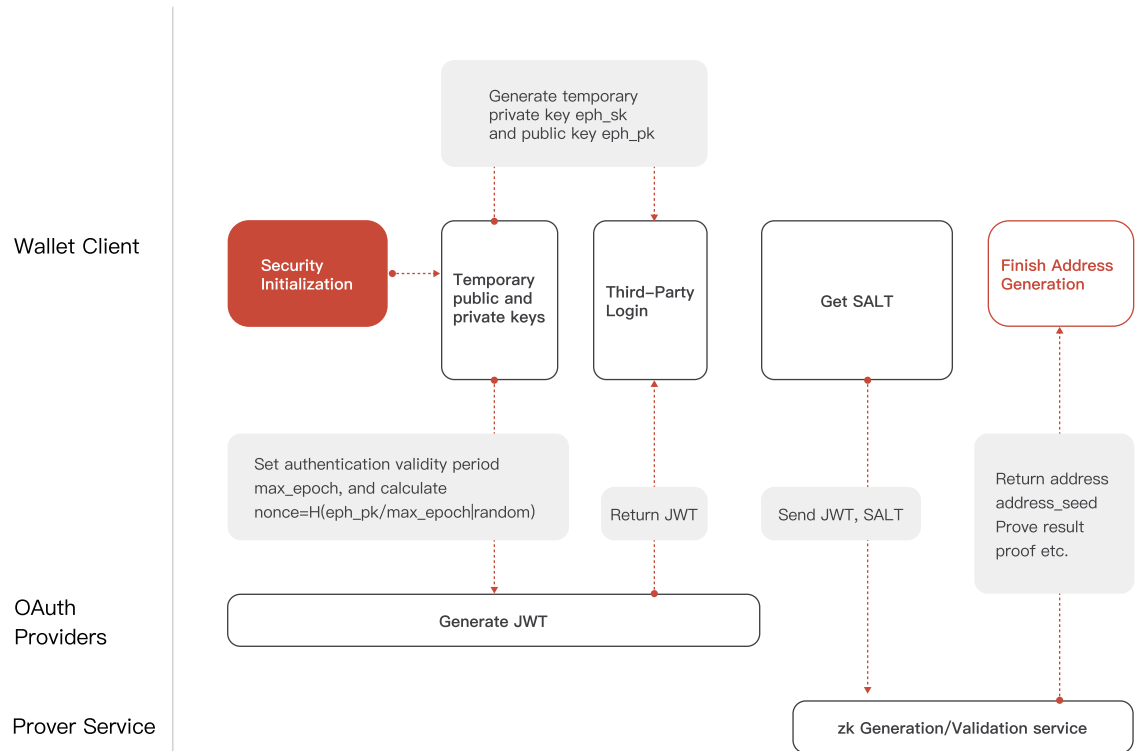


Figure 3: Address Generation Flow

3.4.2 Signature Inspection Transaction Flow

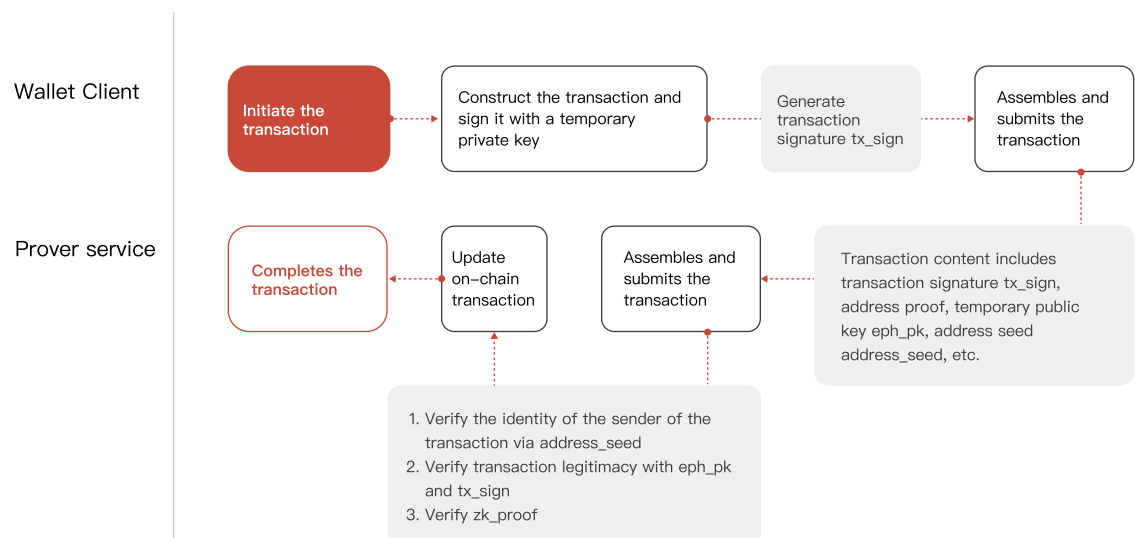


Figure 4: Signature Verification Transaction Flow

3.5 Gas Fee

Gas fee is a fee paid by users when executing transactions or smart contracts on the chain, which is mainly used to reward verification nodes and maintain the security and stability of the blockchain network. BenFen Chain has significantly reduced the average Gas Fee of on-chain transactions through the innovations of Move programming language, Object-Centric Data Model, efficient consensus mechanism, and dynamic Gas pricing.

Gas fee pricing model of BenFen Chain is:

$$Total_gas_fees = computation_units * reference_gas_price + storage_units * storage_price$$

This contains the computation and storage costs incurred by the computation transactions, which are respectively calculated by multiplying the computation or storage units by the relevant prices. Specifically:

- **Reference_Gas_Price:** Each validation node submits the lowest offer they are willing to process a transaction at each epoch. The BenFen chain will automatically sort the quotes submitted by each verification node and select the price at 2/3 calculated based on the pledge ratio as the reference price. When a user submits a gas price higher than the reference price, the difference is considered as a tip payment to the network, and paying the tip allows the user to get a higher priority.
- **Computation_Units:** Different transactions require different amounts of computation time for processing and execution. BenFen Chain converts these varying operational loads into transaction costs by measuring each transaction in the form of computation units.
- **Storage_Price:** This price is set by the governance proposal and is updated infrequently.
- **Storage_Units:** BenFen Chain calculates storage costs on the basis of each storage unit in a transaction, where each byte of data equals 100 storage units.

In addition, the storage mechanism of the BenFen chain provides a storage fee refund when a transaction deletes a previously stored object. Therefore, the net gas fee paid by the user is equal to the gas fee minus the rebate associated with the data deletion:

$$Net_gas_fees = computation_gas_fee + storage_gas_fee - storage_rebate$$

BenFen Chain not only supports using the native token BFC to pay gas fees, but also

allows users to pay with BenFen's native stablecoins BUSD. In this way, users can easily conduct transactions and other activities on BenFen Chain even if they only hold stablecoins. It should be noted that users who opt to pay gas fees with stablecoins will experience very small transaction friction, which will be charged to ensure that the stablecoins can be exchanged for sufficient BFC to cover the gas fees.

4. Native Stablecoin

Based on BenFen's vision, BenFen has launched the native core stablecoin BUSD on the BenFen Chain. BUSD is pegged to mainstream USD stablecoins such as USDT and USDC, ensuring rigid redemption and price stability. Compared to other stablecoin systems, the BenFen stablecoin system introduces several key innovations:

- **Rigid Redemption:** BenFen stablecoins achieve 1:1 redemption with leading stablecoins such as USDT and USDC through cross-chain bridges.
- **Stablecoins as First-Class Citizens:** At the public chain level, BenFen natively treats stablecoins as first-class citizens, allowing users to pay gas fees directly with stablecoins.

4.1 Stablecoin Ecosystem

4.1.1 Stablecoin Circulation within BenFen Ecosystem

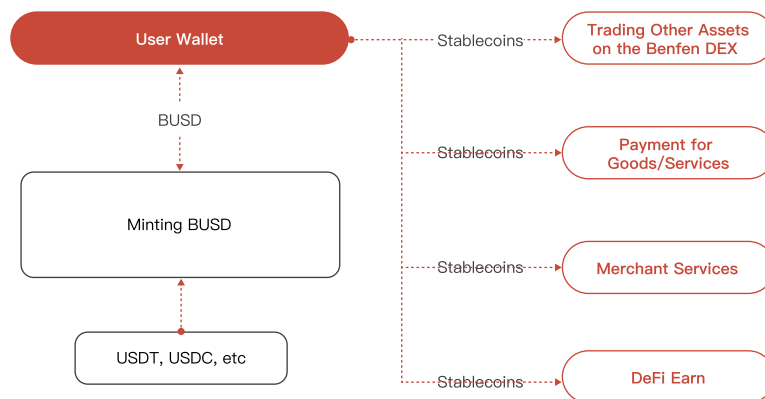


Figure 6: Stablecoin Circulation Chart within the BenFen Ecosystem

4.1.1.1 Paying Gas Fees with Stablecoins

In most mainstream public chain systems today, users are typically required to hold the network's native token to pay gas fees for transactions or interact with decentralized applications (DApps). This requirement introduces additional costs and operational complexity, posing a significant barrier to the broader adoption of Web3 applications. Moreover, the price volatility of native tokens can expose users to additional financial risk.

To address this issue, BenFen introduces a new mechanism that allows users to pay gas fees using supported stablecoins. This means that users can initiate transactions, interact with them, and even develop DApps without needing to hold the native platform token (BFC) — having only stablecoins is sufficient.

Unlike Ethereum's Gas Station Network (GSN) solution, BenFen's stablecoin-based gas payment mechanism does not require additional code logic, SDK integration, or reliance on centralized intermediaries such as relay servers, which often introduce single points of failure. Instead, BenFen leverages a built-in stablecoin service. When a user submits a transaction and chooses to pay for gas with BUSD, the system automatically facilitates the payment on the user's behalf. The user remains unaware of the underlying complexity — no extra steps or transaction retries are necessary.

Furthermore, the system is designed to be extensible. BenFen supports gas payments with any token, provided it is integrated with a compatible token swap platform. This innovative approach offers a more convenient, efficient, and cost-friendly environment for digital asset transactions, while significantly enhancing the usability and accessibility of the decentralized application ecosystem.

4.1.2 Stablecoin Applications in the PayFi Ecosystem

The global payment infrastructure has long been constrained by the rigidity of traditional systems and the fragmentation of banking networks. These limitations have made cross-border fund transfers notoriously expensive, slow, and operationally complex. For users in emerging markets in particular, such barriers significantly hinder their ability to participate in the global economy.

PayFi (Payment Finance) emerges as an innovative paradigm in response to these challenges. By integrating blockchain technology, PayFi combines efficient payment capabilities with advanced financial services, fundamentally reimagining how value flows across borders. PayFi aims to systematically address the shortcomings of traditional financial systems through the following core advantages:

4.1.2.1 Core Advantages of PayFi

- **Global Accessibility and Inclusive Costs:** PayFi eliminates the reliance on traditional banking infrastructure. Anyone, anywhere in the world, can access the global financial network with nothing more than a digital wallet. Leveraging blockchain's low operational cost and real-time settlement capabilities, PayFi dramatically reduces payment costs compared to traditional financial systems, bringing the vision of inclusive finance within reach.
- **Trustless Execution:** All transactions and financial agreements are executed automatically via smart contracts, removing the need for costly and inefficient centralized intermediaries. This ensures fairness in execution, while all rules and transaction histories remain transparent and verifiable on-chain.
- **Programmability:** PayFi is more than just a payment rail—it is a programmable financial platform. Users can define complex conditions for fund flows using smart contracts, such as automated payroll distribution. This level of flexibility opens the door to innovative financial products and entirely new business models.
- **Seamless Ecosystem Compatibility:** PayFi integrates natively with major digital asset ecosystems, particularly stablecoins, offering users and merchants a stable and reliable medium of exchange. By reducing technical barriers and mitigating volatility risks, it accelerates the real-world adoption of crypto payments across diverse commercial scenarios.

4.1.2.2 The Role of BenFen Chain Stablecoins

To realize the vision of PayFi, a new generation of stablecoins is essential—one that is more stable, efficient, and trustworthy, and capable of serving as the core medium of value transfer within the entire PayFi ecosystem. This stablecoin must not only enable seamless sending, receiving, and settlement both on-chain and off-chain, but also offer broad applicability to support a wide range of financial use cases.

The BenFen Chain's core stablecoin BUSD, is purpose-built to meet the demands of the PayFi ecosystem. Leveraging the security features of the Move language, BenFen's native stablecoins offer significantly higher security during transfers compared to contract-based stablecoin implementations.

This ensures a more stable, efficient, and future-proof foundation for diverse and evolving financial applications. Moreover, BenFen stablecoins enable ultra-low-cost value transfers. Whether in cross-border payments, consumer finance, or supply chain finance, users benefit from unprecedented transaction speeds and minimal fees, unlocking the maximum time value of capital. This efficiency is one of the most powerful advantages PayFi brings to its users.

4.1.2.3 Use Cases of PayFi

Now and in the future, the BenFen stablecoin cluster will play a central role in the PayFi ecosystem, enabling a wide range of on-chain and off-chain financial applications.

- **Asset Trading:** As value-pegged instruments, stablecoins serve as a trading medium against the volatility of crypto assets. Users can utilize stablecoins as the main trading pair on platforms such as BenPay DEX, safely and efficiently facilitating the circulation of various digital assets.
- **DeFi Ecosystem:** In decentralized finance protocols, such as collateralized lending and liquidity mining, users can contribute stablecoin liquidity to platforms like BenPay DEX, becoming active participants in the ecosystem and earning sustained yields.
- **RWA (Real World Assets):** Real-world assets, such as real estate, receivables, and mortgage loans, can utilize stablecoins as settlement and payment instruments, enabling on-chain financing, asset tokenization, and broader financial inclusion.
- **Cross-Border Payments and Trade:** Businesses and individuals can use BenFen stablecoins through applications like BenPay to perform near-instant, low-cost cross-border settlements, thereby bypassing the delays and fees associated with traditional payment networks.
- **Everyday Consumer Payments:** Users can top up BUSD to their BenPay Card, and spend them globally just like a traditional bank card. This bridges the gap between digital assets and real-world consumption scenarios.
- **Payroll & Compensation:** Ideal for freelancers, remote teams, and DAO contributors, transparent on-chain records, and streaming payments (e.g., hourly or real-time). This reduces FX volatility exposure and eliminates high international transfer fees.

By enabling these diverse use cases, BenFen stablecoins drive the adoption of blockchain-based payments across broader fintech domains. They serve as a key pillar in PayFi's mission to achieve global scale, connecting innovative on-chain finance with real-world liquidity needs, delivering a financial experience that is truly usable, trustworthy, and sustainable.

5. One-Click Token Issuance

Currently, issuing tokens on-chain typically requires developers to write and deploy smart contracts—a process that involves complex technical procedures, security audits, and high gas fees. This creates a significant barrier for most non-technical users. The challenge is even greater when dealing with more sensitive asset types, such as stablecoins or real-world assets (RWA), which demand standardized contract templates and robust risk control mechanisms. To address this, BenFen Chain introduces the "One-Click Token Issuance" feature, designed to provide a simple, secure, and configurable entry point for token creation. This functionality supports a wide variety of asset types, including standard crypto tokens, stablecoins, and RWAs, enabling users of all backgrounds — from professional developers to non-technical individuals — to safely and efficiently create and issue their own on-chain tokens.

5.1 Token Issuance Mechanism

BenFen Chain adopts an object-centric model, which is fundamentally different from the account-based architecture used by blockchains such as Ethereum. In this design, tokens are not just balances within user accounts — they are independent objects that encapsulate their own data and ownership. The process of issuing a token, therefore, involves defining and managing a new transferable object via smart contracts, known as Move modules. This object-oriented approach makes the logic around asset transfer, destruction, and lifecycle management more transparent and modular, while also enabling parallel execution, significantly improving on-chain performance and throughput.

To simplify and standardize asset issuance, the BenFen framework includes a built-in core module called coin, which defines standard structures and behaviors for all fungible tokens, such as minting, burning, splitting, and merging. Anyone can invoke the standard functions provided by this module to create tokens without redefining or duplicating standards, ensuring security, interoperability, and consistency across the entire ecosystem.

5.2 Specific Process of Token Issuance

The process of creating and issuing a token on the BenFen Chain follows the steps below:

- 1. Token Parameter Configuration:** The user begins by configuring core parameters via the issuance interface. These include the token name, symbol, minimum unit, and initial total supply at launch.
- 2. Token Type Definition:** Based on the user's input, the system automatically generates a dedicated Move smart contract module. At its core, this module defines a unique witness type—an empty struct that stores no data, but serves as a cryptographic identity for the token across the network. This ensures that the newly created token is uniquely identifiable and distinguishable from all other assets.
- 3. Token Registration:** Once the type is defined, the system deploys the module. During initialization, it automatically invokes a registration function from the official coin module. This step registers the new token on the blockchain and generates a critical on-chain object called TreasuryCap. This object acts as the sole authorization to mint new tokens in the future and is securely transferred to the user's wallet.
- 4. Token Minting and Initial Supply:** Using the TreasuryCap held in the user's wallet, the system automatically executes an initial minting operation based on the total supply defined by the user. The minted tokens are generated as a token object and immediately transferred to the user's wallet.

5.3 Types of Tokenized Assets

Beyond the issuance of standard fungible tokens by project teams, BenFen Chain's One-Click Token Issuance feature also supports two of the most crucial areas in the crypto asset landscape: stablecoins and Real World Asset (RWA) tokenization.

5.3.1 Stablecoins

Stablecoins serve as a vital bridge between digital assets and real-world value, forming the foundational layer of the DeFi ecosystem. On BenFen, users can issue their own stablecoins, but must establish a direct on-chain exchange relationship with external, cross-chain imported mainstream stablecoins to ensure reliable value backing. The process works as follows:

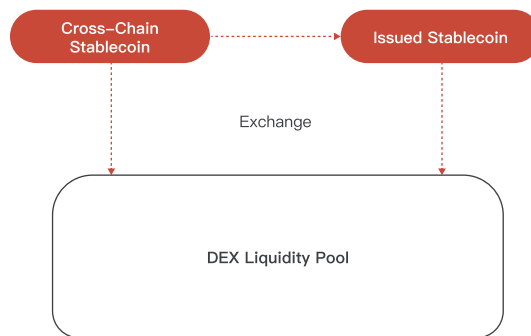


Figure 7: Stablecoins Creation Flowchart

- 1. Introduce Value Reserve:** The issuer must first bridge a certain amount of mainstream stablecoins from other chains to BenFen via the BenFen cross-chain bridge, to serve as the initial reserve.
- 2. Create a Liquidity Pool:** Once the issuer creates a new stablecoin using the One-Click Issuance feature, they are required to set up a liquidity pool on the official BenFen DEX (BenPay DEX), pairing their new stablecoin with an external mainstream stablecoin.
- 3. Maintain Price Peg Stability:** The issuer is responsible for managing the liquidity pool to maintain the stablecoin's price peg. Price data from this pool is continuously monitored by the BenPay DEX oracle, which supplies accurate pricing to other protocols in the ecosystem, such as lending platforms and derivatives exchanges.

The One-Click Stablecoin Issuance feature unlocks a wide range of real-world use cases. Some representative applications include:

- 1. Localized Payments and Settlements:** Enterprises or platforms can issue stablecoins pegged to local fiat currencies to facilitate merchant payments, salary disbursement, and settlements, avoiding FX losses and delays commonly associated with cross-border transactions.
- 2. Web3 Treasury & Fund Management:** Startup teams can issue fiat-pegged stablecoins for early-stage fundraising, operational expenses, and team incentives, ensuring asset stability and reducing financial risks tied to price volatility.
- 3. Supply Chain Finance / Tokenized Receivables:** Businesses can tokenize accounts receivable and other debt-based assets into stablecoins, enhancing liquidity and funding efficiency. These assets can then be split, transferred, or settled on-chain.

4. **Branded or Platform Stablecoins:** Enterprises, DAOs, games, and social platforms can quickly launch their own branded stablecoins as internal settlement units, shielding their in-app economies from volatility and enhancing both user engagement and capital retention.

5.3.2 One-Click RWA Issuance

Introducing real-world assets (RWAs) such as real estate, stocks, bonds, and other tangible assets onto the blockchain through tokenization is a core direction for blockchain to empower the real economy and unlock trillions in asset liquidity. As a key pillar for realizing the vision of a “next-generation real-world payment blockchain,” BenFen Chain leverages the native advantages of the Move language in security (resource model) and programmability to construct a standardized RWA token protocol. This protocol encodes complex processes such as legal compliance, asset verification, and lifecycle management into smart contracts that can execute automatically, aiming to provide an efficient, compliant, one-click issuance and management experience while establishing a scalable, transparent, and trustworthy universal standard.

RWA tokens issued according to this standard are on-chain direct mappings of ownership of specific real-world assets (e.g., financial instruments, commodities, or real estate income rights). The design incorporates three core features that form a foundation of trust: Value Anchoring — Supported by continuous, verifiable off-chain audit. Automatic Cost Accrual — Achieved through a transparent on-chain management fee mechanism. Two-Way Redemption — Ensuring free circulation and the right to ultimately redeem the underlying real-world asset.

All participants must pass KYC/AML identity verification on BenFen Chain to ensure issuance and trading comply with global regulations. Within this compliance framework, the protocol implements the digital issuance and management of assets through the following smart contract mechanisms:

Asset Verification and Audit

Prior to issuance, the issuer must complete and submit third-party verification of the off-chain asset. A key summary (hash) of this proof is recorded on-chain, constituting a prerequisite for issuance:

- **Existence Proof:** Provides warehouse receipts, custodian records, or legal ownership documents.

- **Valuation Proof:** Determines the fair value of the asset based on public market prices, net asset value, or third-party valuation reports.
- **Audit Report:** Issued by a qualified institution, including audit date, scope, asset valuation, and validity period.

Token Issuance

Once the asset verification is approved, the issuer may initiate issuance. The smart contract enforces the following rules:

- **Hard Cap:** The cumulative value of issued tokens must not exceed the net asset value confirmed in the latest audit report.
- **Issuance Record:** Every issuance is linked to a specific version of the audit report and permanently recorded on-chain.

Management Fee Mechanism

The management fee is an optional configuration for the project. Once enabled, the token automatically accrues a management fee during the holding period, calculated proportionally over time. The wallet balance displayed to the user reflects the “net value” after deducting accrued fees, while the market trading price reflects the combined impact of both the underlying asset value and the accrued management fee. This mechanism provides the issuer with a feasible way to cover ongoing operating costs in a transparent and automated manner.

Redemption and Circulation

- **Redemption:** Token holders can initiate a redemption request. The corresponding tokens will be burned, and the issuer delivers the underlying assets offline according to smart contract rules.
- **Circulation:** Tokens can be freely transferred. As high-quality assets, RWAs can flow into the BenFen ecosystem’s DeFi and DEX protocols, improving overall capital efficiency and yield opportunities, and empowering ecosystem assets such as BUSD.

Transparency and Verifiability

All key information is publicly recorded on-chain, allowing any user to independently verify:

- **Current valid audit report information (institution, date, coverage value).**
- **Total token circulation and corresponding asset value.**
- **Management fee rates and cumulative accruals.**

This ensures that the equation “**issued supply ≤ audited asset value**” always holds, and all operational history is fully traceable.

BenFen provides a universal solution for bringing multiple categories of real-world assets on-chain. Typical application scenarios include:

- 1. Real Estate Tokenization:** Property owners or developers can tokenize a piece of residential or commercial real estate using the One-Click Issuance feature. For example, a single property can be split into 100,000 tokenized shares, enabling fractional ownership, financing, dividend distribution, and collateralized lending.
- 2. Commodities On-Chain:** Physical commodities such as gold, silver, oil, and others can be tokenized to represent warehouse receipts, insurance documents, or storage certificates. This facilitates cross-border value transfer and on-chain settlement. For example, a precious metals dealer can issue RWA tokens backed by vaulted gold for fast settlement and risk hedging.
- 3. Art and Collectible Investments:** High-value artworks and collectibles can be fractionalized into RWA tokens, enabling broader participation from retail investors, lowering the investment threshold, and enhancing liquidity in previously illiquid asset classes.
- 4. Music / Film / IP Revenue Rights:** Creators can tokenize future cash flows from music, film, or intellectual property, and sell partial rights for upfront capital. For instance, a musician could issue tokens representing "5-year revenue rights," allowing fans and investors to participate in future royalty sharing.
- 5. Accounts Receivable and Invoicing Assets:** Enterprises can tokenize accounts receivable, invoices, or other debt-based financial instruments via the RWA module. These tokens can be used for on-chain financing, secondary market transfers, and improved liquidity management.

5.4 Paying Gas Fees with Project Tokens

In traditional blockchains, users must pay gas fees using native tokens (such as ETH or BNB) to initiate any transaction. This creates a significant barrier to entry for users—they must first obtain native tokens through specific channels before interacting with applications. To optimize the user experience, BenFen innovatively allows users to pay gas fees directly with whitelisted project tokens. This not only makes on-chain interactions more seamless for users but also provides additional payment utility for tokens issued by ecosystem projects, enhancing their intrinsic value and demand.

This mechanism uses the BenPay DEX oracle to obtain the fair price of project-issued tokens. This price is updated at the beginning of each epoch and remains stable throughout the epoch. When users trade, the system automatically calculates and deducts the equivalent gas fee from the user's project token balance based on this exchange rate.

To protect the entire network from attacks by tokens with poor liquidity and easily manipulated prices, this feature utilizes a community-governed whitelisting system. Projects can submit proposals to have their tokens whitelisted for gas fee payment. The community will vote based on a comprehensive consideration of factors such as project quality, token liquidity, and economic stability. If the proposal receives enough votes in favor, the token will be added to the whitelist and can be officially used to pay gas fees for the entire network.

5.5 Using Sponsored Transactions for Gas Payment

Besides supporting users to pay gas fees with project tokens, Benfen further provides a sponsored transaction feature. Sponsored transactions allow projects to directly cover the gas fees required for user transactions. This significantly lowers the barrier to entry for new users, helping projects attract and retain users more efficiently. Furthermore, projects can selectively sponsor specific types of on-chain transactions to achieve targeted user incentives and ecosystem guidance.

The key to Benfen's implementation of sponsored transactions lies in its transaction structure, which clearly separates the "transaction initiator" from the "gas payer" at the protocol level. This natively decoupled design makes sponsored transactions exceptionally simple to implement, eliminating the need for complex off-chain operations such as "pack-and-forward." Consequently, it significantly reduces development costs and significantly improves transaction security, speed, and transparency.

The specific process for a sponsored transaction is as follows:

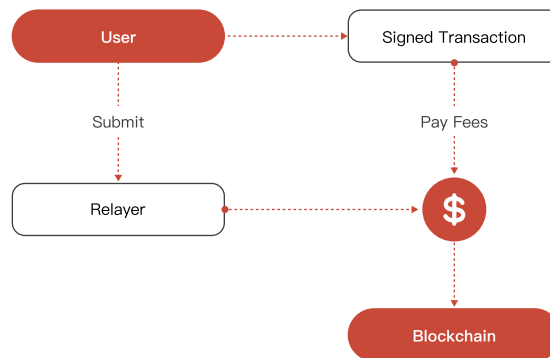


Figure 8: Flowchart of Sponsorship Transactions

1. **User constructs and signs the transaction intent:** When a user initiates a transaction, the DApp constructs a Programmable Transaction Block (PTB) based on the user's intent. This PTB contains the specific on-chain operations to be executed and sets the transaction sender to the user's address. The DApp then requests the user to sign the PTB to confirm their agreement to the intended execution.
2. **Submit the request to the sponsor:** After the user completes the signature, the request data, including the PTB itself and its corresponding signature, will be sent to the sponsor for verification.
3. **Sponsor verifies the request:** After receiving the request, the sponsor performs strict policy validation to prevent abuse. The validation may include user identity, transaction frequency limits, and whether the operations within the PTB fall within the scope of sponsorship, etc.
4. **Sponsor wraps and signs the transaction:** After the validation passes, the sponsor will add gas payment information to the transaction (such as payment address, acceptable gas price, the gas fee limit for this transaction, etc.), and use their private key to sign the complete transaction, authorizing the gas fee to be paid from the sponsor's account.
5. **Transaction submission and on-chain confirmation:** This transaction, containing both the user's and sponsor's dual signatures, is submitted to the BenFen chain node. Before execution, the node will verify the validity of both signatures. After passing verification, the operations in the transaction will be executed, the gas fee will be deducted from the sponsor's account, and the transaction will be completed.

6. Privacy Accounts and Privacy Payments

The transparency of on-chain data is a double-edged sword. For financial applications, the complete disclosure of information such as transaction amounts and account balances not only compromises personal privacy and exposes business secrets, but also hinders large-scale, compliant financial operations from being implemented on-chain.

To address this pain point, BenFen Chain provides native support at the Move virtual machine level, achieving a privacy account and privacy payment system where "data is available but not visible". After a user's assets are deposited into a privacy account, their true balance is completely blocked on the blockchain. In the process of privacy payment, external observers can only capture encrypted interaction records, but cannot know the specific transaction amount. This mechanism ensures the confidentiality of fund flow, reconstructs the privacy paradigm of financial flow from the bottom up, and provides the necessary security foundation and compliance basis for various complex financial scenarios.

6.1 Core Technology

Based on the architecture of the confidential transaction system of FAST MPC and regulatory intervention, BenFen Chain privacy payment system innovatively integrates blockchain technology (Block Node), FAST multi-party computation (FAST MPC), and regulatory compliance mechanism (Regulator). To achieve "data available but invisible" asset transfer in a distributed network, while providing excellent transaction processing speed and low computing costs.

Key Technical Components

1. Block Node

The block node serves as the core of the distributed ledger system, responsible for functions such as transaction verification, consensus, and storage. All transactions (whether Plain Tx or Confidential TX) must be processed by these nodes.

2. Fast Multi-party Computation (FAST MPC)

FAST MPC is the core technology for implementing privacy protection in the system. MPC allows participants to jointly calculate a predetermined function without revealing their respective input data. "FAST" emphasizes that this MPC solution has been optimized for

performance and efficiency to meet the high throughput requirements of the blockchain. The MPC module runs within the Block Node and its main responsibility is to handle key_shard (key fragmentation) and User Private Meta Data, which are used to generate or verify confidential transactions.

3. Key Shard

This is a key element for achieving data security and regulatory intervention. It is generated by the FAST MPC module. User private metadata is encrypted or divided into multiple key shards, which are held by different entities (such as the Block Node and the Regulator). Only by aggregating key shards from different sources (such as the shards of the Block Node and the shards of the Regulator) can the core User Private Meta Data be accessed or decrypted.

Based on this, BenFen Chain will introduce a more decentralized SMPC (Secure Multi-Party Computation) solution in the next stage, dispersing trust from a limited set of verification nodes to a broader network of nodes, significantly enhancing the system's decentralization and resistance to single-point failures/scrutiny. Eventually, BenFen Chain will introduce the full homomorphic encryption (FHE) solution, allowing arbitrary calculations to be performed on encrypted data without decryption, thus enabling privacy computing to evolve to a true zero-trust model, completely eliminating the reliance on trusted intermediaries.

6.2 Detailed Process of Privacy Transactions

The complete life cycle of a typical privacy asset—from creation to use—mainly consists of the following three core stages:

6.2.1 Creation of Privacy Assets: One-Step Privacy Starting from Recharge

BenFen Chain has been improved in architecture by moving privacy selection forward. When users recharge, they can decide whether to recharge the tokens in a private form without multiple steps, providing a smoother experience.

- 1. Initiate Privacy Recharge or Privacy Token Conversion:** When users select to recharge tokens in their wallets, they can simply check the option "Recharge as Privacy Token". In addition, users can also initiate an "asset encryption" transaction through their wallets, specifying the tokens they wish to convert into a private form and the quantity.

2. **Asset Locking:** Once the network confirms the transaction, a special smart contract automatically locks the user's tokens as the value support for the privacy asset being created.
3. **Value Fragmentation:** After receiving the value, network validation nodes use internal shared keys and encryption algorithms to convert the value into a set of unique, non-patterned data fragments.
4. **Certificate Generation:** The system creates a new "privacy asset" object for the user and stores the newly generated data fragments within it.
5. **Completion:** After the transaction is confirmed on-chain, the public tokens are locked, and the user receives an equivalent privacy asset represented by encrypted fragments. The actual value of this asset is no longer visible on the blockchain.

This "recharge as privacy" mechanism eliminates the threshold for users to obtain privacy assets, making privacy protection the default option for on-chain operations rather than a complex additional process.

6.2.2 Privacy Payment

When User A wishes to pay a privacy asset to User B, the process is as follows:

1. **Construct Transaction:** A's wallet creates a transaction indicating B as the recipient and specifying the payment amount. It then sends an authorization request to a trusted validation node, requesting to process the amount into temporary encrypted fragments.
2. **Submit to Network:** The wallet packages the necessary information to execute the transaction and submits it to the network. The transaction includes A's current balance fragments, B's current balance fragments, and the encrypted fragments representing the payment amount.
3. **Backend Computation:** Upon receiving the transaction, the validation node uses shared keys to decrypt and compute the three sets of fragments, and then re-encrypts the result into new encrypted fragments.
4. **State Update:** The computation generates two new sets of data fragments: one representing A's reduced balance, and the other representing B's increased balance. The system then updates these new fragments to A's and B's privacy asset objects, respectively.

5. **Completion:** After the transaction is confirmed on-chain, the value transfer is completed. For any other on-chain user, they can only observe changes in the data within A's and B's privacy asset objects, without knowing the actual transaction amount.

6.2.3 Viewing or Redeeming Assets

When a user wishes to view their actual balance or convert privacy assets back into public tokens, the process is as follows:

1. **Submit Request and Sign:** The user sends a request to a trusted network node via their wallet. The request includes a digital signature generated using the wallet's private key to prove ownership.
2. **Identity Verification:** The node verifies the signature to confirm that the requester is the legitimate owner of the privacy asset on-chain. Identity verification mainly prevents unauthorized access by other users.
3. **Off-chain Restoration:** Once verified, the trusted node reads the user's encrypted fragments from the chain and reconstructs them into a readable balance value using shared keys in its local memory.
4. **Secure Return or Redemption:**
 - **Viewing:** The actual balance is sent back to the user's wallet frontend through a secure, encrypted channel.
 - **Redemption:** The user may authorize a transaction to burn privacy asset proof on-chain. Once confirmed, the originally locked equivalent amount of public tokens will be released and returned to the user.

6.3 Core Features and Differentiated Advantages

6.3.1 Dual-Layer Compliance Design

- **KYC Identity Foundation:** Collaborate with compliance service providers to provide off-chain authentication for enterprise users and generate credentials. This serves as a trust

anchor for all advanced financial activities and also provides a regulatory basis for AML/CFT.

- **Auditable Privacy at Protocol Level:** Based on the **threshold decryption mechanism**, the system has preset a regulatory intervention interface. Specific transaction histories can only be restored upon obtaining a legal judicial order and with the collaboration of multiple parties. This achieves "default privacy, selective disclosure", allowing enterprises to verify compliance with the tax authorities without disclosing the details of each transaction during the audit process.

6.3.2 Ultimate User Experience and Zero Gas Fee Model

BenFen Chain is committed to lowering the threshold for using privacy functions:

- **Seamless Operation:** The steps for privacy transfer are exactly the same as those for regular transfer, and privacy protection runs automatically in the background.
- **Native Sponsorship Transactions:** The protocol layer supports role separation, allowing project parties or merchants to directly pay gas fees on behalf of users, achieving a zero-gas fee experience for users.
- **Native Stablecoin Architecture:** As a "first-class citizen" at the chain layer, stablecoins do not rely on fragile smart contract logic, providing a more solid security foundation for privacy payments.

6.3.3 High Performance and Ecological Scalability

- **Second-Level Confirmation:** The optimized cryptography suite supports a privacy transaction processing capacity of **1,000+ TPS**, meeting high-frequency business demands.
- **All-Dimensional Concealment:** The protection scope covers transaction amounts, sender/receiver addresses, and asset types, fundamentally cutting off the possibility of on-chain data analysis.
- **Batch Operation:** Natively supports enterprise-level batch salary disbursement, airdrop, and other scenarios, perfectly combining efficiency and privacy.

7. BenPay DEX

BenPay DEX is different from third-party DEX on other public chains. Instead, it is a native decentralized exchange built on the underlying system of the BenFen chain. It is not only the core trading platform of the BenFen blockchain but also a crucial prerequisite for the stability mechanism of BenFen Stablecoins.

7.1 BenPay DEX Features

BenPay DEX has the same Liquidity Pool and Automated Market Maker (AMM) model design that regular DEX has. For each transaction, BenPay DEX charges the user of the transaction a commission of 0.1% (in the form of BUSD), of which 50% is used to incentivize liquidity providers and 50% is used to increase the protocol reserve.

Besides, BenPay DEX has several key advantages:

- 1. Trading Convenience:** Stablecoins provide relatively stable value storage, allowing users to trade without worrying about significant price fluctuations.
- 2. Concentrated Liquidity Provision:** BenPay DEX introduces the concept of concentrated liquidity, allowing liquidity providers (LPs) to provide liquidity within a specific price range rather than the entire price spectrum.
- 3. Promoting Ecosystem Development:** A robust DEX can attract more users and developers to join the BenFen blockchain ecosystem. Stablecoins as a trading base can promote the development of more decentralized applications (DApps) and services, driving the growth and prosperity of the entire ecosystem.

7.2 BenPay DEX Built-In Oracle System

The Oracle system of BenPay DEX plays a crucial role in the platform, tasked with providing accurate and real-time asset price information to ensure fairness and transparency in the trading market. The Oracle system of BenPay DEX leverages the advantages of the CLAMM framework and the Move programming language to offer users efficient and secure trading services. By enhancing the authenticity, accuracy, and stability of price information, BenPay DEX builds a trustworthy digital asset trading ecosystem that helps ensure the healthy

operation of the market and increases user confidence and participation in the platform. The main features of the Oracle system are:

- **TWAP (Time-Weighted Average Price) Mechanism:** The Oracle system of BenPay DEX adopts the TWAP calculation method, which relies on average prices rather than instantaneous ones. TWAP smooths out price fluctuations by averaging prices over a period of time, reducing the impact of short-term manipulations and abnormal fluctuations to ensure price stability and credibility.
- **Price Sliding Window:** The Oracle system uses a price sliding window technique to update price data continuously. This ensures that the most recent and relevant price information is always available, effectively preventing price delays or discrepancies.
- **Anti-Manipulation Mechanisms:**
 - **Cooldown Period:** After each price update by the Oracle system, a cooldown period is set during which no further updates are allowed. This effectively limits the risk of market manipulation due to frequent price changes.
 - **Price Deviation Threshold:** If the new price significantly deviates from the current price beyond a preset threshold, the price data will not be accepted, ensuring price stability and reasonableness.
- **Transparency Commitment:** BenPay DEX is committed to ensuring that all price updates and activities of the Oracle system are open and transparent. This means that anyone can verify the accuracy and authenticity of the price data, ensuring a high level of transparency on the platform.

8. BenFen Bridge

BenFen Bridge is a cross-chain bridge connecting the BenFen chain with multiple mainstream public chains. It not only supports interoperability of native assets across different chains but also supports cross-chain minting of mainstream stablecoins such as USDT and USDC from multiple public chains into BenFen chain's native stablecoin BUSD.

To balance security, efficiency, and broad compatibility, BenFen Bridge includes both the BenFen native cross-chain bridge based on smart contracts and cross-chain bridges for heterogeneous chains like Bitcoin and Solana realized through a node network. The native cross-chain bridge, based on smart contracts, ensures decentralized asset transfers between EVM-compatible chains. For heterogeneous chains, such as Bitcoin and Solana, that are non-EVM compatible, cross-chain is achieved via an efficient node network, ensuring faster processing speeds.

Currently, BenFen Bridge supports bidirectional cross-chain asset transfers involving multiple public chains and L2s, including Bitcoin, Ethereum, Solana, TRON, BNB Chain, Optimism, and Base. We are actively developing decentralized cross-chain solutions for Solana and TRON and plan to continue expanding to integrate more mainstream public chains in the future, building a seamless and interconnected blockchain ecosystem.

8.1 Native BenFen Bridge

BenFen Bridge, a native cross-chain bridge on Benfen Chain, is a secure, decentralized, and scalable cross-chain aggregation solution. It adopts the most popular locking and minting mechanism, i.e., BenFen Bridge will lock ETH as a native asset in the smart contract on Ethereum, and mint or destroy the corresponding assets on the subchain according to the direction of the inflow and outflow of cross-chain assets.

As a native cross-chain bridge on the local chain, BenFen Bridge does not require additional trust assumptions. The nodes that provide security for the local chain will also provide security for BenFen Bridge, and the code of BenFen Bridge will be integrated into the code of the local chain.

8.1.1 BenFen Bridge Key Components

- **BenFen Bridge Committee:** In order to inherit the security of BenFen Chain, BenFen Bridge Committee or Bridge Node Network is aligned with the active verifiers of BenFen Chain. Nodes are responsible for observing, verifying, and signing cross-chain events. In addition, the nodes also sign Solidity and Move contract upgrade approvals and emergency governance requests.
- **BenFen Bridge Smart Contracts:** Includes the Solidity contract on Ethereum and the Move contract on BenFen, which handles the locking, minting, and destruction of assets.
- **Full Nodes:** Full Nodes running on Ethereum and BenFen are responsible for listening to cross-chain events or providing verification information to ensure the legitimacy of cross-chain events, providing support for BenFen Bridge nodes and clients.
- **Cross-Chain Client:** The client is the interface for users to interact with BenFen Bridge. The client submits correctly formatted transaction information and collects signatures from BenFen Bridge nodes (signature nodes need to stake more than 1/3 of the funds) to help users complete cross-chain operations.

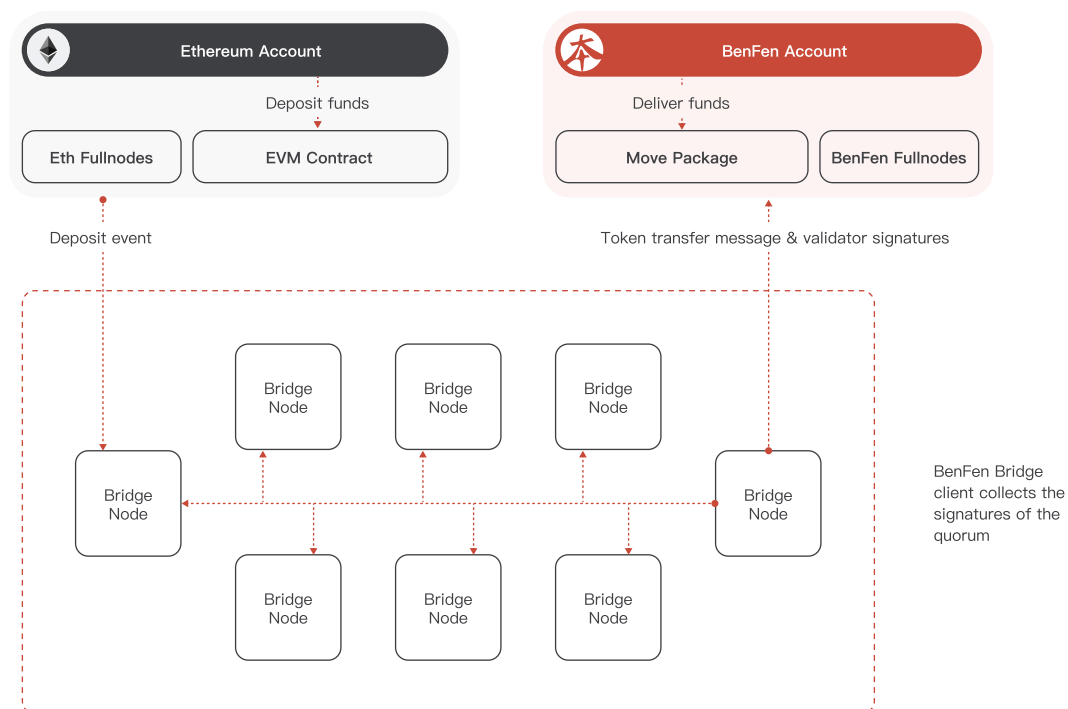


Figure 9: BenFen Bridge Structural Diagram

8.1.2 Cross-Chain Process

Taking the process of a user performing cross-chain transfer from an EVM chain to the BenFen chain via BenFen Bridge as an example, the entire process can be divided into the following steps:

- 1. Initiate Cross-chain Request and Lock Assets:** The user initiates a cross-chain operation via the BenFen Bridge contract deployed on the EVM chain, specifying the token type, amount, target chain (BenFen), and receiving address. Upon receiving the request, the Solidity contract locks the corresponding user assets, records the transaction information on-chain, and triggers a cross-in event.
- 2. Event Listening and Verification:** The BenFen Bridge node network listens in real time for cross-chain events from the EVM chain. Once the user's cross-chain request is captured, the Bridge nodes verify the event's validity and signatures, and prepare to construct the corresponding transaction on the BenFen chain.
- 3. Construct Target Chain Transaction:** After verification, the Bridge nodes construct a cross-chain asset minting or transfer transaction on the BenFen chain. This transaction will send the equivalent assets to the user's specified BenFen chain address according to the user's request, while retaining the original cross-chain information for traceability.
- 4. Multi-signature Confirmation and Broadcast Execution:** The constructed transaction is co-signed by multiple Bridge nodes. When the number of node signatures reaches a preset threshold (default 75%), the transaction is officially submitted and executed on the BenFen chain, completing the final release of cross-chain assets. The user then receives the corresponding assets on the target chain.

The process for users transferring assets from the BenFen chain to other EVM chains is the reverse. The user initiates the cross-chain operation on the BenFen chain, where the contract destroys the assets and generates a transaction proof. The Bridge node network listens to the destruction event, verifies it, and jointly signs a "claim proof." The user can then perform a "claim" operation on the target EVM chain using this proof. Once the contract verifies the validity of the proof, it unlocks the originally locked assets and sends them to the user.

8.1.3 Risk Prevention Measures

To further ensure the security of cross-chain bridges, BenFen Bridge has also taken several

measures to minimize risks:

- **Replay Protection:** To avoid replay attacks, each cross-chain transaction will contain a random number (nonce), and if the random number has been used before, the cross-chain transaction will fail.
- **Cross-chain Finality Confirmation:** In order to reduce the impact of possible reorganization risks in Ethereum, Ethereum transactions will not be considered valid until their blocks are finalized (≥ 2 epochs), which means that a cross-chain transaction from Ethereum to the local branch chain will take about 13 minutes to settle. However, transactions from BenFen Chain to Ethereum are not affected by this and can be finalized in seconds.
- **Committee Management:** Each active verifier is part of a cross-chain committee that is refreshed after each epoch change on the local branch chain, and verifiers rotate their keys for signing certifications or approvals, which take effect on the next epoch. The committee's information is stored in the Ethereum Contract, and the information in the Ethereum Contract is updated synchronously at the start of each epoch of the current subchain. Updates require more than 1/3 of the votes.
- **Contract Upgrades:** Contracts on the local chain require at least 2/3 of the validators to approve an upgrade, and contracts on Ethereum require at least 1/2 of the validators to approve an upgrade.
- **Emergency Pause Mechanism:** In the face of an unexpected catastrophic event or failure, an emergency pause can be used, where all operations are halted until they are lifted. The threshold for initiating an emergency pause is set relatively low to ensure that damage can be stopped quickly in the event of an emergency. To lift an Emergency Pause, more than 1/2 of the staked funds need to be agreed upon.
- **Limit Protection:** BenFen Bridge supports a variety of flexible limit measures, including single transaction, different directions, cumulative 24 hours, and limit based on amount steps, to strike a balance between user convenience and the security of the Bridge vault.

8.2 Cross-Chain Based on Node Network

For EVM-compatible chains that support Turing-complete smart contracts, BenFen Bridge can achieve the complete cross-chain process through the native BenFen Bridge, which is

fully automated, requires no trusted intermediaries, and offers high composability and security. However, for heterogeneous chains such as Bitcoin that do not support Turing completeness, it is impossible to rely on smart contracts to complete on-chain logic verification and state transitions. To achieve asset cross-chain with such chains, BenFen Bridge introduces a second mechanism — a node network—based cross-chain solution. This solution combines multi-node listening, signing, and auditing to ensure security while enabling secure cross-chain transfers of assets on non-contract chains.

In this cross-chain method, BenFen Bridge Nodes act as cross-chain relays, responsible for listening to, signing, and forwarding cross-chain transaction events between Bitcoin and the BenFen chain. Users can use this bridge to achieve bidirectional flow of mapped assets between Bitcoin and the BenFen Chain.

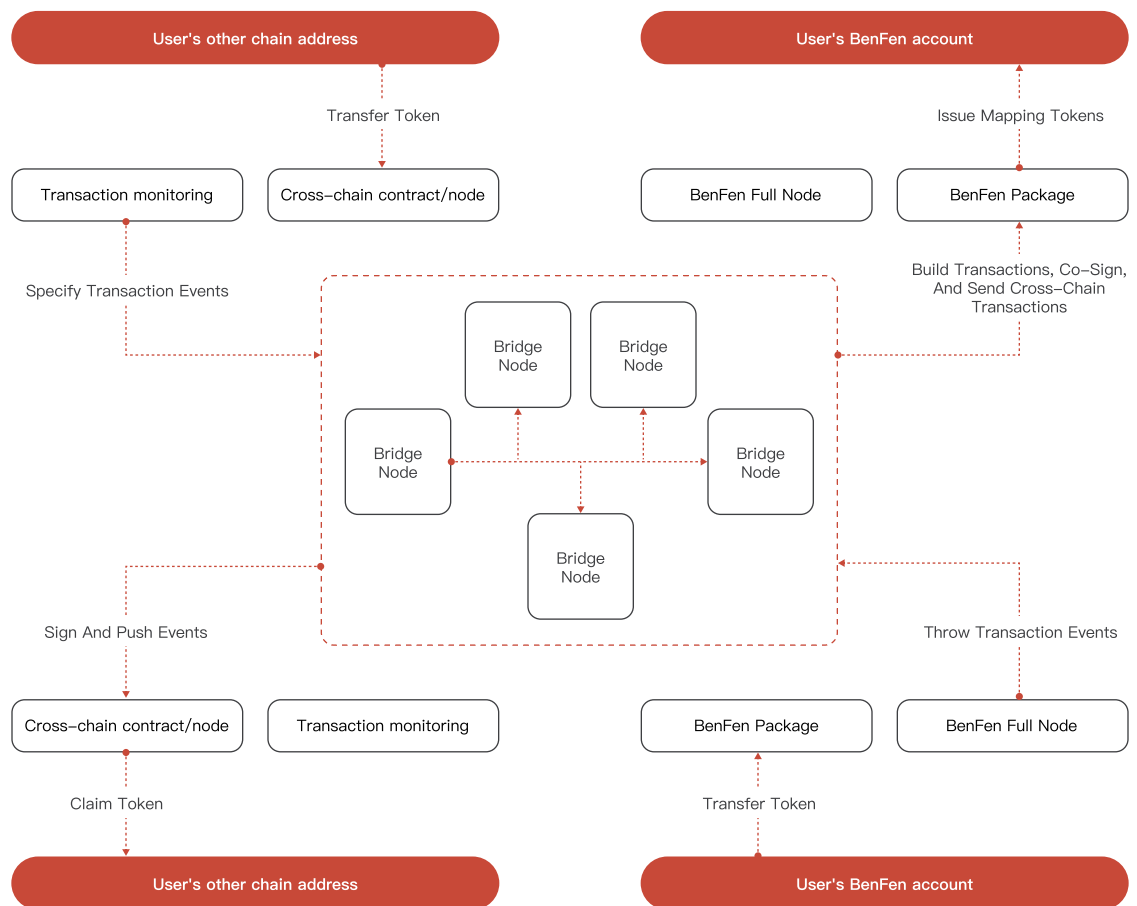


Figure 10: Cross-Chain Flowchart of Node Network

8.2.1 Cross-Chain Process

When a user wants to cross-chain native BTC to the BenFen chain and receive the mapped asset bBTC, the process is as follows:

- 1. Initiate Transfer:** The user sends a certain amount of BTC to the specified BTC address provided by the cross-chain service on the Bitcoin network, attaching the target chain (BenFen), target address, and transfer amount in the transaction.
- 2. Event Listening and Confirmation:** After the transaction reaches the required number of confirmations, the on-chain transaction information is generated. The Bridge Node network detects the relevant transaction event, extracts the transaction details, and prepares to trigger the minting of the mapped asset on the BenFen chain.
- 3. Construct and Sign Cross-chain Transaction:** The Bridge Node constructs a transaction on the BenFen chain to mint bBTC. After multi-node signatures reach the threshold, the transaction is sent to the BenFen chain for on-chain confirmation.
- 4. Asset Arrival:** Once the transaction is executed, the user's BenFen chain address will receive the minted equivalent amount of the mapped asset bBTC, completing the cross-chain process.

When a user wants to redeem held bBTC back to native BTC, the outbound process is as follows:

- 1. Initiate Burn Request:** The user calls the burn function on the BenFen chain to destroy the specified amount of bBTC, and fills in the outbound target chain (Bitcoin) and receiving address.
- 2. Generate Cross-chain Proof:** The burn transaction on the BenFen chain is monitored and extracted by the Bridge Node network. The nodes jointly generate a burn-proof document and perform multi-signature verification.
- 3. Service Verification and Audit:** Upon receiving the fully signed proof document, the cross-chain service conducts validity verification. To further enhance security, this process includes a manual audit step.
- 4. BTC Release:** After passing the audit, the system sends the equivalent amount of BTC from the BTC reserve address to the user's specified Bitcoin address, completing the cross-chain.

9. BenFen Ecosystem

BenFen is committed to building a globally leading stablecoin financial infrastructure. Its core goal is to provide seamless and low-threshold support for financial activities such as payments, trading, and lending through a native stablecoin system, on-chain identity authentication, and high-performance infrastructure. Centered around the BenFen public chain, the ecosystem gradually develops multiple submodules including BenPay, BenPay DeFi Earn, BenPay Card, BenPay Lending, BenPay DEX, BenPay Merchant Services, and BenPay Shop, forming a unified entry point with modularly expandable financial applications.

9.1 BenPay: Web3 Stablecoin Financial Super App

BenPay is the core financial application platform of the BenFen ecosystem, integrating multiple functions such as on-chain payments, non-custodial lending, and order matching. It is positioned as the **“BenFen on-chain super app.”**

As the main user gateway of the BenFen ecosystem, BenPay is built on the BenFen public blockchain, fully leveraging its sub-second block confirmation, low gas costs, and native stablecoin support to provide users with an integrated, multifunctional, secure, and compliant financial experience. Its goal is to eliminate cross-chain fragmentation and operational barriers when users use stablecoin assets for consumption, and lending, constructing a more efficient and open global payment and financial services network.

Currently, the BenPay platform includes the following submodules:

9.1.1 BenPay DeFi Earn

BenPay DeFi Earn serves as a unified gateway within the BenFen ecosystem, providing users with direct access to leading multi-chain DeFi protocols. Its core lies in addressing the operational complexity and high barriers that users encounter when exploring and participating in decentralized finance.

As a key entry point connecting users to the DeFi world, BenPay DeFi Earn is designed with a strong focus on optimizing the interaction process and asset management mechanism. Its main advantages include:

BenPay DeFi Earn serves as a unified gateway within the BenFen ecosystem, providing users with direct access to leading multi-chain DeFi protocols. Its core lies in addressing the operational complexity and high barriers that users encounter when exploring and participating in decentralized finance.

As a key entry point connecting users to the DeFi world, BenPay DeFi Earn is designed with a strong focus on optimizing the interaction process and asset management mechanism. Its main advantages include:

- **Full Asset Control:** Users retain complete ownership of their assets at all times. Funds remain in personal wallets — the platform does not hold or access user assets, ensuring full self-custody.
- **Selected Top Protocols for Access:** All deployable protocols undergo multidimensional screening for security and stability, ensuring only high-quality, industry-leading DeFi protocols are included.
- **Flexible Redemption Mechanism:** Assets can be redeemed at any time, providing strong liquidity and avoiding the usage restrictions of traditional lock-up models.
- **Zero Gas Costs:** Any on-chain operation usually requires paying gas fees. However, on the BenFen blockchain, the platform will pay the gas fees for your investment and redemption, eliminating the need for users to pay additional fees.
- **Security Audit Guarantee:** The BenFen blockchain's core smart contracts have undergone a comprehensive security audit by SlowMist, an authoritative security institution, ensuring system security and contract reliability.

9.1.2 BenPay Card: On-Chain Stablecoin Payment Card

BenPay Card is an important tool within the BenFen ecosystem designed to realize native on-chain stablecoin payments, aiming to promote the seamless circulation and popularization of crypto assets in the real world. The card service is fully built on the BenFen public chain, relying on on-chain identity, native stablecoins, and wallet authorization mechanisms. Users can bridge mainstream stablecoins such as USDT and USDC into BenFen Chain's native stablecoin (BUSD) for direct consumption, covering major online and offline payment scenarios.

BenPay Card adopts a self-custody model, where card access rights are granted by users via on-chain wallet signature authorization, ensuring asset control always remains with the users themselves. Card activation requires no token staking or asset pre-deposit, and the application process is compliant and streamlined, with strong universality and scalability.

In terms of payment experience, BenPay Card implements off-chain fiat payments with automatic settlement mapping to on-chain stablecoin assets. Users' funds can be used immediately for consumption after top-up without additional exchange steps, reducing friction in the payment path. The system supports multi-chain stablecoin asset top-ups and withdrawals, currently covering major networks including Ethereum, Solana, Tron, BSC, Polygon, Arbitrum, Optimism, Base, Avalanche, etc., further enhancing asset liquidity and user accessibility.

To enhance asset security, BenPay Card integrates card freezing controls, on-chain authorization verification, and encrypted data transmission mechanisms, supporting transaction identity verification and permission control without exposing sensitive information, ensuring operation security.

As a vital component of the BenPay payment ecosystem, BenPay Card provides a native payment bridge connecting on-chain assets and real-world consumption. Its launch not only improves the efficiency and scope of stablecoin usage but also further promotes the deployment and popularization of the BenFen ecosystem in the PayFi (payment finance) domain.

9.1.3 BenPay Lending: Decentralized Lending Protocol

BenPay Lending is the decentralized lending protocol under the BenPay platform, adopting a "matching cycle" design that pairs borrowers and lenders each lending cycle to form stable interest rates. Users can borrow stablecoins (e.g., USDT) by collateralizing mainstream crypto assets (e.g., BTC, ETH). The platform contract is fully non-custodial, with on-chain liquidation and risk control mechanisms in place.

Key Features:

- Cycle-based matching for predictable interest rates;
- Support for multiple collateral types;
- Transparent on-chain risk control;
- Flexible repayment paths to suit different user asset preferences.

9.1.4 BenPay Merchant Services

BenPay provides merchants with stablecoin payment solutions supporting the acceptance of major digital assets such as USDT, USDC, and ETH across multiple blockchains. Merchants can quickly generate payment addresses via API, receive on-chain transfers from users, and obtain real-time payment status through webhook callbacks. Supported networks include Ethereum, Tron, BSC, Polygon, Arbitrum, Optimism, etc. The system features high reliability monitoring to help merchants automate chain payments and control workflows.

9.1.5 BenPay On-Chain Red Packets

BenPay innovatively launched the on-chain red packet function, allowing users to send digital red packets of stablecoins via links or QR codes. This feature suits community distribution, user incentives, and social interaction scenarios.

9.2 Technical Foundation and Ecosystem Support

All BenPay service modules are built on the BenFen public chain, supported by the following core capabilities:

- **High-performance Layer 1 Architecture:** constructed with Move language, delivering high throughput and low latency;
- **Stablecoin System:** BUSD is minted by locking mainstream stablecoin assets with 1:1 redemption, ensuring strong stability;
- **zkLogin Non-Custodial Wallet:** supports creating on-chain identities via Google / Apple accounts, lowering user onboarding barriers;
- **Native Cross-Chain Bridge:** BenFen Bridge enables interoperability with major chains, including BTC, ETH, BSC, Polygon, Optimism, Solana, etc..
- **Gas Payments in Stablecoins:** The platform natively supports paying Gas fees with stablecoins, simplifying the user experience.

9.3 Compliance and Security Assurance

BenPay is operated by a US-registered fintech entity holding an MSB (Money Services Business) license issued by the US Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) (registration number: 31000260888727), legally qualified to conduct virtual asset transactions and prepaid account services. The on-chain core smart contracts have been audited and certified by a third-party security firm, SlowMist, ensuring user asset and protocol security.

9.4 Summary

BenPay is not only a key financial application within the BenFen ecosystem but also a "super-app" driving the popularization of stablecoin payments and DeFi. Its multifunctional, integrated architecture, self-custody user control model, deep optimization of stablecoins, and excellent compatibility with traditional payment scenarios position it as a potential next-generation global payment platform.

Going forward, BenPay will continue to expand its service boundaries, covering a wider range of asset types and payment scenarios, thereby accelerating stablecoin adoption within mainstream global financial systems.

10. BenFen ID: An On-Chain KYC and Privacy-Preserving Identity Layer

As real-world financial use cases such as on-chain payments, asset issuance, RWA trading, and lending continue to expand, public chains require more than high performance, low costs, and composable financial infrastructure. They also need a universal identity layer that can support compliant identity verification without exposing users' sensitive personal information.

BenFen ID is introduced in this context as BenFen's on-chain KYC capability. It functions as an on-chain identity credential. After completing identity verification, users can prove that they meet specific identity requirements across DApps or services that support BenFen ID, such as having completed KYC, meeting age requirements, or satisfying regional access rules, while minimizing the direct exposure of full identity data such as names, ID numbers, and dates of birth.

BenFen ID combines off-chain KYC, on-chain credentials, zero-knowledge proofs, and DApp authorization verification to provide a reusable identity foundation for PayFi, RWA, privacy-preserving payments, and compliant financial applications within the BenFen ecosystem.

Its core objective is not to publish complete identity data on-chain, but to establish a balance between verifiability and minimal disclosure. This enables BenFen ID to:

1. Provide users with a reusable identity capability that supports one-time verification across multiple scenarios, reducing the need to repeatedly submit identity documents to different DApps.
2. Provide projects with a composable identity verification gateway, allowing DApps to verify whether users meet specific access requirements based on their own rules, without directly handling users' full identity documents.
3. Enable verification contracts to validate a user's KYC status through a ZK Proof-based mechanism, without exposing the user's underlying identity information.
4. Provide users and projects with traceable on-chain verification and authorization records, instead of allowing raw identity data to be distributed in an uncontrolled manner.

5. Integrate with BenFen's existing ecosystem modules, including stablecoins, RWA, privacy-preserving payments, and BenPay, forming a compliance-ready identity foundation for real-world payment and financial applications.

10.1 Core Mechanism

From a system architecture perspective, BenFen ID is composed of four key roles.

- **User:** The entity that obtains KYC verification and holds a BenFen ID. During the verification process, the user submits the necessary identity information and, in subsequent interactions with DApps, chooses whether to authorize the verification of specific identity conditions.
- **Issuer:** The party responsible for conducting off-chain KYC verification and issuing NFTs and VCs (Verifiable Credentials) based on the verification results. The Issuer is responsible for verifying identity documents and performing liveness verification.
- **Verification Requester:** The role that needs to obtain a user's KYC verification status or identity condition verification result, typically a DApp project team or service provider. The Verification Requester sets verification requirements based on its business rules, such as whether the user has completed KYC, whether the user is at least 18 years old, or whether the user complies with regional access rules.
- **Verifier Contract:** The smart contract that verifies a user's KYC status or identity conditions through zero-knowledge proofs without exposing specific identity information. The Verifier Contract outputs the verification result to the DApp and may trigger on-chain verification records according to business requirements.

10.1.1 Credential Model and Privacy Principles

BenFen ID adopts a model commonly used in zero-knowledge identity systems: one-time verification, user-held credentials, selective proof, and on-chain verification. Its core purpose is not to convert KYC data into publicly accessible on-chain records, but to transform real-world identity verification results into verifiable cryptographic credentials. This allows users, when accessing DApps or on-chain financial services, to prove only that they meet specific identity conditions, without disclosing their full identity information by default.

In this model, off-chain KYC is responsible for verifying the user's real-world identity, while on-chain verification is responsible for confirming whether the user satisfies a specific condition. These two layers are connected through the Issuer, the identity credential held by the user, zero-knowledge proofs, and the Verifier Contract. As a result, BenFen ID transforms identity verification from a process of repeatedly submitting personal information into a reusable on-chain capability that can be applied across multiple business scenarios.

From a technical perspective, the privacy protection of BenFen ID relies primarily on three mechanisms.

First, signed credentials. The Issuer signs the identity verification result, allowing DApps to verify the source and authenticity of the credential without having to perform KYC repeatedly.

Second, cryptographic commitments. User identity attributes can be converted into hashes or commitment values, which are used to prove that a specific identity fact exists and has not been tampered with, while avoiding the direct disclosure of the original data fields.

Third, zero-knowledge proofs. Users can prove that they hold a valid credential and that the attributes within the credential satisfy the conditions required by a DApp, without disclosing the full contents of the credential.

This design enables BenFen ID to support two identity usage models at the same time. By default, DApps receive condition-based verification results, such as whether a user has passed KYC, whether the user meets an age threshold, or whether the user satisfies regional or risk-level requirements. This model is suitable for scenarios such as access control, lending, RWA participation, and DAO eligibility.

In scenarios where the user provides explicit authorization, a DApp may also obtain specific information that the user has authorized for disclosure and verify that such information is derived from a valid credential. The former emphasizes minimal disclosure, while the latter emphasizes authorized disclosure. Together, these two models define the privacy boundaries of BenFen ID.

10.1.2 Identity Verification and Credential Issuance

As real-world financial use cases such as on-chain payments, asset issuance, RWA trading, and lending continue to expand, public chains require more than high performance, low costs, and composable financial infrastructure. They also need a universal identity layer that can support compliant identity verification without exposing users' sensitive personal information.

BenFen ID is introduced in this context as BenFen's on-chain KYC capability. It functions as an on-chain identity credential. After completing identity verification, users can prove that they meet specific identity requirements across DApps or services that support BenFen ID, such as having completed KYC, meeting age requirements, or satisfying regional access rules, while minimizing the direct exposure of full identity data such as names, ID numbers, and dates of birth.

BenFen ID combines off-chain KYC, on-chain credentials, zero-knowledge proofs, and DApp authorization verification to provide a reusable identity foundation for PayFi, RWA, privacy-preserving payments, and compliant financial applications within the BenFen ecosystem.

Its core objective is not to publish complete identity data on-chain, but to establish a balance between verifiability and minimal disclosure. This enables BenFen ID to:

- 1. Identity information submission and initial claims:** The user submits the basic identity information and identity documents required to complete identity verification, forming the identity claims to be verified.
- 2. Document authenticity and subject consistency verification:** The Issuer combines third-party verification capabilities to validate the authenticity of the identity documents, the consistency between the document holder and the applicant, and liveness features, in order to confirm the authenticity of the applying subject.
- 3. Identity credential issuance:** After verification is completed, the Issuer signs the user's identity attributes based on the verification results and generates an identity credential that can be used for subsequent proofs. This credential carries verifiable identity facts rather than a public identity profile.
- 4. User custody and secure storage:** The identity credential is held by the user and stored through local encryption or controlled backup mechanisms, supporting subsequent proof generation, device migration, and identity recovery.

5. On-chain state registration and BenFen ID issuance: Once the protocol requirements are satisfied, the system registers the user's KYC status within the on-chain identity system and completes the issuance of BenFen ID, indicating that the user has obtained an on-chain verifiable identity capability.

From a technical boundary perspective, off-chain verification is responsible for confirming the user's real-world identity, while on-chain issuance is responsible for confirming that this identity has been transformed into an accessible verification capability. What BenFen ID represents is a verified identity status and provable identity conditions, rather than a public collection of personal identity data.

10.1.3 Verification Rules and Execution Mechanism

At the verification layer, BenFen ID is not designed as a standalone KYC form module. Instead, it provides a rule-based mechanism that abstracts business compliance requirements into on-chain verifiable conditions. In different application scenarios, the purpose of identity verification is typically not to repeatedly collect users' complete identity information, but to determine whether a user satisfies specific participation requirements, such as having completed KYC, meeting an age threshold, or complying with regional and risk-related restrictions.

Under this mechanism, business rules may consist of one or more identity conditions and can be combined through logical relationships to form scenario-specific verification policies. Once defined, these rules can be standardized into rule identifiers and converted into verification requests that users can respond to. In this way, off-chain compliance requirements are mapped into on-chain executable identity evaluation logic, enabling scenarios such as registration, transactions, asset subscription, RWA participation, lending access, DAO governance, and merchant services to share the same identity verification layer.

The execution process is a direct extension of the rule mechanism. When an application initiates an identity verification request, the user-side client initiates the proof generation process based on the valid identity credential stored locally. If the user does not yet hold a valid credential, the user must first complete identity verification and credential issuance. If the user already holds a valid credential, the user can generate the corresponding proof according to the predefined rules and submit the verification result after authorization.

What is verified in this process is not the user's specific identity information, but whether the predefined identity conditions are satisfied. The application only receives the rule verification result, rather than raw identity fields such as the user's name, identity document number, or date of birth. As a result, BenFen ID transforms identity verification from the transmission of identity information into a proof of rule satisfaction, thereby enabling a strong privacy-preserving verification mechanism for on-chain use cases.

In scenarios that require on-chain confirmation, the proof result can be further submitted to the Verifier Contract. The Verifier Contract verifies the credential source, the validity of the proof, and whether the proof satisfies the current rule. The contract outputs only the necessary verification conclusion and related records, without disclosing specific identity fields or the original credential content. Based on this result, the application determines whether to proceed with the subsequent business logic, while the on-chain records provide a foundation for auditing, traceability, and compliance review.

The key significance of this mechanism is that on-chain applications obtain a verifiable conclusion on whether specific identity conditions are satisfied, rather than the user's complete identity data itself. This enables BenFen ID to meet compliance access requirements while preserving the principle of minimal disclosure, allowing identity capabilities to become reusable and composable general-purpose infrastructure within the BenFen ecosystem.

10.2 Key Features

- **Minimal Disclosure and Verifiability:** A core feature of BenFen ID is that it transforms identity verification from "submitting complete identity documents" into "proving that specific conditions are satisfied." By default, applications receive verifiable conclusions rather than raw identity data, thereby minimizing privacy exposure while meeting business requirements.
- **Composable Compliance Verification:** Through rule-based condition expression and a unified verification interface, BenFen ID can abstract compliance requirements across different scenarios into composable identity conditions. Different applications can build their own access logic on top of the same identity layer, without having to repeatedly develop the underlying identity verification infrastructure.

- **On-Chain Auditability and Ecosystem Scalability:** A core feature of BenFen ID is that it transforms identity verification from "submitting complete identity documents" into "proving that specific conditions are satisfied." By default, applications receive verifiable conclusions rather than raw identity data, thereby minimizing privacy exposure while meeting business requirements.
- **Composable Compliance Verification:** While preserving user privacy, BenFen ID retains on-chain verification records and authorization records, making identity verification results traceable and auditable. As more payment, RWA, privacy finance, and governance scenarios are integrated, this mechanism can further evolve into a general-purpose compliant identity layer within the BenFen ecosystem.

10.3 Application Scenarios

The introduction of BenFen ID enables identity verification capabilities to be embedded as general-purpose infrastructure across different business modules within the BenFen ecosystem. This allows applications to meet compliance access requirements for real-world financial activities while preserving user privacy.

- **PayFi and Stablecoin Payments:** In PayFi and stablecoin payment scenarios, BenFen ID can serve as a unified identity foundation for payment access, merchant services, risk segmentation, and eligibility checks for specific financial products. By moving identity condition verification to the front of the transaction process, applications can complete the necessary compliance checks without directly handling users' complete identity information, thereby reducing the friction costs associated with repeated KYC procedures.
- **RWA and Compliance Access:** In RWA scenarios, identity verification is a critical prerequisite for issuance, subscription, transfer, and redemption. BenFen ID can abstract rules such as investor suitability, regional restrictions, and KYC/AML requirements into on-chain verifiable conditions. This allows project teams to implement access control without repeatedly collecting users' identity information, while improving the circulation efficiency of compliant assets on-chain.

- **Privacy–Preserving Payments and Selective Disclosure:** In privacy–preserving payment scenarios, BenFen ID naturally aligns with the design principle of "privacy by default, selective disclosure when required." Transaction amounts and behavioral information can remain private, while the identity layer can still provide verifiable access control and auditability when necessary. As a result, privacy protection and compliance requirements are no longer mutually exclusive, but can be made compatible through credentials and proof mechanisms.
- **Lending, DAO Governance, and Merchant Services:** In scenarios such as lending, DAO governance, and merchant services, BenFen ID can be used to determine whether users meet participation thresholds, regional rules, risk–level requirements, or governance eligibility criteria. Its value does not lie in replicating one KYC page after another, but in providing a unified identity verification primitive for the entire ecosystem, allowing real–world identity conditions to be reused by on–chain applications in the same way as assets and payment capabilities.

11. Governance

11.1 BenFen DAO and On-Chain Governance

BenFen has successfully implemented an open, transparent, and fair governance DAO (Decentralized Autonomous Organization) system designed to assist users in safeguarding their interests. Through our DAO system, any user can start proposals at a very low cost and actively vote on any on-chain transactions, engage in community governance, and protect and advocate for their rights.

Decentralized governance plays a crucial role in the Blockchain space, and our designed on-chain governance mechanisms encompass various essential processes such as managing group proposals, user voting, decision making, and execution. These processes are embedded in system modules in the form of smart contracts to ensure the integrity and transparency of governance. Additionally, contract developers can reuse these governance modules to easily incorporate DAO mechanics into their own DApps.

BenFen's DAO system provides users with a powerful tool, enabling them to actively engage in the decision-making process and ensure the full protection of their interests. This innovative design is expected to further drive community participation, promote the maturity and development of the Blockchain ecosystem, and provide users with a stronger voice in collectively building a more trustworthy and robust Blockchain ecosystem.

11.2 Working Mechanism and Proposal Status

1. **[pending]:** Any user can initiate a proposal by staking tokens. The proposal enters the pending stage, during which users can review and discuss the proposal;
2. **[active]:** After the pending stage, the proposal enters the active voting stage. During this period, any user can vote in favor or against the proposal by locking their tokens in the voting pool;
3. **[defeat]:** When the voting stage ends, if the number of votes against the proposal exceeds the number of votes in favor or if the number of votes in favor falls below a system-defined threshold (10 million votes), the proposal is considered defeated;
4. **[agree]:** After the voting ends and if the proposal is not defeated, it awaits setting an execution time by the administrative group. If the execution time is not set at this point, the proposal is in an 'agreed, pending execution time' state;

5. **[queued]**: If the proposal is approved and an execution time is set, it is in a "queued state";
6. **[executable]**: When the proposal meets the execution time interval requirements, the on-chain module automatically captures the corresponding proposal information and executes the proposal's effects in the executable state;
7. **[executed]**: Once the proposal has been executed, it transitions to the executed state.

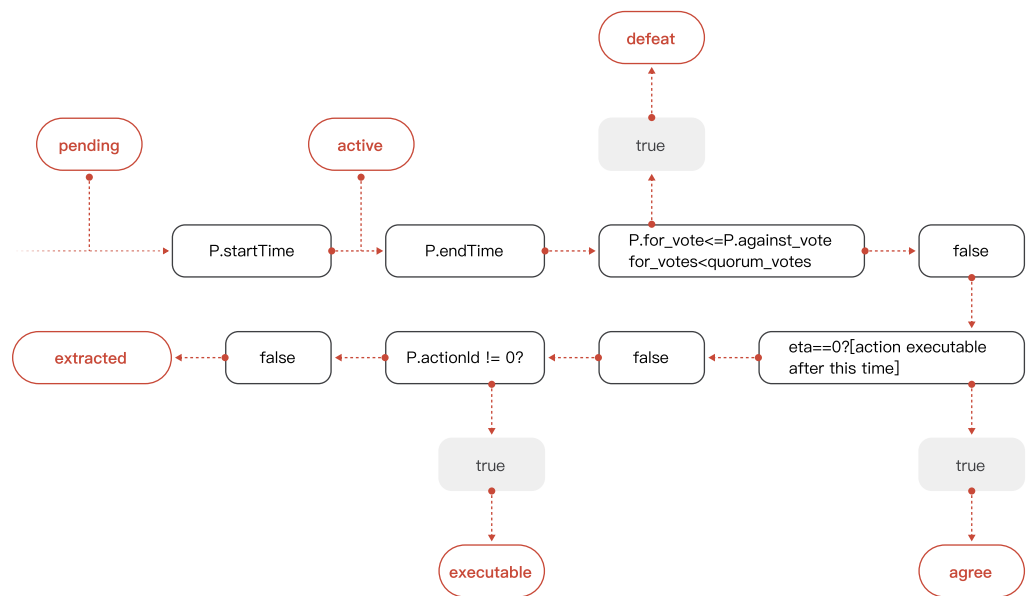


Figure 11: Operational Overview and Proposal Status Flowchart

11.3 DAO System Design Description

We have designed a DAO (Decentralized Autonomous Organization) system based on Move language. It extensively utilizes language specifications like formal verification, preconditions, postconditions, and invariants to fundamentally enhance the security and reliability of the library.

To lower the barrier to user participation, we have implemented highly inclusive measures. Any user can participate in voting by simply staking tokens in the voting pool, and their voting power is directly proportional to the number of tokens staked. In terms of security, we have established higher-level operations that require administrative group permissions, and the administrative group itself needs to meet specific conditions for expansion.

We place significant emphasis on the system's flexibility, allowing it to adapt to various needs and scenarios through configurable DAO parameters and thresholds. Furthermore, deploying DAO modules at the DApp layer enables ordinary users to take full advantage of the DAO system, enhancing its democratic nature and participation.

This comprehensive design provides users with broader participation and decision-making authority, contributing to a more open, democratic, and inclusive governance system. Meanwhile, formal verification and security measures ensure the system's reliability and the safety of user assets, providing the community with a stable and trustworthy governance environment.

12. Roadmap

12.1 Layered Network

Currently, addressing Blockchain scalability issues primarily involves two approaches: Layer 1 and Layer 2 solutions. Layer 1 scalability is constrained by the "trilemma", making it challenging to strike a balance between security and scalability. While BenFen has already achieved significant performance improvements at Layer 1, such as faster transaction confirmations, in some scenarios, faster confirmation times and better scalability are required. Therefore, in BenFen's design, Layer 1 primarily focuses on security, while Layer 2 is responsible for scalability. They work together organically to address blockchain scalability challenges. This layered approach has become a consensus in the public chain space, as seen in Ethereum's adoption of the Rollup development path. The primary functions of Layer 1 and Layer 2 are as follows:

- **Layer 1's Main Functions:**

1. Enhance consensus mechanisms (such as dPoS, DAG, and other technologies) to increase Layer 1's capacity while ensuring security. This aims to maximize the network's utilization.
2. Provide asset definition, issuance, and circulation on Layer 1, as well as facilitate asset transfers between Layer 1 and Layer 2.
3. Offer arbitration mechanisms for Layer 2 to ensure its security, utilizing the security mechanisms of Layer 1 to support Layer 2.

- **Layer 2's Main Functions:**

1. Offload Layer 1 transactions to Layer 2, relieving Layer 1 from the need to concern itself with the details or state changes of Layer 2 transactions.
2. Provide a monitoring mechanism that enables different roles within Layer 2 to supervise each other.
3. Offer evidence preservation functionality, allowing users to arbitrate to Layer 1 for resolution in case of disputes arising from Layer 2 transactions.

12.2 BenFen Layer-2 Solution Overview

12.2.1 State Channels

General State Channels include payment channels, although the state within payment channels is confined to assets. The concept of general state channels aims to expand the notion of states applicable to any application. The core idea of state channels is to migrate state changes between two parties from on-chain to off-chain through mutual supervision. Settlement on-chain occurs when the channel is closed (or it can be optimized for periodic settlement). This effectively consolidates state changes from multiple transactions into one, reducing transaction costs and enhancing overall transaction throughput. State changes within the channel come at an extremely low cost, making it suitable for high-frequency trading or interactive internet applications such as gaming.

Although State Channels can theoretically involve multiple parties, each state change requires unanimous confirmation from all participants. This makes it challenging to scale beyond two participants, limiting its application scope.

12.2.2 Rollups

Rollup is a popular Layer 2 solution that directly submits Layer 2 data to the Layer 1 Blockchain. Layer 1 blocks only record Layer 2 transaction data but do not execute it. Users can access the data on Layer 1 when needed and construct proofs to ensure asset security, especially when challenging the operator is required. Although Rollup is also subject to Layer 1 capacity limitations (as its transactions consume Layer 1 blockchain capacity), it significantly improves performance and scalability, making it a more practical solution. This approach is commonly referred to as "Optimistic Rollup."

Another solution introduces Zero-Knowledge Proofs, which are similar to Optimistic Rollup. However, the inclusion of Zero-Knowledge Proofs reduces withdrawal wait times and theoretically offers shorter processing times. This is because, instead of a challenge period, a ZK-Rollup submits a "validity proof" that Layer 1 simply needs to verify. This approach is typically known as "ZK Rollup."

Specific details regarding BenFen's Layer 2 design will be elaborated in the forthcoming BenFen Layer 2 Design Whitepaper. Here, we've outlined considerations for Layer 2 within the Layer 1 design.

13. Prospects

BenFen, as a next-generation public chain for real-world payment, aims to effectively address the challenges currently faced by blockchain technology and applications, enhancing its usability and promoting widespread adoption. Through improving consensus mechanisms, smart contract programming languages, Stablecoin economic models, and community governance, BenFen enhances security and performance, making it better suited for current DeFi applications. These enhancements also lay the foundation for future architecture to meet the demands of high-performance, low-latency DeFi operations. Through on-chain governance mechanisms, BenFen ensures the continuous evolution of the network and its ecosystem-building capabilities.

Compared to traditional public chains, BenFen exhibits superior performance and security. Furthermore, its native Stablecoin is a robust complement to fiat currencies and existing cryptocurrencies, offering users a novel choice for transactions and value storage. Additionally, by establishing a native Decentralized Exchange (DEX), BenFen lowers user barriers, enhances user experience, and further strengthens the capabilities of its Decentralized Financial platform.

We are committed to putting user value creation at the core of our mission. Through persistent research, innovation, and iterative improvements, we are dedicated to shaping BenFen into a Decentralized Financial platform that excels in security, performance, scalability, and adoption. Our unwavering focus is on delivering greater opportunities and value for users, developers, and merchants.

14. Reference

1. Y. Zohar. (2020). Move Prover. Retrieved from <https://www-cs.stanford.edu/~yoniz/cav20.pdf>
2. Wikipedia contributors. (n.d.). Decentralized autonomous organization. In Wikipedia. Retrieved from https://en.wikipedia.org/wiki/Decentralized_autonomous_organization. Note: APA suggests providing a retrieval date for sources that may change over time, like Wikipedia.
3. Mysten Labs. (n.d.). Why we created Sui Move. Medium. Retrieved from <https://medium.com/mysten-labs/why-we-created-sui-move-6a234656c36b>. Note: Author(s) and publication date are missing; “Mysten Labs” is assumed to be the author; “n.d.” denotes “no date.”
4. Move Language Team. (n.d.). Move Spec. Retrieved from <https://github.com/move-language/move/blob/main/language/move-prover/doc/user/spec-lang.md>. Note: The specific authors of the GitHub document are not listed, and publication date is not provided.
5. Singh, S. F., Michalopoulos, P., & Veneris, A. (2023). DEEPER: Enhancing Liquidity in Concentrated Liquidity AMM DEX via Sharing. In Proceedings of the 2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) (pp. 1–5). Dubai, United Arab Emirates. <https://www.eecg.utoronto.ca/~veneris/23cryptox.pdf>
6. Blackshear, S., Cheng, E., Dill, D. L., Gao, V., Maurer, B., Nowacki, T., Pott, A., Qadeer, S., Rain, D., Russi, S., Sezer, S., Zakian, T., & Zhou, R. (2019). Move: A Language With Programmable Resources. Retrieved from <https://developers.libra.org/docs/move-paper>.
7. (2022). DAG meets BFT. Retrieved from <https://decentralizedthoughts.github.io/2022-06-28-DAG-meets-BFT/>.
8. Danezis, G., Kokoris-Kogias, E., Sonnino, A., & Spiegelman, A. (2021). Narwhal and Tusk: A DAG-based Mempool and Efficient BFT Consensus. CoRR, abs/2105.11827. Retrieved from <https://arxiv.org/abs/2105.11827>
9. Guerraoui, R., Kuznetsov, P., Monti, M., Pavlovic, M., & Serebinschi, D.-A. (2018). AT2: Asynchronous Trustworthy Transfers. CoRR, abs/1812.10844. Retrieved from <https://arxiv.org/abs/1812.10844>

10. Spiegelman, A., Giridharan, N., Sonnino, A., & Kokoris–Kogias, L. (2022). Bullshark: Dag bft protocols made practical (full paper). arXiv preprint arXiv:2201.05677. Retrieved from <https://arxiv.org/abs/2201.05677>
11. Dill, D. L., Grieskamp, W., Park, J., Qadeer, S., Xu, M., & Zhong, J. E. (2021). Fast and Reliable Formal Verification of Smart Contracts with the Move Prover. CoRR, abs/2110.08362. Retrieved from <https://arxiv.org/abs/2110.08362>
12. Optimism Community. (n.d.). Rollup Protocol. Retrieved from <https://community.optimism.io/docs/protocol/2-rollup-protocol/#moving-from-op-mainnet-to-ethereum>. Note: Author(s) and publication date are missing; “Optimism Community” is assumed to be the author; “n.d.” denotes “no date.”
13. Liu, Y., & Tsyvinski, A. (2018). Risks and Returns of Cryptocurrency. August 2018. *Note: The exact format of a working paper citation can vary. If this is an article, include the journal title, volume.