$afe AF: User-Friendly Privacy-Preserving Protocol for Compliant Cryptocurrency Transactions

Michal “Mehow” Pospieszalski, Justus Ranvier, Emanuele Ragnoli, Vincenzo Botta, Jakub Zurawinski

AmericanFortress, Jackson Hole, Wyoming USA

Multiple patents pending

`https://americanfortress.io`

Version 3.1, 21st May 2026

Abstract

AmericanFortress™ (AF) introduces a user-friendly, privacy-preserving transaction protocol designed to make cryptocurrency payments easier to use while reducing the public exposure of transaction relationships. The AmericanFortress Protocol (AFP) enables users to transact through human-readable identifiers known as FortressNames™ rather than manually exchanging blockchain addresses. Under the protocol, wallets use public paycodes, cryptographic key derivation, and privacy-preserving signaling to generate recipient-specific blockchain addresses that are meaningful to the transacting parties but difficult for third-party observers to link to public identities or transaction histories.

AFP is designed to improve both usability and privacy without requiring changes to the underlying public blockchains on which transactions settle. A sender can look up a recipient's FortressName, retrieve the associated public paycode, and compute a unique destination address for that relationship. The recipient's wallet can recognize the transaction through encrypted signaling, while outside observers see only ordinary blockchain activity. To support reliability and recoverability, AFP uses multimodal signaling across off-chain, on-chain, and backup pathways, with noise and beacon-addressing techniques intended to reduce traffic-analysis risks.

Many privacy systems anonymize the sender from the recipient as well as from the public. AFP preserves recipient awareness, allowing a recipient to know who sent funds while preventing public observers from learning the same relationship. AFP uses zero-knowledge technology to give recipients stronger confidence about the origin of a payment without exposing the sender's broader wallet activity. Privacy protects users from public surveillance while still giving counterparties the information they need to recognize, verify, and manage legitimate transactions, including selective disclosure, counterparty assurance, and credential-based compliance workflows.

In post-quantum-oriented deployments, AFP may also support zero-knowledge lineage and authorization proofs for hierarchical deterministic wallets where compatible proof-verification infrastructure is available. These proofs can allow a wallet to demonstrate control over a BIP32-Ed25519-derived public key and its derivation path without exposing the master seed, private keys, or unrelated wallet state.

AF Token, ticker $AF, provides utility within the AmericanFortress ecosystem by supporting name reservation, signaling infrastructure, credentialed access, paymaster or tolling services, and ecosystem participation. Rather than positioning privacy as a standalone anonymity feature, AF frames it as infrastructure for practical digital-asset payments: easy to use, interoperable across chains and wallets, intelligible to the parties involved, and capable of supporting privacy-preserving compliance where required by users, partners, or regulated counterparties.

AF provides a decentralized Send-to-Name™ experience for cryptocurrency transactions: simple enough for mainstream users, private enough to reduce unnecessary public surveillance, and flexible enough to support wallets, exchanges, custodians, payment processors, DeFi applications, and institutional integrations across multiple blockchain environments.

Contents

1 Introduction

While blockchain transparency is beneficial for security, it can also expose transactional data to public scrutiny, putting user privacy at risk. The AmericanFortress Protocol (AFP) addresses this issue by implementing a "Send-to-Name" mechanism, allowing users to transact through unique, human-readable identifiers called FortressNames, and a privacy-preserving signaling structure that keeps transaction metadata secure. Transaction details remain visible on the public blockchain, but the privacy-preserving signaling structure prevents the mapping of human-readable identifiers to dynamically generated addresses, so only the transacting parties can link the transactions to their identities.

2 Utility of AF Token

AF Token serves as the utility token within the AF Protocol (AFP), enabling users to:

- Reserve Unique FortressNames: 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 AF Token holders to undergo optional KYC/AML checks and share verified credentials securely, supporting verifiable off-chain identity claims.

Although users can hold or interact with AF Token directly, AF performs the above functions automatically for users that purchase names. For end users, AF Token infrastructure supports a consumer-friendly decentralized Send-to-Name experience without requiring users to understand the underlying protocol mechanics.

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

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

- FortressNames as 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.

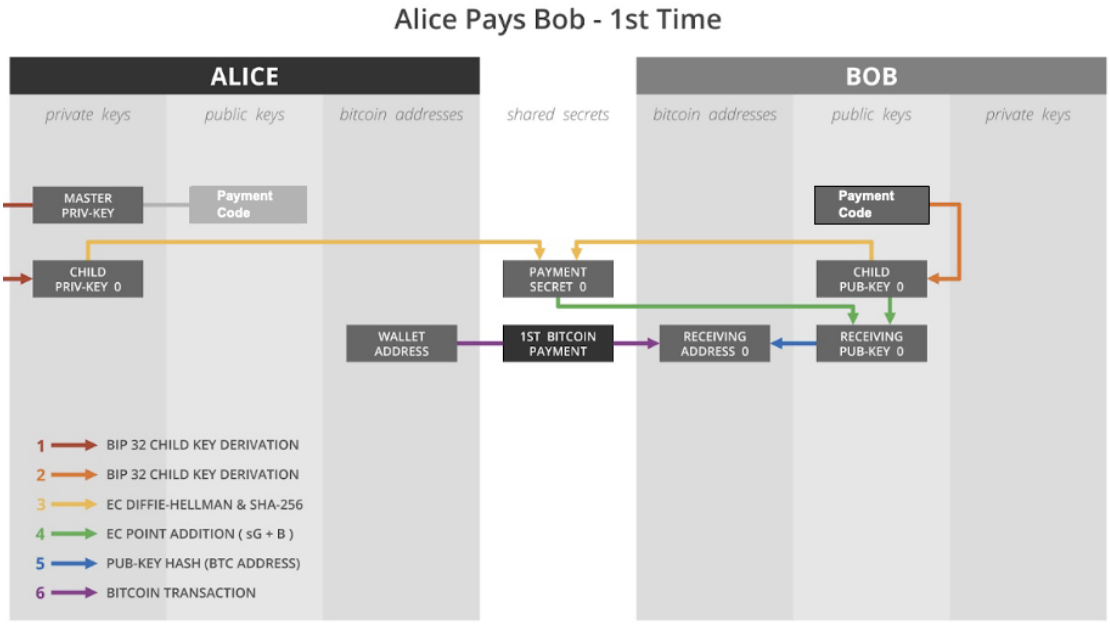
3.1 Protocol Overview and Computation of Public Paycodes

AFP enables a wallet to derive a recipient-specific destination address for supported chains and assets using paycode-based cryptographic key derivation. Whenever a master private and public key pair is created, it defines a curve with a large key space rather than a single key (including secp256k1 and Ed25519 deployments). AFP allows Alice's wallet to derive a destination address controlled by Bob's corresponding wallet key material, without exposing the sender-recipient relationship publicly. For a given sender-recipient pair, the derived address is relationship-specific: Alice's wallet can derive the outbound Alice–Bob destination path for payments to Bob, while Bob's wallet can recognize the corresponding inbound path using Bob-controlled key material

and the AFP signal. A zero-knowledge (ZK) proof can further show that funds sent on that path originated from Alice's key material used in the derivation.

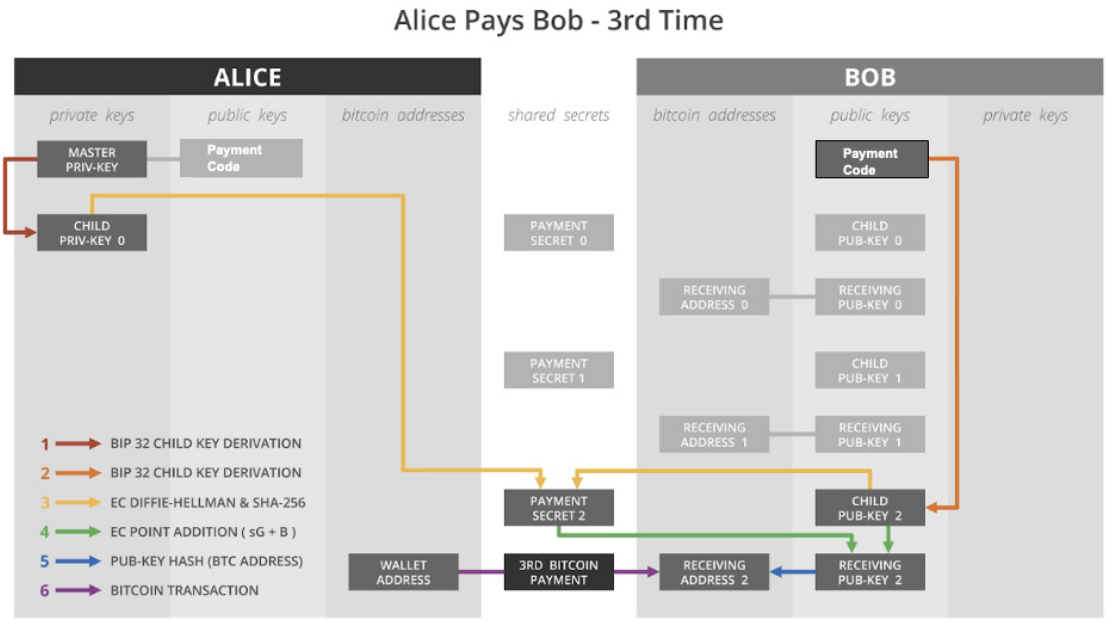
In this way, any two parties in the AFP system, such as Alice and Bob, can derive a shared payment secret unique to their relationship. At a simplified level, if Alice controls a private key a with public key $A = aG$, and Bob's paycode exposes a public derivation key $B = bG$, Alice can compute aB and Bob can compute bA. Because $aB = abG = bA$, both parties arrive at the same relationship-specific shared value without publishing it. AFP hashes this value together with chain, asset, direction, and index data to produce a payment secret for that relationship. The payment secret is then used as input to address derivation, not as the address itself. For Alice-to-Bob payments, the resulting derivation produces a Bob-controlled receiving address. For Bob-to-Alice payments, the corresponding direction-specific derivation produces an Alice-controlled receiving address.

If Charlie sends to Bob, Charlie and Bob derive a separate Charlie-Bob payment secret and address space. This ensures that each sender-recipient relationship has its own destination paths and that public observers cannot compute receive addresses from public names or paycodes alone.



The AFP Public Paycode is a public payment-code object derived from the user's wallet key hierarchy and used exclusively for AFP address derivation and signaling. It functions as a public identity and routing object within AFP, but should not be treated as a conventional xpub for ordinary account discovery or address scanning. AFP uses the paycode to derive relationship-specific destination addresses without exposing those addresses through the public name registry. The AFP Public Paycode is designed to improve 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 the corresponding AFP receive addresses from those public values alone. In normal operations AFP enables the computation of the first unique address for a recipient in every tuple of users. On some chains and environments AFP enables unique addresses for every transaction or makes that a user-selectable option.

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 paycode-based derivation of relationship-specific destination addresses. 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 AFP is its signaling system, which supports encrypted name lookup for Public Paycodes. For Bob to compute all possible addresses on which Alice can 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 AFP

- 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.
- Privacy-Preserving Transactions: By using relationship-specific, and in some deployments transaction-specific, destination addresses, the system reduces third-party ability to trace transaction histories or compute receive addresses from publicly accessible information.
- Backward Compatibility with OBPP-5: While building on OBPP-5, AFP is backward-compatible, enabling legacy BIP-47/OBPP-5 wallets to send funds to an AFP enabled wallet. However, the reverse requires an explicit send option for compatibility.

3.2 System Implementation Approaches

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

AmericanFortress-Hosted Infrastructure Approach

The initial AF Protocol deployment uses an AmericanFortress-hosted infrastructure model. Under this model, AmericanFortress operates the core non-custodial infrastructure required for Send-to-Name functionality, including signaling delivery, paycode lookup support, name-reservation automation, AF Token locking automation, recovery support, and related transaction-acceleration infrastructure.

This approach simplifies adoption by allowing users to access AFP functionality without directly managing AF Token operations, signaling infrastructure, or protocol-level coordination

themselves. When a user purchases or maintains a FortressName, the relevant AF Token locking, name-reservation, signaling, and infrastructure operations can be handled automatically by AmericanFortress-operated systems in the background.

AmericanFortress-hosted infrastructure does not custody user funds or assets and does not control user private keys. Users retain control of their wallets and transactions, while the hosted infrastructure provides the non-custodial coordination layer needed for name resolution, signaling, recovery, and transaction routing. Wallets are responsible for confirming that the required infrastructure is available and operating correctly before allowing a transaction to proceed.

Custodians, exchanges, wallets, and other platforms may integrate AFP through the AF SDK. In those cases, the integrating platform remains responsible for its own user relationship, custody model, and compliance obligations. AmericanFortress provides the Send-to-Name, signaling, paycode, privacy-preserving transaction, and acceleration infrastructure, but does not become a custodian merely by operating AFP infrastructure.

Future deployments may allow additional infrastructure operators, subject to technical, operational, compliance, and diligence requirements. For the initial deployment, however, the core AFP signaling and acceleration infrastructure is operated by AmericanFortress.

In this model:

- **Ease of Use:** Users are not required to directly manage AF Token locking, name-reservation mechanics, or signaling infrastructure. AmericanFortress-hosted systems automate these protocol interactions for ordinary users.
- **Operational Consistency:** Core signaling, paycode lookup support, recovery support, and acceleration infrastructure are operated by AmericanFortress to provide a consistent deployment environment.
- **Non-Custodial Infrastructure:** AmericanFortress-hosted infrastructure coordinates protocol functions but does not custody user assets, control user private keys, or act as the sender or recipient of user funds.
- **SDK-Based Distribution:** Wallets, custodians, exchanges, and applications may integrate AFP through the AF SDK while relying on AmericanFortress-operated infrastructure for the underlying Send-to-Name and signaling functions.

Distributed User-Driven Model

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

- Direct Token Access: Users can hold AF Token directly to perform name reservations and engage in AFP functionality, while the core signaling and acceleration infrastructure remains operated by AmericanFortress in the initial deployment.
- Community Ownership: This model encourages a sense of collective responsibility, fostering deeper engagement within the ecosystem.

The distributed model suits tech-savvy users who can manage the operational complexity. As stated previously, AmericanFortress will be performing the above operations for retail users via AmericanFortress-hosted and AF SDK-integrated wallets.

Balancing Hosted and User-Directed Use

The AF Protocol supports both a consumer-friendly hosted experience and more direct user interaction with AF Token and protocol functions. In the hosted model, AmericanFortress automates name reservation, token locking, signaling, recovery, and acceleration infrastructure

for users. In the user-directed model, advanced users may interact more directly with AF Token and selected protocol functions. In both cases, the core initial infrastructure is operated by AmericanFortress and remains non-custodial.

3.3 Zero-Knowledge Proof Technologies in AFP

AFP's privacy model is strengthened by zero-knowledge proofs that allow a recipient wallet or authorized verifier to verify the correctness of transaction relationships without exposing unrelated balances, addresses, or transaction history. These proofs can establish that the funds originated from the sender's authorization context, that the recipient-specific address derivation was performed correctly, or that the shielded note, nullifier, spend authorization, or other confidential-state transition is valid while still concealing balances, intermediate states, or unrelated wallet activity. The protocol is compatible with multiple proof-system families, including *zk-SNARKs*, *zk-STARKs*, and other succinct non-interactive proof constructions selected according to chain constraints and application requirements.

The application of these proofs to sender identification, source-of-funds continuity, and Confidentiality Machine flows is described in the Proof of Sender section. In this context, a Confidentiality Machine flow means an AFP deployment where funds pass through shielded state before settling to a recipient-specific destination, with zero-knowledge proofs preserving sender-origin assurance and paycode-lineage verification for the recipient.

AFP's proof layer can also be extended to post-quantum lineage and authorization proofs for hierarchical deterministic wallets. In a BIP32-Ed25519 deployment, a wallet can use a post-quantum zero-knowledge proof to show that a public key was derived from a valid master seed and derivation path, and that the signer controls the corresponding derived key material, without revealing the seed or private keys. This preserves the existing public-key and address format while allowing the authorization proof to be verified through a post-quantum proof system such as a ZK-STARK.

4 Multimodal Signaling for Paycode Transmission

Signaling is a core protocol function of the AF Protocol. As introduced in the protocol overview, signaling allows a recipient wallet to recognize the relevant sender relationship without exhaustively deriving possible destination paths for every potential counterparty. Without signaling, the recipient wallet would need to scan a very large set of possible sender-recipient paths, which is computationally expensive and does not scale. Signaling resolves this by communicating, in encrypted form, the minimum information needed for the recipient wallet to identify the relevant relationship-specific path while preserving privacy.

AFP treats signaling as a first-class concern and therefore implements it across *multiple* transport modes rather than one. We refer to this composite as *multimodal signaling*. The design goals are four:

- Computational efficiency: Recipient wallets can recover the correct derivation path without scanning the universe of possible senders.
- Privacy: The signal itself, and the aggregate volume of signals, do not leak the sender–recipient relationship to public observers.
- Redundancy: The system tolerates the temporary unavailability of any single transport.
- Recoverability: A wallet restored from seed can recover both incoming and outgoing transaction metadata, including counterparty name data, from stored paycode signals.

A single transport cannot satisfy all four goals simultaneously on all chains. AFP therefore separates signaling concerns from value transfer where possible and combines multiple transports under a policy layer that decides which to use by default, which to fall back to, and what privacy-protective overlays to apply.

4.1 What is Multimodal Signaling?

Multimodal signaling is the combination of (i) one or more *primary* signaling transports, (ii) an *inline backup* path that travels with the funds themselves, and (iii) two privacy-protective *overlays*, noise and beacon addressing, that apply across transports. The subsections below describe each component, what it carries at a conceptual level, and the privacy properties it is intended to provide. Implementation details such as specific storage networks, smart-contract standards, or encrypted-messaging protocols can vary by deployment and by target chain.

Primary Off-Chain Pathways

In a typical AFP deployment, the default signaling transport is off-chain. The sender's wallet emits a signal, an encrypted payload containing only what the recipient needs to identify the relationship and derive the correct destination path, and delivers it over an AmericanFortress-operated off-chain channel, such as a decentralized storage layer, private messaging relay, or comparable infrastructure service used by the AFP deployment.

DeFi Signaling Cryptography

In DeFi and smart-contract-integrated deployments, AFP signaling uses hybrid public-key encryption. The sender performs an ECDH-style key agreement using sender-controlled key material and the recipient's AFP paycode or signaling public key. In simplified form, if the sender samples an ephemeral key e and publishes $E = eG$, and the recipient has signaling public key $B_{\text{sig}} = b_{\text{sig}}G$, the sender derives an encryption secret from eB_{sig}, while the recipient derives the same secret from $b_{\text{sig}}E$. Both values equal $eb_{\text{sig}}G$. That shared value is passed through a key-derivation function and used to encrypt the signal payload with authenticated encryption. The encrypted payload may carry the sender paycode, routing metadata, supported-chain or asset context, nonces for replay protection, and optional proof or credential references. Integrity protection allows the recipient wallet to reject modified signals, while encryption prevents relays, storage providers, smart contracts, and public observers from learning the sender-recipient relationship or computing the recipient-specific destination address.

The signal contains an envelope addressed to a destination that the recipient can recognize, together with encrypted material that the recipient decrypts using key material it already controls. The signal does not carry the actual funds, does not expose the receive address on chain, and does not expose the sender's identity beyond what the recipient is already entitled to learn through the paycode relationship.

Off-chain signaling improves privacy in two ways. Because the signal itself is not written to a public ledger, its content is not subject to passive, forever-public retention by chain observers; only parties with access to the off-chain channel and to the recipient's decryption material can learn anything useful. Off-chain signaling also reduces public observability of signaling *volume*. Public chains leak traffic patterns by default: if every send-to-name interaction deposited a signal on-chain, the number, size, and timing of those deposits would themselves become an analytical surface. Routing default signals off-chain means the aggregate signaling volume associated with a given user or deployment is not directly visible to external observers.

Primary On-Chain Pathways

Some deployments benefit from an on-chain signaling pathway either as the primary transport or in parallel with off-chain delivery. In AFP, on-chain signaling is deliberately modeled as a *separate* chain of signals rather than as metadata embedded in the value-transfer transaction itself. For example, a signal is delivered as encrypted metadata in a minimal-value transaction or, on chains that support it, via a dedicated smart contract designed for signaling.

The signaling channel is conceptually decoupled from the actual value transfer. A single signal can represent an intent to transact across any chain or token, now or in the future, and a given value-transfer transaction need not carry its own signal at all. Because signaling and value transfer are not forced to share a transaction, it is significantly harder to correlate a signal with a specific settlement event using only public chain data. Unlike the classic BIP-47 / OBPP-5 pattern, which always embeds signaling with the funds as part of the same transaction's change output and therefore ties signal volume, signal timing, and payment timing together on-chain, AFP keeps the two surfaces separate.

Where on-chain signaling is used, AFP still treats it as an encrypted, relationship-specific payload. An observer can see that *a* signaling transaction or contract call occurred, but cannot decrypt the payload, cannot derive the recipient-specific address from it, and cannot attribute it to a particular user without access to the recipient's key material.

In-Line Backup Signaling

AFP also defines an *inline backup* signaling mode for cases where the preferred signaling transports are unavailable; for example, if an off-chain signaling relay is temporarily unreachable, or if a deployment's on-chain signaling channel is congested or unsupported on a given chain. In inline backup mode, the signal travels with the funds themselves. On UTXO-style systems, this typically takes the form of embedding the necessary signaling material in an auxiliary output of the value-transfer transaction, analogous to the BIP-47/OBPP-5 convention; on other chains, the equivalent is a small auxiliary payload attached to the payment transaction.

Inline signaling is explicitly a backup rather than a preferred mode because it re-couples signaling and value transfer. When a signal rides with the funds, an observer who watches the chain sees signaling and payment happen simultaneously, which reduces the correlation benefit described above. AFP's default policy is to route the true signal through the primary pathways and, when inline delivery is nevertheless used, to use inline content that contains only noise while the true signal is sent separately through another transport. The mere existence of inline content is not, by itself, evidence that the transaction carries a real signal.

Noise Protocol

Because signal content is encrypted under the recipient's keys, a passive observer cannot read a given signal. Encryption alone, however, does not protect against inference based on signaling *volume* or *timing*. If real signals are the only events that traverse a signaling channel, an observer can still infer activity from the fact that a signal exists at all.

AFP addresses this by defining a noise protocol: wallets and infrastructure components emit decoy signals that are indistinguishable from real signals under the threat model. Real and decoy signals share the same format, the same transport, and the same delivery characteristics, so that the presence of a signal on any given channel does not imply the occurrence of a real transaction. In aggregate, noise makes it significantly harder to use traffic analysis to attribute signaling to specific users or to infer that a particular deployment is processing a particular volume of real payments.

Noise is applied across transports. It is not a substitute for encryption; it is a complementary overlay that protects the aggregate signaling surface even when individual signal payloads are already confidential.

Beacon Addressing

The final overlay is beacon addressing. Rather than sending each signal to a destination that is uniquely observable per user, AFP directs signals to destinations that represent a pool of users. A beacon can be implemented as a shared address, channel, contract endpoint, storage namespace, or relay destination associated with many wallets, such that a signal arriving at that destination cannot be attributed to any single recipient by an outside observer.

AFP applies cryptographic masking to beacon traffic. The sender does not publish a recipient-specific routing label. Instead, the sender constructs a beacon capsule containing an ephemeral public key, an encrypted signal payload, and an authentication tag. The sender derives the encryption key through an ECDH-style shared secret using sender-controlled ephemeral key material and the recipient's AFP paycode or signaling public key, then applies a key-derivation function and authenticated encryption to the signal payload. The resulting capsule appears as random data to anyone who does not control the recipient-side key material.

The beacon destination itself can be rotated by epoch, pool, or deployment policy so that signaling does not create a stable, per-recipient public endpoint. Recipient wallets monitor the beacon pools to which they belong and attempt recognition or decryption locally. Beacon masking relies on the fact that only the intended recipient can derive the decryption key for a given capsule. A beacon capsule may contain an ephemeral public key, encrypted payload, and authentication tag. Publicly, all capsules have the same format. Privately, the intended recipient tests whether a capsule is for them by deriving the candidate shared secret and checking whether the authentication tag verifies. Non-recipients and outside observers see only pseudorandom encrypted data. Because real capsules and decoy capsules use the same external structure, a beacon observer cannot tell whether a capsule corresponds to a real payment, a decoy signal, or a different recipient in the same beacon pool.

Beacon addressing is therefore a privacy-protective overlay, not a routing substitute. Signals still traverse the primary pathways described above, but the destination layer no longer exposes a uniquely observable recipient address. Its purpose is to prevent signaling infrastructure from reintroducing the same per-user observability that AFP's encryption, noise, and recipient-specific address derivation are designed to avoid.

4.2 Signaling Architecture

The components above combine into a layered architecture rather than a flat list of options:

1. **Default primary pathways.** Wallets attempt to deliver each true signal through the deployment's primary transports, typically off-chain, and optionally in parallel with an on-chain signaling chain where appropriate.

2. **Fallback pathways.** If a primary pathway is unavailable, the wallet falls back to inline backup signaling. In this case, the wallet's default policy is still to send the real signal through the remaining primary pathway if one is available, and to populate the inline content with noise.

3. **Privacy-protective overlays.** Across all transports, AFP applies the noise protocol and beacon addressing to obscure signaling volume, timing, and per-user attribution.

A properly operating AFP wallet uses primary pathways first, treats inline signaling as a resilience measure rather than a feature, and relies on noise and beacon addressing as always-on overlays. These decisions are visible to the wallet and its user, but not to third-party observers of the chain.

AFP differs from prior paycode schemes in this layering. OBPP-5 and the BIP-47 family always embed signaling with the funds as part of the same transaction, which means the signaling

surface is, by construction, also the payment surface. AFP instead routes the default signal through a separate channel, so that a single signal can represent any transaction on any chain or token, now or in the future, without forcing each payment to carry its own observable signaling artifact. Beacon addressing, the noise protocol, inline backup signaling, and off-chain signaling, among other mechanisms, are additional distinctions embodied in AFP and covered in the patent-pending AF Protocol (see the Patent Families section).

4.3 Key Benefits of Multimodal Signaling

Enhanced privacy. Dispersing transaction signals across on-chain and off-chain pathways, combined with noise and beacon overlays, ensures that only intended parties can identify and process signals. External observers cannot easily infer transaction volumes or relationships from public data.

Redundancy and reliability. Multiple transports mean that a signal can still be recovered from an alternate pathway if one fails. A send-to-name transaction should succeed from the user's perspective even if a specific signaling channel is temporarily degraded.

Transaction-history recovery. Because signals are durable and relationship-specific, a wallet restored from seed can recover both incoming and outgoing transaction metadata, including counterparty name data, from stored paycode signals, even if data from one pathway is inaccessible. Recovery does not depend on any single transport remaining healthy.

4.4 What It Is Not

AFP's multimodal signaling is not a mixer. Chain analysis functions normally: balances, amounts, and settlement timing remain observable on the underlying chain exactly as they would be without AFP.

What AFP changes is the *signaling surface*:

it provides users with an efficient, privacy-preserving way to generate and use unique, relationship-specific on-chain addresses for each other, without coupling that signaling surface to the value-transfer surface.

5 Proof of Sender, Proof of Origin, and Sender Identification

A major design goal of AFP is to preserve *recipient awareness of sender identity* without exposing the sender–recipient relationship to public observers. In many financial contexts, privacy protects the transacting parties from third-party surveillance while still allowing those parties to know who they are dealing with.

In conventional public-chain transactions, third parties can often infer payment relationships from address reuse or transaction metadata. In some privacy-preserving systems, the opposite problem appears: public observers are blinded, but the recipient also lacks an inherent way to know who actually sent the funds. Through the interaction of names, paycodes, signaling, and counterparty-specific address derivation, the recipient can identify the sender relationship at the application layer while outside observers remain unable to derive that same relationship from public chain data alone.

5.1 Recipient Awareness Without Public Linkage

The AFP model allows users to transact through human-readable names and public paycodes that are meaningful to the parties but do not directly reveal the actual receive addresses used on-chain. When a sender initiates a transaction, the sender and recipient participate in a relationship-specific derivation flow tied to the recipient's paycode and the sender's signaling event. The recipient wallet can therefore associate the resulting transaction relationship with the sender identity already known through the AFP relationship model, even though a third party observing the chain cannot infer that same relationship from the on-chain data.

A privacy-preserving system does not need to blind the sender from the recipient in order to protect users from public surveillance. In many real-world payment settings, the recipient benefits from knowing who sent the funds, maintaining a coherent transaction history, replying to the sender, and, where appropriate, combining the transaction with selective credential sharing or compliance workflows. AFP is designed to preserve those recipient-facing properties while reducing public identity linkage.

5.2 Proof of Sender in the AFP Model

In the AFP model, sender identification is not limited to a user-interface label or a signaling hint. The protocol also provides a *proof of sender* or *proof of origin* showing that the transaction was in fact initiated by the party associated with the relevant paycode and name, so the recipient can receive cryptographic assurance that the funds were sent by the expected counterparty rather than relying on suspicion alone.

The proof-of-sender concept ties together three layers of the transaction relationship:

1. the sender's identity layer, represented by the paycode and associated name;
2. the transaction-derivation layer, in which the sender computes the recipient-specific destination path; and
3. the authorization layer, in which the sender proves control over the key material that actually originated and authorized the funds.

The sender–recipient relationship can remain hidden from public observers while still being provable to the recipient.

5.3 Role of Zero-Knowledge Proofs

Zero-knowledge proofs provide the cryptographic bridge between sender identification and transaction privacy in AFP. The recipient should be able to verify that a payment is linked to the expected sender, but that verification should not expose the sender's unrelated balances, addresses, transaction history, or confidential state to the public.

In AFP, the proof links the sender's key lineage, AFP identity, recipient-specific address derivation, and fund authorization. The recipient wallet can verify that the sender identity represented by a paycode and name is connected to the destination path used for the payment and to the key material that authorized the funds. In shielded-flow deployments, the same proof model can also link the confidential or shielded movement of funds that occurred before the visible settlement event.

Basic Example: Sender-Origin Proof. A simple example illustrates the role of the proof layer. Suppose Alice sends funds to Bob using Bob's FortressName and paycode. Alice's wallet derives a recipient-specific destination address for the Alice–Bob relationship and sends Bob an encrypted AFP signal. Alice can also generate a zero-knowledge proof showing that the payment

is linked to her AFP identity and authorization context without exposing her unrelated wallet activity.

In a non-shielded flow, the proof can show that Alice controls the private key corresponding to the source address used to fund the payment, and that the same sender-side key lineage is associated with Alice's AFP paycode. At a simplified Schnorr-style level, Alice commits to secret key material for both the source address and the paycode, derives a challenge from the commitments, the source public key, and the paycode, and responds in a way that lets Bob verify consistency without learning Alice's private keys. In simplified terms, the proof ties together three public facts, namely Alice's paycode, the source public key used to fund the transaction, and Bob's recipient-specific destination, while hiding the private witnesses that make those facts consistent. The hidden witnesses include Alice's source private key, Alice's paycode-related secret key material, and the shared payment secret used for the Alice–Bob derivation. Bob does not learn those witnesses; he only verifies that a valid proof exists linking the source authorization, Alice's paycode lineage, and the derived destination path. At a high level, the proof says that there exist secret values, namely Alice's source private key, Alice's paycode-related secret key material, and the Alice–Bob shared payment secret, that make the source public key, Alice's paycode, and Bob's derived destination consistent with the same sender-controlled lineage. The recipient therefore receives cryptographic assurance that the payment came from the party associated with Alice's paycode, rather than only relying on a user-interface label or signaling hint.

In a Confidentiality Machine flow, the same idea extends across the shielded path. Alice may first move transparent funds into shielded state and later de-shield them to Bob's recipient-specific destination address. The proof can show that the original transparent funding transaction, the shielded spend authorization, the de-shielded settlement, and Alice's AFP paycode lineage are connected to the same sender-controlled authorization context. Bob can verify sender-origin continuity, while the proof does not reveal Alice's unrelated source addresses, complete transaction graph, intermediate shielded balance, or other confidential wallet state.

This is the practical purpose of zero knowledge in AFP: the recipient can verify sender origin, address-derivation correctness, and fund-authorization continuity, while public observers cannot reconstruct the sender-recipient relationship from chain data alone.

The sender-recipient relationship remains hidden from public observers, while the recipient can verify that the payment originated from the expected sender context. The proof does not require the recipient to learn unrelated wallet balances, unrelated transaction history, or other confidential state.

AFP is compatible with multiple zero-knowledge proof systems, including zk-SNARKs, zk-STARKs, and other non-interactive proof systems. Deployments select the proving system based on chain constraints, verification cost, proof size, performance, and trust assumptions. The proof layer verifies sender-origin correctness while minimizing disclosure.

5.4 Confidentiality Machine Proof of Funds Compatibility

The AF Protocol can be paired with a Confidentiality Machine (CM) that adds a shielded transaction layer to the ordinary AFP send-to-name flow. CM is based on the same general class of shielded-transaction techniques pioneered by systems such as Zcash: transparent funds can enter shielded state, zero-knowledge proofs can validate shielded movement without exposing transaction details, and funds can later de-shield to a transparent destination. In AFP, that destination is not a reusable public address but a recipient-specific address derived through the AFP paycode and signaling model. The result is a $t \to z \to t$ flow: funds enter from a transparent account or UTXO, pass through shielded state, and settle back to a transparent recipient-specific address.

The AF implementation differs from Zcash-style shielded systems in two important respects. First, CM is designed to operate as a confidentiality layer for AFP-compatible assets and

deployments, rather than requiring users to move value to a separate privacy chain or external mixer. Second, CM is paired with AFP sender-recognition and CM-POF, so the recipient can verify sender-origin continuity and paycode lineage even though public observers cannot link the sender, shielded state, and recipient-specific settlement address.

AFP preserves sender intelligibility for the recipient. A conventional shielded transfer can hide the sender not only from public observers, but also from the recipient. That is undesirable in many commercial, institutional, and compliance-sensitive payment contexts. In a CM deployment, AFP keeps the public sender–recipient relationship hidden from the chain, while allowing the recipient wallet to verify that the payment is linked to the expected sender identity, paycode, and key lineage.

In a CM flow, funds entering shielded state are represented by a note commitment rather than by a publicly readable balance. The commitment binds the note value, recipient data, and randomness, while hiding those values from public observers. When the note is later spent, the system publishes a nullifier derived from note-specific secret material. The nullifier allows the network to reject double-spends without revealing which committed note was consumed. CM-POF then connects this shielded-note lifecycle to AFP's sender-origin model: it proves that the transparent funding transaction, shielded spend authorization, de-shielded settlement, and recipient-specific AFP destination are all linked to the same sender-controlled authorization context.

The Confidentiality Machine Proof of Funds (CM-POF) is the proof layer that connects these pieces. It links the sender's AFP identity layer, the shielded transaction path, and the recipient-specific settlement address without exposing the sender's broader wallet history. The proof establishes four relationships:

- The sender's master private key, or key material derived from it, authorized the de-shielded spend to the recipient-specific destination address.
- The same sender-controlled key lineage authorized the original shielding transaction and controlled the transparent accounts or UTXOs used to fund the shielded state.
- The key lineage used for shielding and de-shielding is also the lineage associated with the sender's AFP paycode and therefore the sender's protocol identity.
- The value delivered to the recipient-specific destination was sourced from sender-controlled shielded state, not from unrelated third-party pooled funds.

Put simply, CM-POF proves continuity across three layers: source authorization, shielded-state authorization, and recipient-specific settlement. The public chain sees commitments, nullifiers, and settlement events. The recipient receives proof context showing that those events are connected to the expected sender lineage. Public observers do not receive enough information to reconstruct that relationship.

This creates a different privacy posture from anonymity-first shielded systems. CM can reuse the shielded-note and zero-knowledge design pattern associated with Zcash-style systems, but it adds recipient-facing sender assurance and AFP-specific proof-of-funds continuity. The goal is not to blind all parties equally. The goal is to hide the transaction relationship from public observers while preserving intelligibility between the sender and recipient.

These relationships allow the recipient to verify sender-origin continuity without receiving the sender's complete source graph, intermediate shielded balance, unrelated addresses, or broader transaction history. Public observers see the public-chain events available on the underlying ledger, but they do not receive the AFP proof context needed to map the sender's identity, the shielded state, and the recipient-specific destination into a single relationship. The recipient can know who paid, verify that the payment came through the claimed sender-controlled lineage, and maintain a coherent transaction record, while third-party observers do not learn the sender–recipient relationship from public chain data alone.

5.5 Recipient Protection

Many privacy systems hide the sender not only from the public, but also from the recipient. That may be acceptable in some anonymity-first contexts, but it is often undesirable in commercial, regulated, or reputation-based transactions. In those settings, the recipient needs to know who paid them, whether that party is credentialed, whether a transaction is part of an ongoing business relationship, or whether a payment came from the expected counterparty at all.

AFP is designed so that privacy does not require recipient blindness. Instead, the protocol aims to preserve:

- **public privacy**, meaning outside observers cannot easily map identities to transaction relationships; and
- **recipient intelligibility**, meaning the recipient can still know who sent the funds and can receive cryptographic assurance that the transaction came from that sender.

5.6 Reducing the Need for Viewing-Key Infrastructure

Many privacy-preserving systems face a usability and compliance challenge because the recipient does not inherently know who sent the funds. In such systems, the protocol requires a separate selective-disclosure or viewing-key mechanism so that a recipient, auditor, or authorized counterparty can later determine transaction origin. While such architectures can be useful in some contexts, they introduce additional complexity, operational burden, and disclosure-management requirements.

AFP can reduce reliance on dedicated sender-identification viewing-key mechanisms *inside* a confidentiality architecture because the sender–recipient identity relationship is already established through the protocol's names, paycodes, and signaling model. In an AFP-style interaction, the central problem is not reconstructing sender identity after the fact, but rather proving that the funds actually originated from the sender identity already known to the recipient.

For confidentiality-machine-style flows, the protocol can focus on proving sender continuity and source integrity rather than forcing the recipient to rely on a separate viewing-key regime just to learn who sent the money. AFP preserves recipient awareness of sender identity at the application layer and directs its cryptographic machinery toward proving origin, continuity, and correctness, avoiding the complexity typically associated with dedicated viewing-key infrastructure.

5.7 Optional Selective Source-of-Funds Disclosure

In some deployments, AFP also supports optional source-of-funds disclosures for cases where a recipient, institutional counterparty, or compliance workflow requires greater assurance about the originating path of funds. Such disclosures are selective and need not be part of the default user experience. For example, the sender may provide recipient-verifiable proof regarding the originating address set, key lineage, or source transaction context without broadly disclosing unrelated wallet activity. The design keeps transactions hidden from the public, intelligible to the parties, and selectively disclosable only where necessary.

5.8 Post-Quantum Lineage and Authorization Proofs

AFP can support a post-quantum proof mode for hierarchical deterministic wallets, particularly BIP32-Ed25519 wallet structures. In this mode, the wallet does not need to migrate to a new public key or register a new address. Instead, the existing BIP32-Ed25519 public key remains the public identifier, while a zero-knowledge proof demonstrates that the signer knows the master seed or derived key material required to produce that public key through the stated

derivation path. In simplified notation, a seed x_0 and derivation path $(i_1, \ldots, i_n)$ produce a derived Ed25519 key pair and public key A_n. The post-quantum proof does not reveal x_0 or the derived private key material; instead, it proves that the public key A_n was produced by correctly applying the stated derivation procedure and that the signer controls the authorization material associated with that derived key.

In compatible environments, the proof can replace or supplement the classical signature authorization step with a post-quantum proof of lineage and authorization. A recipient, verifier, or compatible blockchain environment can verify that the public key was honestly derived and that the transaction was authorized by the corresponding wallet lineage, without learning the seed, private keys, nonce material, or unrelated wallet state.

In optimized deployments, the derivation proof can be separated from the per-message signing proof. In split-proof deployments, the derivation proof establishes the relationship between the seed lineage and the public key once, while the per-message proof establishes authorization for a specific message or transaction. This avoids recomputing the full derivation proof for every ordinary transaction and allows AFP to preserve the same sender-origin and paycode-lineage semantics described above while providing a migration path toward post-quantum authorization.

Current post-quantum proof systems involve performance and deployment tradeoffs. In particular, proving full BIP32-Ed25519 derivation inside a STARK circuit can be computationally expensive, and some blockchain deployments would require support for verification of the proof format. For this reason, post-quantum lineage proofs should be treated as an advanced or future-facing AFP deployment mode rather than a default requirement for ordinary Send-to-Name transactions.

6 Use Cases for AFP and the Send-to-Name Protocol

6.1 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.

6.2 Decentralized Finance (DeFi) Integration

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

6.3 Privacy-Enhanced Wallet Services

Wallets using AFP 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.

6.4 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. AF Token is used to reserve and lock these names, adding practical utility and contributing to supply reduction.

6.5 Strategic Additions and Distribution

To expand the AF Protocol's market reach and deepen token utility, the following strategic initiatives may be pursued:

Enterprise Licensing Model

Offering an enterprise-grade SDK that enables wallets, fintechs, custodians, exchanges, and payment processors to integrate Send-to-Name and privacy-preserving signaling directly into their platforms. Licensing may include built-in AF Token functionality, tying enterprise integrations to recurring protocol usage while accelerating adoption across large-scale user bases.

Institutional KYC Integrations

Establishing partnerships with leading identity verification providers to deliver seamless, compliant KYC/AML credentialing within the protocol. This would enable institutional clients to meet regulatory requirements without sacrificing privacy, positioning AF as a trusted layer for compliant digital asset transactions.

7 Economic Model and Utility

AF Token powers key functions within the AF Protocol, including name reservation, signaling, credentialed access, paymaster tolling, Confidentiality Machine services, and infrastructure participation. The economic model combines usage-based locking with revenue-linked token mechanisms, including buybacks, burns, reserves, and ecosystem programs where permitted and approved under applicable governance or treasury policies.

7.1 Tokenomics Overview

Total supply: 10,000,000,000 AF Token.

Ticker: $AF.

Illustrative launch price: $0.10.

Illustrative fully diluted valuation at launch: $1,000,000,000.

Token allocation breakdown:

Category	**Tokens**	**% of Supply**
Community / User Incentives	3,000,000,000	30.00%
Treasury	1,760,000,000	17.60%
Engineering	1,200,000,000	12.00%
Team & Advisors	1,000,000,000	10.00%
Marketing	1,000,000,000	10.00%
Liquidity / Market Making	1,000,000,000	10.00%
MF Private Round 2	715,000,000	7.15%
MF Private Round 1	325,000,000	3.25%
Total	**10,000,000,000**	**100.00%**

Private Round 1 and Private Round 2 refer to private rounds of the AF Token sale prior to TGE, including allocations to early investors and strategic contributors.

Vesting and cliff schedule:

Category	TGE Unlock	Cliff	Vesting Model
MF Private Round 1	25.00%	none	75.00% linear over 8 months
MF Private Round 2	15.00%	none	85.00% linear over 12 months
Liquidity / Market Making	100.00%	none	N/A
Team & Advisors	5.00%	none	95.00% linear over 24 months
Engineering	5.00%	3 months	Remaining allocation linear over 24 months
Marketing	6.00%	none	94.00% linear over 18 months
Community / User Incentives	2.50%	none	97.50% linear over 48 months
Treasury	5.00%	6 months	Remaining allocation linear over 48 months

At TGE, the initial circulating supply is expected to be approximately 1,521,500,000 AF Token, or 15.215% of total supply, including liquidity and market-making allocations. Excluding liquidity and market-making allocations, the initial circulating supply is approximately 521,500,000 AF Token, or 5.215% of total supply. These figures are based on the token allocation and vesting assumptions in the tokenomics model and may be updated before TGE.

7.2 Utility for Name Reservation and Signaling

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

- Name Reservations and Credentialed Access: Users can lock AF Token to reserve unique, globally recognizable names and access credentialed identity features described in the KYC/AML Compliance and Identity Verification section. These remain locked as long as the reservation is active, creating a steady reduction in circulating supply.
- Signaling Usage: AF Token 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.

7.3 Revenue-Linked Buybacks, Burns, Locking, and Ecosystem Programs

Revenue-Linked Token Mechanics

AF Token is designed to connect protocol activity with token utility through name reservations, signaling, paymaster tolling, Confidentiality Machine usage, and other infrastructure services. In addition to locking mechanisms, the protocol may allocate a protocol-defined portion of eligible revenues to market buybacks, token burns, ecosystem reserves, infrastructure incentives, or other governance-approved uses.

For name reservations, eligible revenue may support programmatic AF Token buybacks from the market. For certain name products, including lifetime-name reservations, tokens acquired through those buybacks may be burned rather than retained in reserves. The amount of AF Token acquired will depend on the market value of AF Token at the time of execution and on the protocol parameters then in effect.

Confidentiality Machine revenue may follow a similar model. A protocol-defined portion of CM-related revenue may be allocated to buyback-and-burn activity, reserves, or other utility-supporting mechanisms approved under the protocol's governance or treasury policy. The exact

allocation percentages may vary over time based on governance decisions, market conditions, regulatory considerations, and operational requirements.

These mechanisms are intended to link token flows to actual usage of AFP services rather than to discretionary market intervention. Buyback, burn, locking, reserve, and incentive policies should therefore be understood as protocol-economic mechanisms tied to name reservation, signaling, CM usage, paymaster tolling, and infrastructure activity.

At a protocol-accounting level, the number of locked tokens depends on active name reservations, credentialed-access features, and signaling requirements. Eligible revenue from name reservations, CM usage, and paymaster tolling may be allocated across reserves, infrastructure incentives, buybacks, or burns according to governance-defined parameters. For lifetime-name reservations, acquired tokens may be burned rather than retained, while recurring services may allocate eligible revenue across buybacks, reserves, or ecosystem programs.

7.4 Utility-Based Locking and Signaling Usage

AF Token is designed to emphasize locking for name reservations and usage in signaling because these mechanisms connect token utility to actual protocol activity:

- Real Utility from Name Reservations: Name reservations require AF Token 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 AF Token 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, linking token demand to actual network usage.

By connecting token demand to name reservations, signaling, and related protocol services, AF Token fosters tokenomics tied to real use and user participation within the AF Protocol.

7.5 Utility from Paymaster Tolling and Sponsored Execution

In addition to name reservations and signaling, AF Token supports usage tied to *paymaster tolling* or *sponsored execution services*. In these models, a protocol component or smart-contract-based paymaster provides a functional service to wallets, applications, custodians, or counterparties and charges a fee for that service. The fee is not framed as an arbitrary tax, but as payment for privacy infrastructure, name resolution, signaling delivery, transaction sponsorship, credential-aware policy checks, or other execution-layer services provided by the AFP ecosystem. Revenue from paymaster tolling, sponsored execution, and Confidentiality Machine services may also feed into the protocol's revenue-linked token mechanics, including buybacks, burns, reserves, infrastructure incentives, or other governance-approved uses.

Tolling ties token demand to real protocol activity. A tolling service model can complement name reservations by introducing recurring transactional demand from high-frequency users, enterprise partners, or integrated applications. Rather than depending solely on user acquisition at the naming layer, the protocol also benefits from ongoing usage at the execution and infrastructure layer.

Why Tolling Fits the AFP Model

The AF Protocol is not only a naming layer; it is also a privacy-preserving transaction infrastructure layer. Where that infrastructure is used as a smart-contract service, sponsored transaction layer, or policy-controlled transaction gateway, a tolling model is a natural economic fit. It aligns token demand with actual service consumption and supports a usage-based commercial model that is easier to justify to enterprise integrators and sophisticated market participants.

Revenue Quality and Demand Quality

From a tokenomics perspective, paymaster tolling can improve the *quality of demand* because it is tied to recurring operational use. This can strengthen the protocol's economic model in three ways:

1. **Recurring usage:** integrated wallets and applications consume the service repeatedly rather than only at the point of user onboarding;
2. **Enterprise monetization:** AF SDK-integrated platforms can generate demand linked to real customer flows; and
3. **Infrastructure-linked value capture:** the token is supported by protocol activity that corresponds to concrete services delivered by the network.

Sustainable protocol economics should be driven by real utility, locking, infrastructure participation, and commercial use rather than by purely cosmetic supply mechanics.

7.6 Governance Framework

The AF Protocol will incorporate a governance framework to manage protocol parameters, support reliable network operations, and align token utility with actual usage of name reservation, signaling, and infrastructure services. Key features of the governance framework include:

- Dynamic Adjustments: The framework enables AmericanFortress-operated infrastructure to modify protocol variables such as the number of tokens locked per name, with future approved infrastructure operators able to participate where governance and diligence requirements are met. These adjustments respond to market conditions, aligning supply and demand with real-world needs.
- AF SDK-Integrated Platforms: Wallets, custodians, exchanges, and applications integrating through the AF SDK remain responsible for their own user relationships and compliance obligations, while AmericanFortress-operated infrastructure aligns core protocol operations with governance decisions to maintain stability and support the protocol's objectives.
- Support for Diverse Models: The governance framework will accommodate both hosted and user-directed models, allowing seamless integration of AmericanFortress-hosted infrastructure and more direct user interaction with protocol functions.
- Long-Term Sustainability: By dynamically managing tokenomics, the governance framework will ensure that AF Token remains viable as a utility token, supporting the protocol's growth while maintaining stability.

8 KYC/AML Compliance and Identity Verification

Know Your Customer (KYC) and Anti-Money Laundering (AML) expectations are important considerations for the adoption and legitimacy of cryptocurrency protocols. The AF Protocol is designed to support KYC/AML and travel-rule workflows through selective credential disclosure, subject to jurisdiction, implementation, and the requirements of participating counterparties.

8.1 Credentialed Access with AF Token

Users can lock AF Token to access credentialed identity features and obtain cryptographic credentials tied to blinded or unblinded claims. To obtain credentials, users undergo identity verification with participating credential issuers. A credential can be understood as a signed claim or signed commitment to a claim. For example, an issuer may verify Alice's identity documents and issue a credential supporting the claim "Alice is over 18 and resident in the United States." Alice can later prove a predicate about that credential, such as $age \geq 18$, without necessarily revealing her full name, document number, address, or complete identity record.

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 use selectively disclosing a passport-based credential 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 is designed so that only entities authorized by Alice can access the relevant proof or credential material, 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.

Users can complete a KYC process and obtain decentralized, blinded, and/or unblinded credentials to share with counterparties, proving for example that they are "over 18 and a resident of Wyoming," or selectively disclosing a passport-based credential, among other proofs.

8.2 Privacy-Preserving Compliance

By combining "Send-to-Name" with credentialed access, the AF Protocol is intended to balance credentialed compliance workflows and user privacy. Users can present credentials to counterparties without exposing personal information on the blockchain, where those counterparties accept such proofs.

8.3 Benefits of the Integrated Approach

- Regulatory Alignment: Designed to support KYC/AML and travel-rule workflows through selective credential disclosure, subject to jurisdiction, implementation, and participating counterparty requirements, where those workflows apply.
- User Privacy: Supports public pseudonymity through nyms, while allowing selective credential disclosure when required.
- Flexibility: Allows users to choose between pseudonymous and credentialed transactions based on their needs and regulatory obligations.
- Reduced Address-Manipulation Risk: AFP reduces reliance on manual address handling, which can lower the risk of address-substitution and copy-paste phishing attacks. Users can verify counterparty names and credentials before sending funds, instead of relying only on raw blockchain addresses.

By incorporating these mechanisms, the AF Protocol provides a privacy-focused framework intended to support credentialed compliance workflows in the digital asset space, as required by jurisdiction, implementation, and participating counterparties.

9 Integration with Existing Naming and Credential Systems

AFP signaling is designed to integrate with selected blockchain naming services and decentralized identity frameworks, including ENS, Basenames on Base, Unstoppable Domains, Dash DpNS, and other compatible naming systems. These integrations allow AFP-compatible wallets to resolve familiar human-readable identifiers while still using AFP paycodes, signaling, and recipient-specific address derivation to preserve transaction privacy.

In Base ecosystem deployments, Basenames may provide a natural user-facing identity layer, while AFP provides the privacy-preserving payment, signaling, and sender-recognition layer underneath. This allows a user-facing Base identity to coexist with relationship-specific destination addresses, reducing the need to expose static receive addresses in ordinary payment workflows.

AF is actively pursuing integrations with selected name systems so that users can interact through familiar names while wallets apply AFP's privacy-preserving derivation and signaling logic in the background.

10 Conclusion

The AF Token and the AmericanFortress Protocol provide a practical approach to privacy-preserving cryptocurrency payments. By combining Send-to-Name usability, multimodal signaling, recipient-aware privacy, credentialed access, and revenue-linked utility mechanisms, AFP aims to support digital asset transactions that are easier to use, harder to publicly correlate, and better suited to wallet, institutional, and application-level integrations.

11 Patent Families

The following patent families relate to technologies referenced or used in the AmericanFortress Protocol, including wallet infrastructure, cryptographic transaction systems, privacy-preserving paycode infrastructure, zero-knowledge identity credentials, Confidentiality Machine proof-of-funds flows, and payment-code lineage proofs. The "MF" codes are internal portfolio identifiers. Public application or publication numbers are listed where available. Where an application remains unpublished or a publication number has not yet been assigned, the family is identified by title and filing status.

MF-P0001, Crypto Currency Hardware Wallet
U.S. Divisional Application No. 19/551,596
PCT Publication: WO 2024/043935
PCT Application: PCT/US22/75476
Status: Pending family; national phase filings pending in selected jurisdictions.

MF-P0002, Secure Cryptographic Server Card
U.S. Patent Application No. 17/732,511
PCT Publication: WO 2024/043936
PCT Application: PCT/US22/75477
Status: Allowed in the United States; national phase filings pending in selected jurisdictions.

MF-P0003, Cryptographically Secured Hybrid Cryptocurrency System
U.S. Patent No. US12412162B2
U.S. Application No. 17/583,189
Status: Granted.

MF-P0005, CFilter Caching for Crypto Currency Wallet
U.S. Patent Application No. 18/301,773
U.S. Publication: US20230385810A1
Status: Published.

MF-P0006, Privacy-Preserving Cryptocurrency Transactions
PCT Publication: WO 2025/244654
PCT Application: PCT/US25/35538
Status: Pending.

MF-P0008, Zero Knowledge Proof Identity Credentials (AML)
U.S. Patent Application No. 18/815,394
U.S. Publication: US20250069062A1
Status: Published.

MF-P0009, Cryptographically Confidential Transaction on Distributed Public Ledgers (referenced in the Proof of Sender section)
U.S. provisional application filed; PCT filing in process.
Status: Pending / publication not yet public.

MF-P0010, Cryptographic Proofs of Master-Key Lineage for Payment Codes and Payment Addresses
PCT Application: PCT/US26/27468
Status: Pending / publication pending.

MF-P0011P, Post-Quantum Zero-Knowledge Lineage and Authorization Proofs for Hierarchical Deterministic Wallets
U.S. provisional application filed; PCT filing in process.
Status: Pending / publication not yet public.