BUBIWOT Litepaper

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 atop Bitcoin Lightning and Babylon CosmWasm smart contracts. 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, in-person 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

The BUBIWOT protocol represents a paradigm shift in decentralized identity by anchoring its web of social trust directly to the economic security of the Bitcoin network. It achieves this through a novel synthesis of in-person attestations and cutting-edge cryptoeconomics inspired by the Babylon protocol.

At its core, BUBIWOT utilizes a trust-minimized Bitcoin Staking model. Unlike traditional approaches that require bridging assets (a significant security risk) BUBIWOT allows guardians to stake their Bitcoin remotely. The capital remains in self-custodial contracts on the Bitcoin blockchain, serving as a security bond without ever leaving its native environment.

This architecture enables **fully automated and uncensorable slashing**. If a guardian attempts to compromise the network (e.g., by providing a fraudulent attestation), their actions cryptographically lead to the leaking of their private key. This leaked key is the only instrument that can authorize a pre-signed slashing transaction on the Bitcoin blockchain, resulting in an immediate and irreversible loss of their staked collateral. This mechanism ensures that every social attestation is backed by a tangible economic guarantee.

BUBIWOT is designed to achieve the following core objectives, secured by this robust model:

- **Economically Secured Identity:** Establish a strong-form Proof-of-Personhood where IRL attestations are backed by slashable Bitcoin stakes, creating a Sybil-resistant identity layer.
- **Trust-Minimized Account Recovery:** Enable secure, decentralized account recovery where guardians are economically bound to act honestly, mitigating collusion risks through automated slashing.
- **Anchored UBI & Finance:** Facilitate the distribution of Universal Basic Income (UBI) on a network whose integrity is continuously anchored to the Bitcoin chain via timestamping, ensuring transaction finality and security.
- **Censorship-Resistant Infrastructure:** Provide a platform where rules are enforced by immutable Bitcoin logic and verifiable cryptography, not by fallible intermediaries.

In essence, BUBIWOT transforms social trust into a system of verifiable and cryptoeconomically-aligned accountability, paving the way for truly sovereign digital existence.

3 Technical Architecture

The BUBIWOT ecosystem is composed of four primary, interconnected entities:

1. **User Session:** Users generate ephemeral keys on new devices. Initially, this grants limited account access, prompting the need for IRL attestation to gain full control.
2. **Guardian Peers:** These are trusted participants, selected by the user, who perform mutual key-swaps and cryptographic attestations in person.
3. **Web/P2P Layer:** Utilizing libp2p and the BUBIWOT protocol, this layer is responsible for the efficient batching and routing of attestations, as well as for peer discovery.
4. **Babylon CosmWasm Smart Contract:** This on-chain component functions as the **control plane**, managing cryptographic pre-approvals, account recovery logic, and coordinating with the Bitcoin chain for staking and slashing events.

The interaction between these entities is visualized in Figure 1.

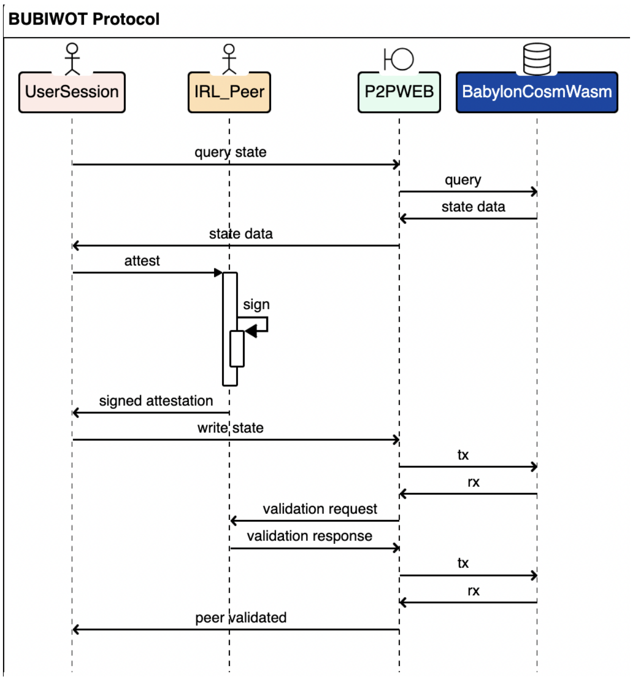

Figure 1: BUBIWOT Protocol Entities and Interactions.

4 Account Recovery Workflow

The account recovery process is designed to be both secure and user-friendly.

4.1 Step 1: Ephemeral Session Initiation

A user initiates the recovery process on a new device. This action generates a temporary session that has partial and limited access to the account's functionalities.

4.2 Step 2: Critical IRL Attestation

To proceed, the user must physically meet with at least one of their designated guardian peers. During this in-person meeting, they securely exchange ephemeral keys. The guardian then cryptographically signs a pre-approval for the account recovery.

4.3 Step 3: p2pweb via libp2p

The guardian's attestation is securely routed through BUBIWOT's decentralized peer-to-peer layer. Attestations are batched to enhance efficiency and reduce transaction costs.

4.4 Step 4: Threshold Verification

The Babylon smart contract verifies the IRL attestation. If the predefined threshold of attestations is met, the contract triggers the full account recovery process.

4.5 Step 5: Finalized Recovery

Upon successful verification, the CosmWasm contract securely restores the user's account keys, reinstating control over their staked Bitcoin and associated token balances.

5 Cryptographic and Economic Foundations

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

- **IRL Web of Trust:** This foundation allows for the secure distribution of shard-based account recovery keys among trusted peers.
- **Babylon Smart Contracts:** These facilitate verifiable identity validation and manage the economic incentives tied to staked Bitcoin.
- **Lightning Network:** This provides for rapid and secure Bitcoin transactions, which are essential for staking rewards and application-layer payments.
- **Strong-form Proof-of-Personhood:** BUBIWOT establishes a robust method for identity validation, a critical component for scalable UBI.

6 Economic Incentives

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

- Users stake Bitcoin via remote staking contracts on the Bitcoin blockchain to participate.
- Guardian attestations are incentivized through rewards in both Bitcoin and the protocol's native token.
- To deter malicious behavior, automated slashing penalties are imposed on guardians who act dishonestly.

7 AGI-Resistant Security

A key design consideration is resilience against future threats, including Artificial General Intelligence (AGI). The protocol employs socio-economic game theory and mandatory IRL attestations to create a security model that is difficult for automated systems to compromise.

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 Bitcoin (BTC), BUBI tokens, and other digital assets, facilitating frictionless transactions and reliable financial inclusion.
- **Secure Communication:** Supports both ephemeral peer-to-peer messaging and durable communications recorded permanently on-chain, enabling immutable data provenance.
- **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.

9 Risk Analysis and Mitigation

BUBIWOT anticipates several potential threats and proactively implements safeguards:

9.1 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. Furthermore, the risk of having their combined Bitcoin stake slashed provides a powerful economic deterrent against collusion.

9.2 Sybil Attacks

Threat: Malicious actors attempt to create numerous fraudulent identities to manipulate UBI distribution.
Mitigation: Mandatory IRL attestations, backed by the economic cost of a Bitcoin stake, impose a practical, real-world barrier against automated mass-account generation.

9.3 Loss of Devices or Keys

Threat: Accidental key loss jeopardizes user accounts and staked funds.
Mitigation: Robust social recovery through trusted IRL peer groups, coupled with threshold cryptography, provides resilient account recovery solutions.

9.4 Malicious Node Behavior

Threat: Nodes in the P2P layer may selectively censor, delay, or alter attestations.
Mitigation: Attestation batching and cryptographic verification mechanisms identify misbehavior. Redundant peer routing and, ultimately, timestamping state onto Bitcoin via Babylon ensures message reliability and censorship resistance.

10 Tokenomics and Distribution

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

- **Total Supply and Emission:** A clearly defined total supply with controlled emission rates aligned with protocol adoption metrics.
- **Initial Distribution:** Tokens are earned primarily through verified IRL attestations, rewarding users for onboarding authentic peers.
- **Incentives and Penalties:** Guardians and validators earn tokens for truthful participation, while dishonest behavior is disincentivized through slashing mechanisms tied to staked Bitcoin collateral.
- **Token Utility and Demand:** Tokens function as transactional mediums, staking assets, and reputation markers, thus maintaining inherent utility.

11 Conclusion

The BUBIWOT protocol establishes an innovative and decentralized framework for identity management. By leveraging the security of the Bitcoin network through remote staking, 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.