BUBIWOT Litepaper 0.2

towards sovereign accounts, banking, and communication

Robert F. Ussery III

June 2025

Abstract

BUBIWOT (Bitcoin-backed Universal Basic Income Web of Trust) introduces a novel decentralized identity and account recovery protocol built on the Babylon protocol, integrating a novel cryptographic key recovery scheme using CosmWasm smart contracts to create a decentralized web of trust. The protocol establishes a sustainable economic model where token holders earn a share of protocol revenue in Bitcoin, and it powers a decentralized, censorship-resistant social platform. The protocol leverages real-life peer-to-peer (IRL) attestations to securely establish and recover accounts, proving humanity through strong-form identity, and economically incentivizing truthful participation. This paper provides a concise overview of the BUBIWOT architecture, its core functionalities, and the economic incentives that underpin its security model.

1 Introduction

The BUBIWOT protocol is engineered to address critical challenges in decentralized identity management and account security. By integrating real-world, inperson verification with a robust cryptographic and economic framework, BUBIWOT aims to provide a secure, censorship-resistant, and user-centric system for identity attestation and account recovery.

2 Overview

BUBIWOT is designed to achieve the following core objectives:

- Facilitate in-real-life (IRL) peer-to-peer identity attestations.
- Enable cryptographic, decentralized account recovery.
- Distribute Universal Basic Income (UBI) tokens backed by staked Bitcoin.
- Provide a yield-bearing native token (BUBI) that captures a share of network fees.
- Enable a decentralized, value-ranked content and communication platform.
- Ensure robust security and censorship resistance.
- Provide economic incentives to foster honest participation and disincentivize malicious behavior.

3 Technical Architecture

The BUBIWOT ecosystem is best understood as a multi-layered stack designed for sovereignty and security. It is composed of four primary, interconnected components:

1. **The BUBIWOT Appchain:** A sovereign, application-specific blockchain built with the Cosmos SDK. It serves as the core execution environment, validating transactions and maintaining the ledger of accounts and token balances. It integrates Babylon's consumer module to anchor its security directly to the Bitcoin network.
2. **The Smart Contract Layer:** The protocol's application logic is encapsulated in upgradeable CosmWasm smart contracts written in Rust. These contracts manage user accounts, guardian relationships, the UBI minting process, and on-chain pointers for the social platform, enabling flexible governance and evolution.
3. **The In-Browser P2P Client:** The user-facing application, built with modern web technologies (TypeScript, CosmJS, libp2p, Nostr), functions as a light client. It securely manages user keys and orchestrates communication with the BUBIWOT Appchain for transactions and with decentralized P2P networks (Nostr, libp2p) for social interactions and secure data exchange.
4. **Off-Chain Validator Services:** Critical functions that bridge to the Bitcoin network are handled by off-chain services run by the appchain's validators. The most important of these is a **Threshold Signature Scheme (TSS) Service**, which allows validators to collectively manage a Bitcoin treasury. This enables the protocol to programmatically distribute Bitcoin rewards and fee dividends as instructed by the smart contracts, without a single point of failure.

4 Account Recovery via Bottom-Up Secret Sharing

The account recovery process is redesigned around a powerful cryptographic primitive known as Bottom-Up Secret Sharing (BUSS), as detailed in the ANARKey paper. This eliminates complex on-chain state management in favor of a more secure and efficient two-phase, primarily off-chain process. This process consists of a one-time backup phase and a recovery phase.

4.1 Phase 1: One-Time Key Backup

This is an off-chain setup process performed by the user's client to generate and store public recovery data.

1. **Guardian Selection:** The user selects a set of guardians and a recovery threshold ($t+1$) in their client.
2. **Off-Chain Share Generation:** The user's client requests a "share" from each guardian over the P2P network. Each guardian's client uses its own secret key to deterministically compute a unique share for the user and sends it back. Guardians do not store this share.
3. **Public Data Creation:** The user's client combines its own secret key with the shares from its guardians to define a secret polynomial. It then computes a set of public points from this polynomial. This is the **public recovery data**.
4. **On-Chain Storage:** The user submits a single transaction to store this public recovery data in the BUBIWOT smart contract, permanently linking it to their account.

4.2 Phase 2: Account Recovery

When a user loses their device, they use their new device to perform the following off-chain reconstruction.

1. **Data Retrieval:** The user's client fetches the public recovery data from the smart contract.

2. **Share Re-computation:** The user contacts the required threshold of guardians ($t+1$). The guardians perform the exact same deterministic computation as before to re-generate the exact same shares and send them to the user.

3. **Key Reconstruction:** The user's client combines the public data points with the newly received guardian shares. This is enough information to perfectly reconstruct the original secret polynomial and compute the original secret key. The user's account is now recovered without any complex on-chain voting or session management.

5 Cryptographic and Economic Foundations

The security of the BUBIWOT protocol rests on several key pillars:

- **IRL Web of Trust:** The protocol is founded on an economic web of trust. Security doesn't rely on technically proving an in-person meeting, but on the principle that guardians are economically liable for their attestations. This foundation supports a novel **Bottom-Up Secret Sharing** scheme, allowing for cryptographic key backup among trusted, dynamically managed peers. **To prevent cascading failures (the "domino effect" where recovering one user's key could lead to the compromise of another), users who choose to act as guardians use a dedicated, separate "guardian key" for recovery operations. This isolates a user's guardian duties from their personal account key. However, this critical design choice introduces a user-experience trade-off: users who act as guardians must securely manage a second key. Loss of this guardian key does not result in a loss of the user's own funds, but it does prevent them from helping others in recovery, and requires them to reestablish their guardian relationships.**

- **BUBIWOT Smart Contracts on a Sovereign Appchain:** The core logic runs in smart contracts on the BUBIWOT Appchain, a sovereign blockchain built with the Cosmos SDK. This appchain uses the Babylon protocol to anchor its security to Bitcoin. The smart contracts function as a decentralized and immutable bulletin board for storing the **public recovery data** required by the BUSS scheme, while also managing the protocol's economic incentives, on-chain Sybil penalties, and content pointers for the social platform.

- **Trust-Minimized BTC Distribution:** The protocol can programmatically distribute Bitcoin rewards and network fees from a protocol-owned vault. This vault is secured by a Threshold Signature Scheme (TSS) operated by the BUBIWOT appchain's own validator set, removing single points of failure and allowing smart contracts to safely trigger BTC payouts.

- **Strong-form Proof-of-Personhood:** BUBIWOT establishes a robust method for identity validation, a critical component for scalable UBI.

- **User-Defined Trust Policies:** BUBIWOT rejects a one-size-fits-all security model. Instead, each user defines their own on-chain policy for who they trust. A user can set specific requirements for anyone wishing to attest for them, such as a minimum reputation score, a minimum amount of staked BUBI, or whether the attestor must already be a a verified human. This creates a flexible, user-sovereign trust graph. New users can set lenient policies to get bootstrapped into the network, while established users can enforce stringent policies to maximize their security.

6 Economic Incentives

The economic model is designed to align participant interests with the security and integrity of the network.

- Users stake Bitcoin on the L1 blockchain via the Babylon protocol to participate.

- **Productive BUBI Token:** Holding BUBI tokens entitles the user to claim a proportional share of the network's accumulated Bitcoin fees, making it a productive, yield-bearing asset.

- Guardian attestations are incentivized through rewards in both Bitcoin and the protocol's native token. Bitcoin rewards are distributed from a decentralized, protocol-owned vault controlled by the BUBIWOT validator set via a Threshold Signature Scheme (TSS).

- To deter malicious behavior, slashing penalties are imposed on guardians who act dishonestly.

- **UBI is distributed via a user-initiated "pull" model. Verified humans can claim their accrued BUBI tokens at any time, which are newly minted upon claim. This empowers users and aligns token emission directly with active participation.**

7 Risk Analysis and Mitigation

BUBIWOT anticipates several potential threats and proactively implements safeguards:

7.1 Collusion Among Guardian Peers

Threat: Multiple guardians might conspire to maliciously control or recover a user's account.

Mitigation: Users set customizable multi-attestation thresholds, requiring a quorum of guardians for any critical action. The cryptographic scheme ensures that fewer than the threshold number of guardians have zero information about the user's key. **Furthermore, the risk of a cascading "domino effect" is mitigated by having users who opt-in to be guardians use a dedicated guardian key. This separates their guardian responsibilities from their personal account security. This means these users are responsible for backing up a second key (e.g., via a mnemonic phrase). While loss of this key doesn't impact their own funds, it is a critical piece of their participation in the social web of trust.** The ability to dynamically replace guardians via a time-locked transaction further reduces long-term collusion risk.

7.2 Sybil Attacks

Threat: Malicious actors attempt to create numerous fraudulent identities to manipulate UBI distribution.
Mitigation: The protocol features a two-level defense system.

1. **Level 1: Automated On-Chain Penalties.** The protocol's primary defense is economic. By requiring staked BTC and making guardians financially liable for their attestations, BUBIWOT creates a powerful disincentive against approving fake accounts. Should a Sybil account be identified, it is automatically penalized on-chain by having its BUBI tokens confiscated and reputation destroyed. The guardians who attested for the Sybil are also penalized, reinforcing the web of trust.

2. **Level 2: Bitcoin-Grade Consensus Security.** For catastrophic, large-scale attacks that threaten the protocol's integrity, BUBIWOT inherits Bitcoin's security via the Babylon protocol. If malicious actors attempt to attack the BUBIWOT appchain itself (e.g., by double-signing blocks to revert penalties), their actions constitute a BFT consensus violation. Babylon's protocol is designed to detect such violations, which automatically reveals the attackers' private keys. This allows anyone to submit a transaction to the Bitcoin network to slash the attackers' staked Bitcoin, providing a crucial backstop that secures the BUBIWOT chain's state and its enforcement of penalties.

7.3 Loss of Devices or Keys

Threat: Accidental key loss jeopardizes user accounts and staked funds.
Mitigation: Robust social recovery is achieved via the cryptographic **Bottom-Up Secret Sharing** scheme. By retrieving public data from the smart contract and collecting deterministic shares from a threshold of guardians, a user can securely reconstruct their original key on a new device. **Crucially, this recovered key is the same key that controls the user's staked Bitcoin on the L1, ensuring that the primary economic stake is protected by the social recovery mechanism.**

7.4 Guardian Unresponsiveness & P2P Disruption

Threat: A user's recovery may be stalled or blocked if their guardians are offline, have lost their keys, or refuse to cooperate.
Mitigation: The protocol implements a multi-layered approach to ensure guardian availability.

- **Off-Chain Liveness Signaling:** The BUBIWOT client can use the **Nostr** protocol for lightweight, off-chain "heartbeats." Guardians can periodically publish a signed Nostr event to signal their activity. This provides a real-time social signal of liveness that helps users monitor the health of their guardians without incurring on-chain fees.

- **On-Chain Guardian Replacement:** A user can initiate a formal, time-locked replacement process on the BUBIWOT appchain at any time. This provides a definitive, trust-minimized mechanism to maintain a healthy and active set of guardians, ensuring recovery is always possible. The time-lock ensures the existing guardian has a window to observe the pending change.

8 Use Cases

The BUBIWOT protocol is designed to support a wide variety of essential human interactions through secure, decentralized technology:

- **Banking and UBI:** Users can securely send and receive BUBI tokens on the appchain. Crucially, holding BUBI tokens allows users to claim a proportional share of the network's BTC fees, creating a sustainable yield. The protocol itself can programmatically distribute rewards directly in Bitcoin (BTC) using a trust-minimized TSS vault.

- **Decentralized Authentication (Human-Verified OAuth):** BUBIWOT can serve as a decentralized authentication layer for both Web2 and Web3 applications. External services can post on-chain, incentivized "attestation requests" which any user can fulfill by providing a cryptographic signature. A Web2 service can prompt a user to sign a challenge message and offer a BUBI reward, which is held in escrow by the smart contract. Upon successful signature verification on-chain, the user receives the reward, and the Web2 service receives a verifiable proof of authentication. This creates a powerful, Sybil-resistant alternative to traditional login systems, backed by real economic incentives.

- **Decentralized Social Platform:** The protocol powers a censorship-resistant social media ecosystem. Users publish content (e.g., posts, replies) to decentralized **Nostr** relays. The BUBIWOT smart contracts store immutable, on-chain **pointers** to this content, including hashes, topics, and reply threads. This unique hybrid design enables a scalable social platform where content can be ranked and filtered by value (donated BUBI), creating a rich, user-curated attention economy.
- **Durable Identity and Reputation:** Users establish cryptographic proof-of-personhood through IRL attestations. This strong-form identity supports decentralized access control, reputation building, and social recovery, enhancing digital sovereignty.
- **Real-Time Social Consensus and Attention Economy:** The P2P client layer enables real-time flagging and voting on peer interactions, creating a dynamic social consensus layer. Users can attach micropayments (in BUBI) to messages or actions to incentivize others' attention, fostering a vibrant, responsive, and economically sustainable social graph.

9 Tokenomics and Distribution

The economic sustainability of BUBIWOT is reinforced through carefully structured tokenomics:

- **Total Supply and Emission:** A clearly defined total supply with a predictable emission model. New tokens are minted exclusively when verified users actively claim their Universal Basic Income (UBI). This "pull" mechanism ensures that supply expansion is directly tied to user engagement, rather than a passive, predetermined schedule.
- **Initial Distribution:** Tokens are distributed primarily through verified IRL attestations and UBI claims, rewarding users for onboarding authentic peers and actively participating in the network.
- **Incentives and Penalties:** Guardians and validators earn tokens for truthful participation, while dishonest behavior is economically disincentivized through slashing mechanisms tied directly to staked Bitcoin collateral.
- **Token Utility and Demand:** The BUBI token possesses deep utility. It functions as a medium of exchange in the protocol's attention economy, a reputation marker, and most importantly, a **yield-bearing asset** that grants holders a claim on the network's BTC-denominated fees. This creates a powerful and sustainable demand driver.

10 Conclusion

The BUBIWOT protocol establishes an innovative and decentralized framework for identity management. By leveraging the security of the Bitcoin network, the trust inherent in real-world relationships, and a system of incentivized human participation, BUBIWOT provides a robust, scalable, and secure solution for identity validation. This positions it as a foundational technology for global-scale UBI distribution and secure, decentralized account management.