User-Friendly Privacy-Preserving Protocol for Compliant Cryptocurrency Transactions

Authors: Michal “Mehow” Pospieszalski, Billy Mullins

Company: SwissFortress AG, Baar, Switzerland

Website: www.swissfortress.com

Version 1.4

November 26, 2024

Abstract

We outline a user-friendly and privacy-preserving protocol, (“SwissFortress Protocol”) powered by FortressCoin, designed to enhance both confidentiality and usability in cryptocurrency transactions while maintaining KYC/AML compliance. FortressCoin incentivizes and supports a decentralized privacy infrastructure, enabling users to engage in secure transactions while maintaining control over transaction visibility.

1. Introduction

While blockchain transparency is beneficial for security, it can also expose transactional data to public scrutiny, putting user privacy at risk. The SwissFortress Protocol addresses this issue by implementing a send-to-name mechanism, allowing users to transact through unique, human-readable identifiers, and a privacy-preserving signaling structure that keeps transaction metadata secure. This approach ensures that while transaction details remain visible on the public blockchain, the privacy-preserving signaling structure prevents the mapping of human-readable identifiers to dynamically generated addresses, ensuring that only the transacting parties can link the transactions to their identities.

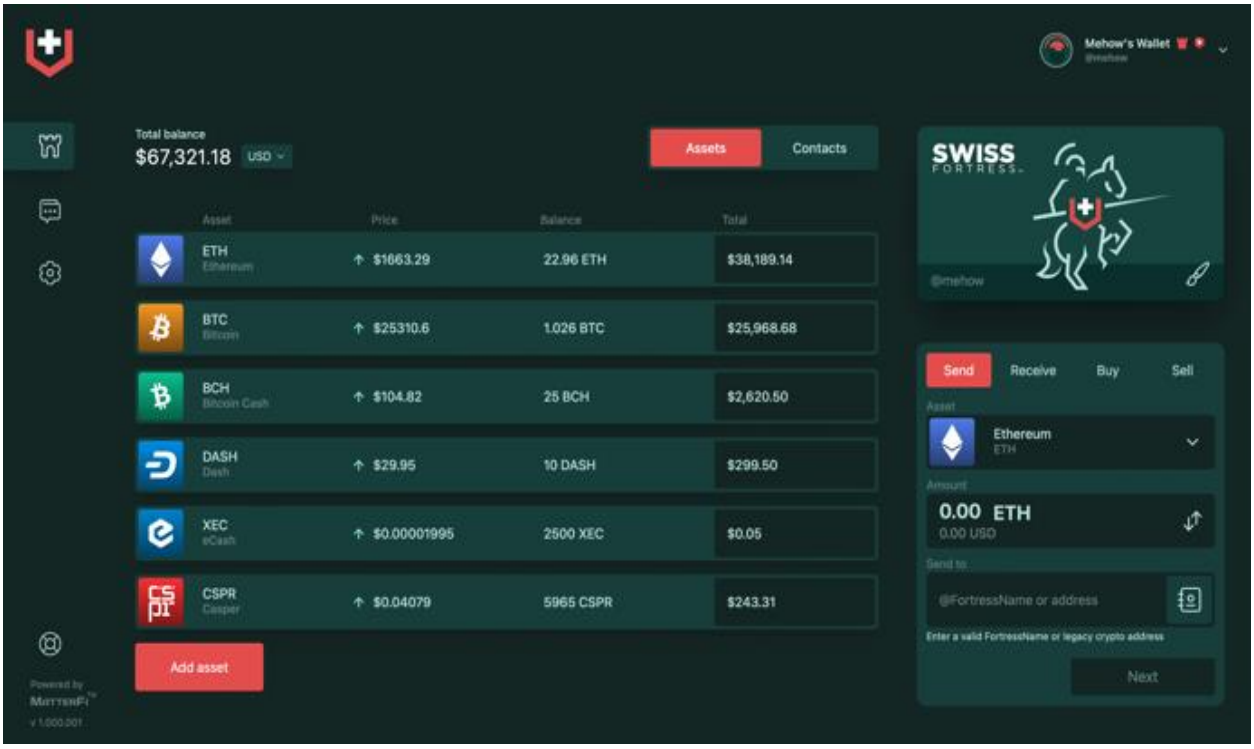
2. Utility of FortressCoin

FortressCoin serves as the utility token within the SwissFortress Protocol (SFP), enabling users to:

- **Reserve Unique Names**: Secure a unique, globally recognized name to facilitate private, send-to-name transactions.
- **Access Privacy-Preserving Infrastructure**: Incentivize participants who operate nodes for off-chain signaling and data storage.
- **Credentialed Access**: Enable FortressCoin holders to undergo optional KYC/AML checks and share verified credentials securely, irrefutably proving their off-chain identity.
- **Governance**: Allow FortressCoin holders to influence protocol updates and privacy standards.

Although users can manipulate FortressCoin directly, SwissFortress performs the above functions automatically for users that purchase names. For the users the FortressCoin infrastructure enables Paypal-like decentralized “send to name” without the user having to understand the protocol.

SwissFortress Wallet



3. Overview of the Send-to-Name and Signaling Protocol (SFP)

The SF protocol facilitates transactions using globally unique names without exposing transaction data publicly. Components include:

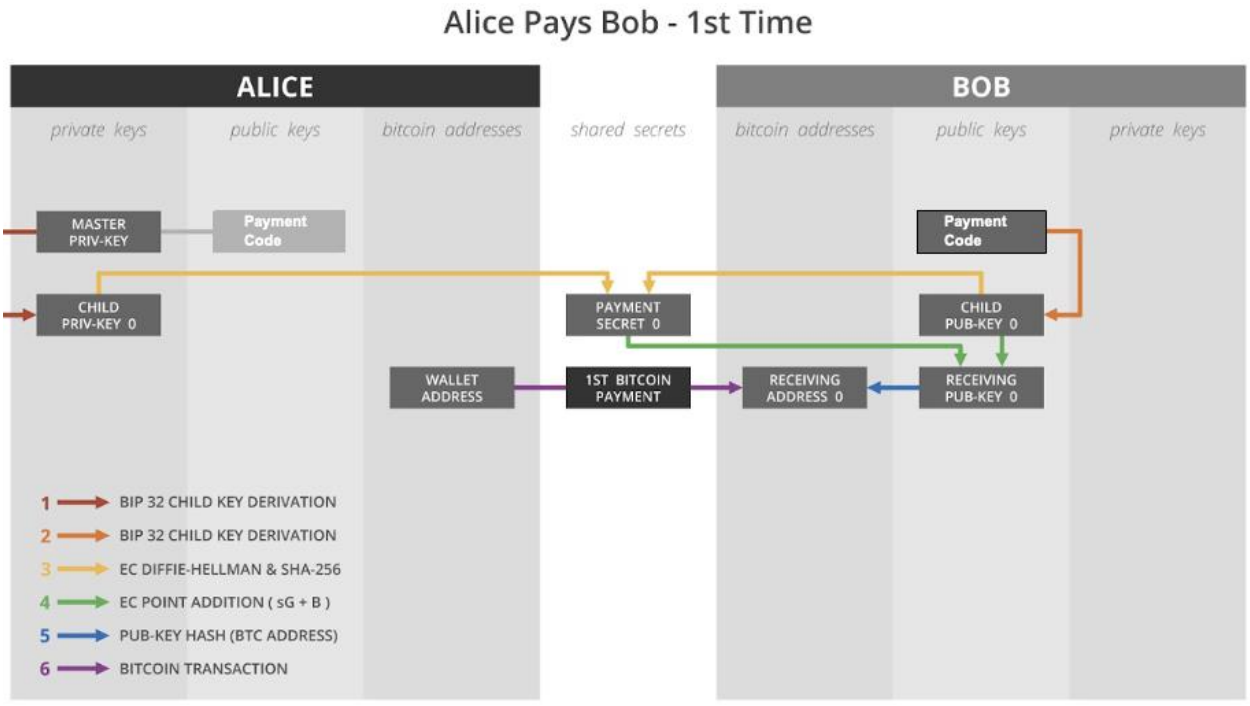
- **Human-Readable Identifiers**: Unique names allow user-friendly transaction identification across platforms.
- **Public Paycodes and Key Infrastructure**: To establish secure, verifiable transactions.
- **Multimodal Signaling Pathways**: Combined on-chain and off-chain pathways for redundant, private, and efficient signaling.

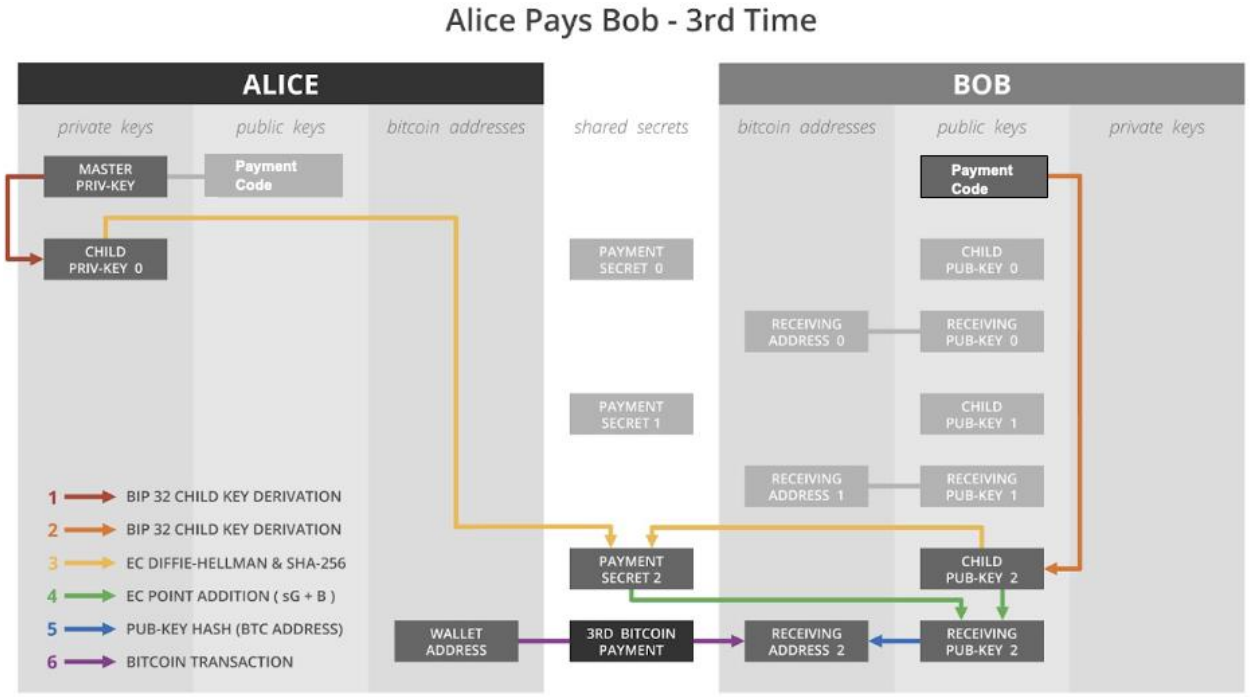
3.1. Protocol Overview and Computation of Public Paycodes

SFP enables wallet users to compute a counterparty's receive address on any blockchain and token via a one-way cryptographic proof. An important concept to understand is that whenever a master private and public key pair is created, it defines a curve with a large key space rather than a single key. SFP allows a user, **Alice**, to deterministically compute a receive address that is guaranteed to be on **Bob's curve** (compatible with both secp256k1 and Ed25519 curves). This computed address can only be generated by Alice for transactions to Bob, thereby forming a cryptographic proof that Alice has sent funds to Bob. Additionally, a **Zero-Knowledge (ZK) proof** ensures that the funds Alice sends to Bob originate from her private key, which is the same key used to compute the Alice-Bob receive address.

In this way, any two parties in the SFP system, such as Alice and Bob, compute unique addresses for each transaction, enhancing privacy. For example:

- When Alice sends to Bob, the **Alice-Bob key** is computed.
- When Bob sends to Alice, a distinct **Bob-Alice key** is generated.
- If a third party, Charlie, sends to Bob, a separate **Charlie-Bob key** is computed, ensuring all computed addresses are unique to each sender-receiver pair.





The **Public Paycode** is a hardened xpub used exclusively within the SFP. This hardened xpub acts as a shared identity key that Alice and Bob use to calculate unique addresses for every transaction. If used as a regular xpub, these addresses would be meaningless, as they are designed specifically for privacy within SFP. The SFP Public Paycode helps achieve **maximum privacy on existing**

blockchains without requiring any modifications to the blockchain itself. By design, **third-party observers** can access users' names and paycodes but cannot compute their receive addresses on-chain.

The **name lookup and discovery** feature is critical for the protocol, allowing both on-chain and off-chain mappings of **human-readable identifiers** to Public Paycodes. Through this feature, Alice can quickly find Bob's paycode, and vice versa, enabling the computation of unique addresses through a one-way, non-interactive cryptographic proof. This way, Alice and Bob's identities are represented as paycodes without direct on-chain linkage, preserving privacy while ensuring verifiable KYC-compatible interactions.

A fundamental component of SFP is its **signaling system**, which supports encrypted name lookup for Public Paycodes. For Bob to compute all possible addresses on which Alice may send him funds, only a single **signal** is required. This signal, encrypted with Bob's public key, allows him to recognize Alice's intent to send funds while ensuring privacy. Without this signaling, Bob would need to compute his unique addresses for all possible users, which, while possible, is computationally inefficient.

Key Features of the SFP

1. **Human-Readable Identifiers and Public Paycodes**: The protocol supports both on-chain and off-chain mappings, allowing discovery of paycodes through name lookup and computation of unique addresses for secure transactions.
2. **Privacy-Preserving Transactions**: With each transaction generating a unique address, the system prevents third-party observers from tracing transaction histories or computing receive addresses based on publicly accessible information.
3. **Backward Compatibility with OBPP-5**: While building on OBPP-5, SFP is backward-compatible, enabling legacy BIP-47/OBPP-5 wallets to send funds to an SFP enabled wallet. However, the reverse requires an explicit send option for compatibility.

3.2. System Implementation Approaches

The SwissFortress Protocol supports two complementary approaches for implementation, enabling both user flexibility and scalability across various ecosystems:

Partner-Based Ecosystem Approach

The partner-based approach simplifies the adoption of the SwissFortress Protocol by leveraging trusted service providers who act as intermediaries. These partners manage key operations such as token locking, name reservations, and privacy-preserving signaling on behalf of users. In this model:

- **Ease of Use**: Users are not required to hold FortressCoin directly, as service providers handle all protocol-related interactions.
- **Expanded Accessibility**: This approach lowers barriers for non-technical users, ensuring widespread adoption across diverse user bases.

- **Ecosystem Stability**: Service providers align with the governance framework to adjust parameters like token locking dynamically, ensuring ecosystem sustainability.
- **Support for the Lighthouse Effect**: Partners act as beacons within the ecosystem, drawing in new users by demonstrating the protocol's benefits and capabilities.

This approach combines user-friendly accessibility with centralized operations to maximize reach and usability.

Distributed User-Driven Model

The distributed user-driven model empowers users to directly interact with the protocol in a decentralized manner. In this approach:

- **Full Decentralization**: Users may hold FortressCoin directly to perform name reservations and engage in signaling.
- **Enhanced Privacy and Autonomy**: Without intermediaries, users retain full control over their transactions and operations.
- **Community Ownership**: This model encourages a sense of collective responsibility, fostering deeper engagement within the ecosystem.

While this approach offers greater control and privacy, it is better suited for tech-savvy users who can manage the operational complexity. As stated previously, SwissFortress will be performing the above operations for retail users via the SwissFortress and partner wallets.

Balancing the Two Approaches

These dual frameworks provide the flexibility needed to adapt the protocol to different user needs and market conditions. Together, they ensure that the SwissFortress Protocol can cater to both casual users and advanced participants, driving long-term adoption and sustainability.

4. Multimodal Signaling for Paycode Transmission

As detailed in Section 3, computational efficiency requires a reliable signaling system. SFP achieves this through multimodal signaling, a robust approach that employs multiple, distinct pathways for transmitting transaction signals. This method enhances privacy, reliability, and redundancy. By dispersing transaction signals across both on-chain and off-chain pathways, the protocol ensures each transaction remains private, resilient to potential failures, and recoverable when necessary.

4.1. What is Multimodal Signaling?

Multimodal signaling refers to the use of various transmission methods to optimize privacy and reliability for transaction signals. The pathways include:

- **Primary Off-Chain Pathways**: Decentralized storage networks and private messaging servers serve as channels for transmitting signals. By keeping transaction signals off-chain, data remains hidden from public view, preventing third-party tracking based on signal volume. Notably, decrypting these signals is impossible for unauthorized parties.
- **Primary On-Chain Pathways on the Fortress Chain**: In parallel, signals can also be sent directly on the FortressCoin chain as encrypted metadata within minimal-value transactions. This pathway provides a decentralized, secure storage of signals.
- **In-Line Backup Signaling**: If the primary on-chain pathway is unavailable, a signal will be sent with the funds on the chain. In normal operations, however, inline signaling will usually contain only noise, with the true signal sent separately. This backup measure ensures signal continuity.
- **Noise Protocol**: To prevent external observers from inferring transaction activity based on signaling volume, the protocol incorporates random “noise” signals. These decoy signals obscure actual transaction signals, making them difficult to isolate or analyze.
- **Beacon Addressing**: Signals are sent to non-deterministic addresses representing a pool of users, ensuring that signal volume cannot be attributed to any single user.

A key distinction between OBPP-5 and the SFP’s signaling approach is that OBPP-5 always embeds signals with the funds as part of the same transaction as change. In contrast, SFP sends signals through a separate signaling chain (the primary on-chain pathway, FortressCoin), allowing each signal to represent any transaction across any chain or token now or in the future. This approach significantly reduces the ability to correlate signals on conventional blockchains. Additional distinctions in the patent pending SF protocol include the use of beacon addressing, noise protocol, in-line backup signaling, and off-chain signaling, among other enhancements.

4.2. Key Benefits of Multimodal Signaling

- **Enhanced Privacy**: By dispersing transaction signals across both on-chain and off-chain pathways, multimodal signaling ensures that only intended parties can identify and process signals, obscuring transaction volumes from third-party analysis.
- **Redundancy and Reliability**: With multiple transmission pathways, the signal can still be recovered from an alternate pathway if one fails, ensuring transaction signals reach their destination under various conditions.
- **Transaction History Recovery**: Multimodal signaling allows for efficient recovery of transaction histories from stored paycode signals, even if data from one pathway is inaccessible. When a user restores a wallet from seed, all their transactions both incoming and outgoing will be recovered along with the counterparty name data.

4.3. Example in Practice

When a user initiates a send-to-name transaction, their wallet defaults to using both the primary off-chain pathway and on-chain pathway simultaneously to securely and privately signal the recipient’s wallet. If the on-chain pathway is temporarily unavailable, the wallet automatically switches to inline signaling. To further safeguard privacy, the wallet consistently uses the Noise Protocol to add random

decoy signals, masking transaction activity. This layered approach ensures that transaction signals remain private, resilient, and easily recoverable.

4.4. What It's Not

This is not a mixer. Chain analysis functions normally with this system. It simply provides users with an efficient method to generate and use unique on-chain addresses for each other.

5. Use Cases for SFP and the Send-to-Name Protocol

5.1. Cross-Border Payments

The protocol allows individuals and businesses to make international transactions with privacy through send-to-name functionality, using secure, low-cost signaling pathways without revealing transaction metadata.

5.2 .Decentralized Finance (DeFi) Integration

DeFi applications can use SFP to enable private wallet-to-wallet and wallet-to-smart contract interactions, expanding access to lending, borrowing, and staking while preserving anonymity. For example, DeFi using SFP can distinguish between users and also utilize our end-to-end KYC proof system for a novel approach to compliance.

5.3. Privacy-Enhanced Wallet Services

Wallets using SFP allow private transaction histories to be stored securely, with transactions recoverable only by the user. This setup enables wallets to offer private data restoration and selective transaction visibility.

5.4. Name Reservations for Unique Identifiers

The protocol's send-to-name feature enables users to reserve unique names, much like domain names, for transaction identification. FortressCoin is used to reserve and lock these names, adding practical utility and contributing to supply reduction.

6. Economic Model and Utility

FortressCoin powers key functions within the SwissFortress Protocol, driving utility through organic demand in the form of signaling and name reservations. Unlike traditional models that use burns or buybacks to influence price, FortressCoin emphasizes genuine utility-based locking and usage, creating a sustainable ecosystem.

6.1. Utility for Name Reservation and Signaling

FortressCoin is designed to support two primary functions: name reservations and signaling. Both mechanisms create organic demand by locking FortressCoin for use within the ecosystem, thereby reducing circulating supply naturally:

- **Name Reservations and KYC**: Users can lock FortressCoin to reserve unique, globally recognizable names and KYC (see Section 7) on the FortressCoin chain. These remain locked as long as the reservation is active, creating a steady reduction in circulating supply.
- **Signaling Usage**: FortressCoin facilitates signaling between wallets, creating demand based on genuine network activity and usage. This demand is intrinsic to the protocol's functionality, as signaling enables privacy-preserving, user-friendly transactions.

6.2. Why We Don't Prioritize Burning or Buybacks

6.2.1. Burning

Burning has become a common practice in the cryptocurrency space, but it does not necessarily lead to meaningful price appreciation for several reasons:

- **Impact on Circulating Supply**: Burn events often reduce supply that are outside the circulating supply, like reserve tokens. This type of burning creates only the appearance of scarcity rather than an actual increase in demand for circulating supply.
- **Lack of Long-Term Price Support**: While burning can create a temporary price boost, it does not inherently drive long-term demand. Without a sustained increase in actual use cases, burning fails to address the root of price growth, which is organic demand from usage.

6.2.2. Buybacks

Using funds from name sales or protocol earnings to buy back tokens is another tactic some projects employ, but we see drawbacks with this approach:

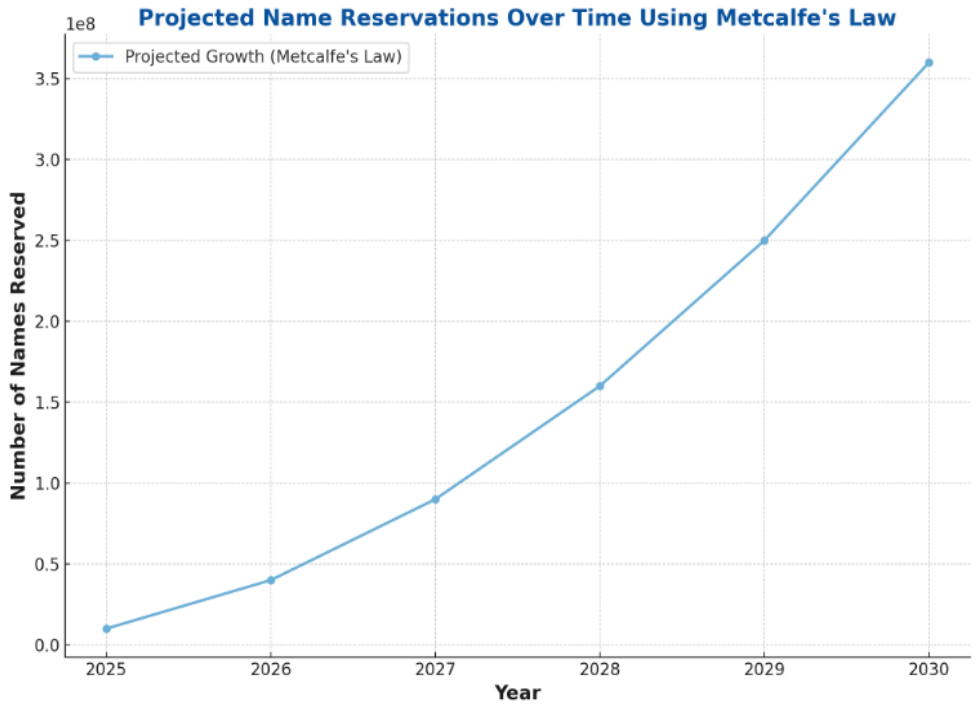
- **Artificial Market Support**: Buybacks create a temporary demand that can be perceived as market manipulation. This artificial demand does not reflect real usage or ecosystem growth and may ultimately undermine investor trust.
- **Short-Term Impact**: Buybacks may create only short-lived price increases, which often reverse when buyback activity ends. Sustainable price growth comes from ongoing demand within the ecosystem, not one-time or repeated buybacks.
- **Missed Opportunity**: Funds used for buybacks could be more effectively allocated to development, marketing, and partnerships that foster genuine demand and protocol growth, directly benefiting the ecosystem.

6.3. Why Locking and Utilization are Superior

We believe that locking FortressCoin for name reservations and using them in signaling is a superior model for creating long-term value and price support:

- **Real Utility from Name Reservations**: Name reservations require FortressCoin to be locked as long as the reservation is active. This creates an enduring reduction in circulating supply tied to an actual feature that users value.
- **Signaling-Driven Demand**: Utilization of FortressCoin through signaling is genuine usage that directly correlates with the protocol's core functionality. This demand isn't artificial but is generated by user activity within the network, leading to an organic increase in value.

By focusing on demand-driven mechanisms and avoiding artificial price supports like burning or buybacks, FortressCoin fosters sustainable tokenomics that reflect real use and user participation within the SwissFortress Protocol.

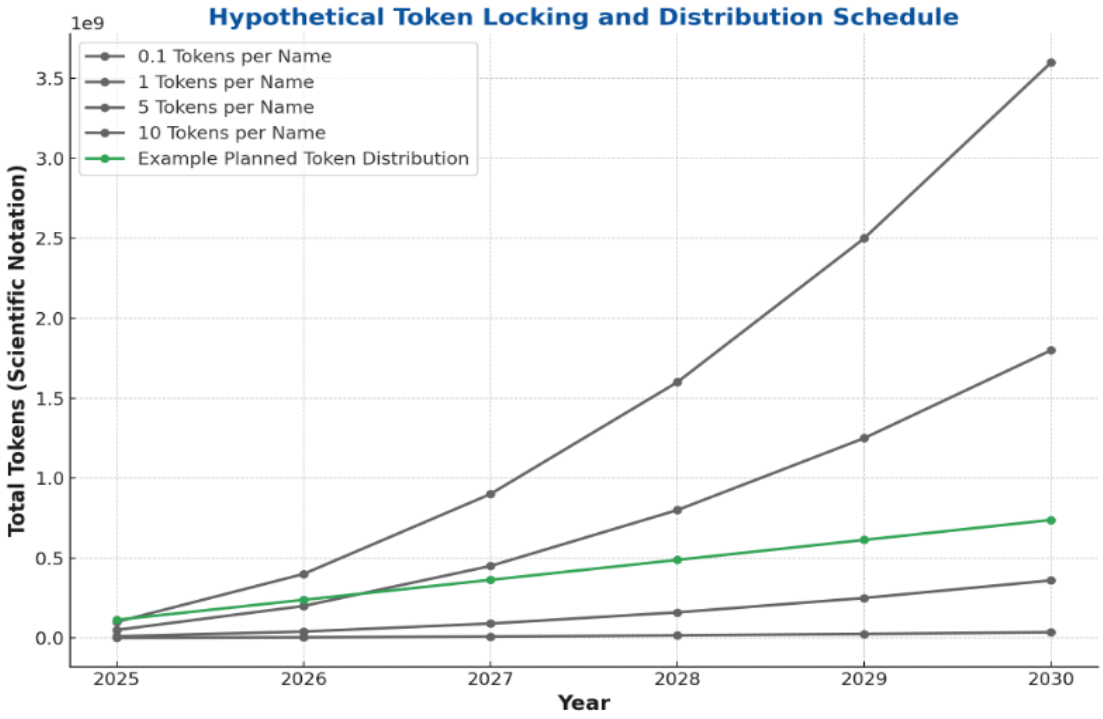


Projected Name Reservations Over Time Using Metcalfe's Law

This chart illustrates the anticipated growth in name reservations within the SwissFortress Protocol ecosystem, modeled using Metcalfe's Law. The exponential increase reflects the strengthening network effects as more users adopt the privacy-preserving send-to-name functionality. This growth trajectory aligns with the protocol's goal of creating a secure, user-friendly framework. These numbers reflect numbers of wallet owners with a name that represents a destination address that supports cross chain sends. The scale of growth should be expected to scale as the number of users in the global cryptocurrency ecosystem scales and adopt send to name functionality.

Hypothetical Token Locking and Distribution Schedule

This chart explores hypothetical scenarios for token locking based on varying tokens-per-name assumptions, contrasted against a token distribution curve. It showcases how token locking supports name reservations and signaling activities, demonstrating a dynamic balance between adoption-driven locking and systematic token distribution. This approach highlights the protocol's focus on sustainable growth and utility-driven demand.



6.4. Governance Framework

The SwissFortress Protocol will incorporate a governance framework to stabilize FortressCoin's price and supply, ensuring a functional and sustainable ecosystem. Key features of the governance framework include:

1. **Dynamic Adjustments**:
    - The framework enables ecosystem partners to modify protocol variables such as the number of tokens locked per name. These adjustments respond to market conditions, aligning supply and demand with real-world needs.
2. **Ecosystem Partner Contributions**:

    - Service providers will play a central role in governance, acting as stewards of the protocol. They align their operations with governance decisions to maintain stability and support the protocol's objectives.
3. **Support for Diverse Models**:
    - The governance framework will accommodate both the partner-based and user-driven models, allowing seamless integration of centralized and decentralized approaches.
4. **Long-Term Sustainability**:
    - By dynamically managing tokenomics, the governance framework will ensure that FortressCoin remains viable as a utility token, supporting the protocol's growth while maintaining stability.

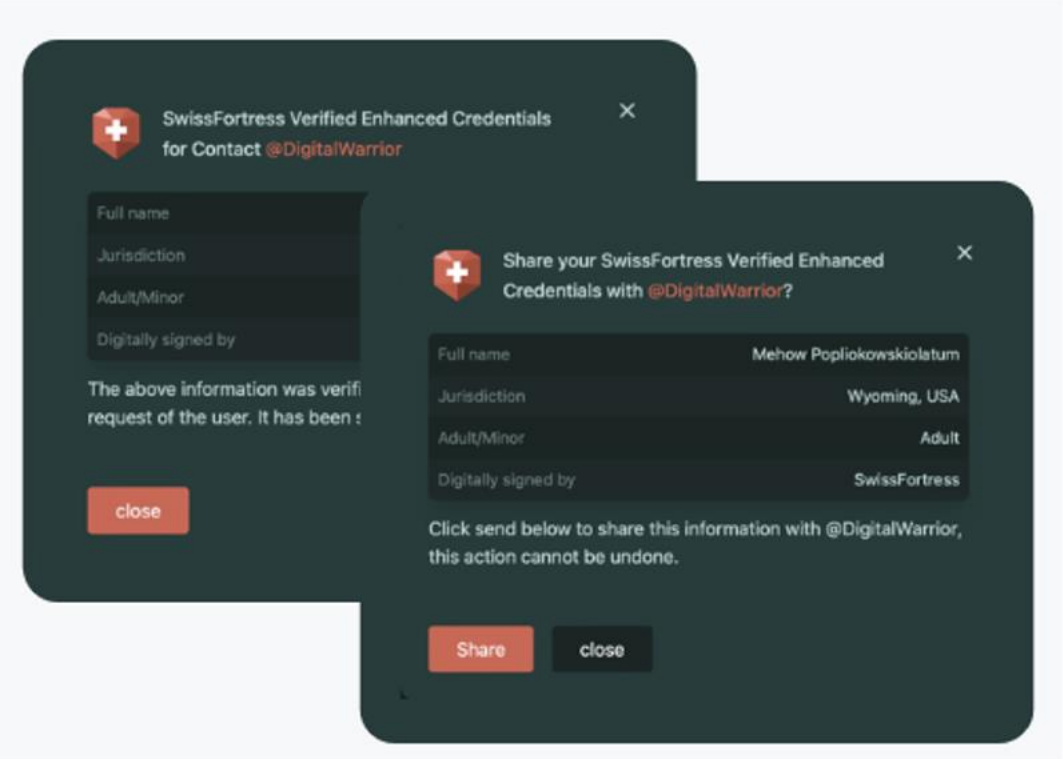
7. KYC/AML Compliance and Identity Verification

Ensuring compliance with Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations is crucial for the adoption and legitimacy of cryptocurrency protocols. The SwissFortress Protocol integrates robust identity verification mechanisms to meet these regulatory requirements while preserving user privacy.

7.1. Credentialed Access with FortressCoin

Users can lock FortressCoin to create a decentralized, cryptographic proof of identity. They may choose to undergo identity verification processes, obtaining credentials that attest to either blinded or unblinded claims or a combination of both about themselves.

For example, if Alice wishes to prove to a counterparty that she is over 18 and a resident of the USA, she could create an "Adult American" proof. Alice does not want to reveal her name as part of this proof, so the proof is a blinded claim. To create it, Alice would submit her driver's license to a KYC authority. The authority would then issue a cryptographic proof, signed by them, which Alice can use. She can share this proof with other parties who are likely to trust it if they recognize the authority as reputable.



Alice can create as many cryptographic proofs as she likes, with no technical limit. These proofs can be blinded, unblinded, or combinations of both. For instance, in addition to the "Adult American" proof, Alice could have a proof revealing a copy of her passport or a separate proof for her driver's license, and so forth.

This credentialed access allows users to participate in transactions with DeFi, CeFi/custody providers, and on-chain counterparties requiring KYC/AML compliance without disclosing their identity publicly. The protocol ensures that only entities authorized by Alice can access her proof, maintaining the confidentiality of user information.

No central storage of KYC information is necessary for this system to function. Additionally, even if a third-party observer were to obtain identity proofs related to a specific name, they could not compute the addresses used by the user based on this information alone.

In summary, users can complete a KYC process and obtain decentralized, blinded, and/or unblinded credentials to share with counterparties. This allows them to prove, for example, that they are "over 18 and a resident of Wyoming," or to provide a "full copy of their passport," among other proofs.

7.2. Privacy-Preserving Compliance

By combining “Send-to-Name” with credentialed access, the SwissFortress Protocol achieves a balance between regulatory compliance and user privacy. Users can prove their compliance status

through their credentials without exposing personal information on the blockchain. This approach aligns with global regulatory standards while upholding the core principles of privacy and decentralization.

7.3. Benefits of the Integrated Approach

- **Regulatory Alignment**: Can allow users to meet international KYC/AML and travel rule requirements, facilitating broader adoption and integration with traditional financial systems.
- **User Privacy**: Maintains user anonymity through nyms, ensuring that personal information is not publicly disclosed.
- **Flexibility**: Allows users to choose between pseudonymous and credentialed transactions based on their needs and regulatory obligations.
- **Security and Phishing Elimination**: Utilizes cryptographic methods to secure identity verification processes, preventing unauthorized access and identity theft. SFP can eliminate most forms of modern phishing attacks which rely on a user allowing an attacker's address to take control of assets or sending assets to an attacker's address directly. SFP doesn't require a user to manipulate addresses at all. They can simply check a counterparties name and KYC proofs before any transaction which is significantly easier than verifying addresses.

By incorporating these mechanisms, the SwissFortress Protocol provides a compliant yet privacy-focused solution for cryptocurrency transactions, addressing the challenges of regulatory adherence in the digital asset space.

8. Technical Specifications

- **Blockchain Compatibility**: The protocol supports multiple chains (e.g., Ethereum, Bitcoin) to allow for broad accessibility and integration.
- **Public Key Standards**: Backwards compatible with BIP-47/OBPP-5 public paycodes for interoperability and privacy. BIP-47/OBPP-5 wallets which presently no longer exist in the wild can send funds to an SFP enabled wallet but vice versa cannot occur unless a user specifies this type of send in advanced options.

9. Integration with Existing Naming and Credential Systems

SFP signaling is compatible with some integration with existing blockchain naming services (e.g., ENS) and decentralized identity frameworks. The protocol ensures that FortressCoin backed transactions are user-friendly, leveraging global name identifiers across systems to enable streamlined transactions and network-wide usability.

10. Roadmap

Phase 1: Protocol Launch

- Core protocol development, unique name reservation feature, initial partnerships, and onboarding.

Phase 2: Expanded Blockchain Compatibility

- Integration with major DeFi platforms and wallet partnerships to expand FortressCoins use case and user base.

Phase 3: Advanced Privacy and Governance Features

- Deploy enhanced privacy layers, new signaling pathways, and further governance tools to engage the community in protocol evolution.

11. Conclusion

The FortressCoin and the Send-to-Name and Privacy-Preserving Signaling Protocol (SFP) provide a transformative approach to cryptocurrency privacy. By supporting multimodal pathways and unique name reservations, FortressCoin enables a secure, privacy-focused ecosystem where value is derived from actual user-driven demand, aligning the utility with the expectations of a robust, decentralized financial system.

12. Citations

- **U.S. Patent Application No. 63/578,658**: *Decentralized Use of Zero Knowledge Proof with Enhanced Identity Credentials to Lower External Counterparty Risks, for Example to Combat Money Laundering*
- **U.S. Patent Application No. 63/512,052**: *Privacy-Preserving Cryptocurrency Transactions with Enhanced Credentials and User-Friendly PayCode Infrastructure*
- Open-Transactions White Paper, Chris Odom