The VibeSwap Wallet Recovery Standard

A Human-Centered Approach to Never Losing Your Crypto

Version 1.0 | February 2024

Executive Summary

Every year, billions of dollars in cryptocurrency are lost forever because someone forgot a password, lost a piece of paper, or passed away without sharing access. This doesn't have to happen.

The VibeSwap Wallet Recovery Standard introduces a new way to protect your digital assets—one that works the way humans actually live. Instead of relying solely on a 24-word phrase written on paper, you can now recover your wallet through trusted friends and family, time-delayed security measures, and even a "digital will" that activates if you're gone.

Most importantly, this system is designed to resist sophisticated attacks—including those that might come from advanced AI systems in the future.

The Problem We're Solving

The Current State of Crypto Security

Today, most cryptocurrency wallets work like this:

1. You create a wallet
2. You receive a "seed phrase" (12-24 random words)
3. You're told to write it down and never lose it
4. If you lose it, your money is gone forever

This approach has failed millions of people:

- **$140 billion** in Bitcoin alone is estimated to be permanently lost
- **20%** of all Bitcoin has never moved and is likely inaccessible
- Countless families have lost inheritances because a loved one passed away
- Hardware failures, house fires, and theft destroy backup phrases daily

Why Traditional Backups Fail

Method	What Goes Wrong
Paper backup	Fire, flood, theft, forgetting location
Metal plate	Still can be lost or stolen
Password manager	Forget master password, company shuts down
Give to family	They lose it, or relationship changes
Bank safety deposit	You die, family can't access

The fundamental problem: We're asking humans to be perfect at something humans are bad at—never losing a piece of information over decades.

Our Solution: Recovery That Works Like Life

The Core Idea

Instead of one backup method, we provide **five different ways** to recover your wallet. If one fails, others remain. Together, they create a safety net that catches you no matter how you fall.

Think of it like having:

- A spare key with your neighbor
- A locksmith who can help (but takes a week)
- A family member who inherits if you're gone
- A court system for disputes
- An unbreakable backup in a vault

The Five Recovery Methods

1. Guardian Recovery: Your Trusted Circle

What it is: Choose 3-10 people you trust. If you lose access, any 3 of them (for example) can help you recover.

How it works:

```
You add guardians:
├── Mom
├── Brother
├── Best friend
├── Lawyer
└── Colleague

If you lose access:
1. Your brother contacts your mom and best friend
2. All three approve your new wallet address
3. You wait 24 hours (in case of fraud)
4. Your identity transfers to your new wallet
```

Why it's safe: An attacker would need to convince 3 of your trusted people to betray you. If your guardians are spread across different parts of your life (family, friends, professional), this is nearly impossible.

Real-world analogy: It's like needing 3 out of 5 family members to agree before accessing a shared family safe.

---

2. Time-Lock Recovery: The Waiting Game

What it is: Anyone can try to claim your wallet, but they have to wait 7-30 days while you're notified through every possible channel.

How it works:

```
Someone claims your wallet:

Day 0: They post a 1 ETH "security deposit"
       You receive notifications:
       - Email
       - Text message
       - App notification
       - On-chain alert

Day 1-7: Waiting period
         You can cancel at any time
         (Their deposit goes to you as compensation)

Day 8: If you haven't cancelled, recovery completes
       They get their deposit back
```

Why it's safe:

- Attackers risk losing 1 ETH (~$2,500+) if you notice
- You have a full week to respond through any channel
- Even if you're traveling or busy, you'll likely see one notification

Real-world analogy: It's like someone filing to transfer your house deed, but you have 30 days and multiple mail/email notifications to object.

---

3. Dead Man's Switch: Your Digital Will

What it is: If your wallet is inactive for one year, a person you've chosen (your "beneficiary") can claim it.

How it works:

```
You set up the switch:
├── Timeout: 1 year
└── Beneficiary: Your spouse

Life continues normally:
├── Every transaction resets the timer
├── Every login resets the timer
└── You can manually reset anytime

If something happens to you:
├── 30 days before: Warning notifications
├── 7 days before: Urgent notifications
├── 1 day before: Final warning
└── Day 365: Beneficiary can claim
```

Why it's safe:

- Only activates after extended inactivity
- Multiple warnings give you chances to reset
- You choose who inherits (spouse, child, charity)

Real-world analogy: It's like a will that automatically activates, but with a year of waiting and multiple warnings.

---

4. Arbitration: The Crypto Court

What it is: A panel of neutral jurors reviews your evidence and decides if you're the real owner.

How it works:

```
You lost everything but can prove ownership:

1. You submit evidence:
   ├── Photo ID (encrypted)
   ├── Video of yourself
   ├── Transaction history you remember
   └── Social media proof

2. Five random jurors are selected
   (They've staked money to be fair)

3. Jurors review for 7 days

4. Majority vote decides outcome:
   ├── Approved: You get access
   └── Denied: You lose your deposit
```

Why it's safe:

- Jurors have money at stake (they lose it if they vote unfairly)
- Multiple jurors prevent single points of corruption
- Evidence requirements make fraud difficult

Real-world analogy: It's like a small claims court, but faster and online.

---

5. Quantum Backup: The Unbreakable Vault

What it is: A special type of backup key that even future quantum computers can't break.

How it works:

```
When you set up your wallet:

1. Your computer generates special "quantum-proof" keys
2. You print them or store on a USB drive
3. These keys are registered with your wallet

If you need to recover:

1. You retrieve your printed/stored keys
2. You sign a recovery request
3. Recovery happens immediately
```

Why it's safe:

- Uses math that quantum computers can't break
- Works even if normal encryption becomes obsolete
- Immediate recovery (no waiting period needed)

Real-world analogy: It's like a master key made of an unbreakable material.

Protection Against AI Attacks

Why This Matters

As artificial intelligence becomes more powerful, we need to prepare for a world where AI could:

- Generate fake video calls pretending to be you
- Impersonate you in emails and messages
- Coordinate sophisticated fraud at scale
- Find vulnerabilities humans would miss

We've designed our recovery system to resist even these advanced threats.

Our Seven Layers of AI Defense

Layer 1: History Can't Be Faked

The problem AI faces: An AI might create a convincing fake identity today, but it can't create years of transaction history retroactively.

How we use this:

- We track how long your wallet has existed
- We analyze your transaction patterns over time
- New accounts (under 30 days) have restrictions
- Your "behavioral score" increases with time

Example: An AI creates a fake account to steal your wallet. But your real account has 3 years of history and 500 transactions. The fake has none. Recovery denied.

Layer 2: Time Is On Your Side

The problem AI faces: AI can act fast, but legitimate owners have time to notice and respond.

How we use this:

- Every recovery has a mandatory 24-hour delay
- Time-lock recovery adds 7+ more days
- Notifications go to every channel you've registered

- You can cancel from any channel

Example: An AI initiates recovery at 3 AM hoping you won't notice. You get a text, an email, and an app notification. You cancel from your phone. AI's deposit is now yours.

Layer 3: Money Talks

The problem AI faces: Attacking at scale costs real money.

How we use this:

- Every recovery attempt requires a 1 ETH deposit (~$2,500+)
- Failed/fraudulent attempts lose the deposit
- This makes mass attacks economically unfeasible

Example: An AI wants to attack 1,000 wallets. It would need $2.5 million in deposits. If even half are caught, it loses $1.25 million. Not profitable.

Layer 4: Rate Limits

The problem AI faces: AI can try millions of times, but we don't let it.

How we use this:

- Maximum 3 recovery attempts per address
- 7-day cooldown between attempts
- Permanent ban after fraud report

Example: An AI tries to recover your wallet and fails. It must wait 7 days. After 3 failures, that AI-controlled address can never try again.

Layer 5: Physical World Anchors

The problem AI faces: AI exists in the digital world, but recovery can require physical proof.

How we use this:

- Register a hardware security key (YubiKey, Ledger)
- Video verification with random prompts ("hold up 3 fingers and say today's date")
- Physical mail with recovery codes

Example: An AI deepfakes your face on video. But when asked to hold up a specific number of fingers while saying a randomly generated phrase, it fails because it can't predict the prompt.

Layer 6: Your Social Network

The problem AI faces: AI might impersonate you, but convincing your real friends and family is harder.

How we use this:

- Guardians should be people who know you personally
- We encourage video call verification between guardians
- Your "social graph" (who you transact with) is analyzed

Example: An AI convinces one guardian. But your mom, your brother, and your best friend all need to approve. They call each other and realize something's wrong. Recovery blocked.

Layer 7: Pattern Detection

The problem AI faces: AI often acts in ways that are subtly inhuman.

How we use this:

- We detect suspiciously perfect timing (machines use round numbers)
- We flag unusual patterns (requests at strange hours, rapid retries)
- We compare behavior to your historical patterns

Example: An AI submits a recovery request at exactly 12:00:00.000 (a perfectly round timestamp). Humans almost never do this. Flagged as suspicious.

Getting Started

For Users: Setting Up Your Safety Net

Step 1: Add Guardians (10 minutes)

```
Choose 3-5 people:
☐ Someone from your family
☐ Someone from your friend group
☐ Someone professional (lawyer, accountant)
☐ Someone in a different country (optional)
☐ Someone tech-savvy who can help others
```

Step 2: Set Up Dead Man's Switch (2 minutes)

```
☐ Choose your beneficiary
☐ Set timeout (1 year recommended)
☐ Make sure your beneficiary knows about this
```

Step 3: Register Hardware Key (5 minutes)

```
☐ Get a YubiKey or similar device
☐ Register it with your wallet
☐ Store in a safe place
```

Step 4: Enable Notifications (3 minutes)

```
☐ Verify your email
☐ Add your phone number
☐ Enable push notifications
☐ (Optional) Add Telegram/Discord
```

Step 5: Generate Quantum Backup (5 minutes)

```
☐ Generate quantum-resistant keys
☐ Print or save to USB
☐ Store in fireproof safe or safety deposit box
```

For Developers: Integration Guide

```
// Install the SDK
npm install @vibeswap/recovery

// Initialize
import { RecoveryClient } from '@vibeswap/recovery'
const recovery = new RecoveryClient({ provider })

// Add a guardian
await recovery.addGuardian({
  address: '0x...',
  label: 'Mom',
  verificationMethod: 'video_call'
})

// Check recovery eligibility
const { allowed, reason } = await recovery.canAttemptRecovery()

// Initiate recovery (requires bond)
await recovery.initiateTimelockRecovery({
  lostAddress: '0x_old',
  newAddress: '0x_new',
  bond: ethers.parseEther('1')
})
```

Frequently Asked Questions

General Questions

Q: What if I lose my phone and can't receive notifications?

A: That's why we use multiple channels. If you've set up email, SMS, and push notifications, losing one device doesn't prevent you from seeing alerts. You can cancel recovery from any device where you can access any of these channels.

Q: What if all my guardians lose their wallets too?

A: Each guardian should set up their own recovery options. The beauty of the system is that it's recursive—your guardians can recover their wallets, then help you. We recommend having at least one guardian who uses different custody methods than you.

Q: Can I change my guardians?

A: Yes, anytime. You can add or remove guardians whenever you want. Changes take effect immediately. We recommend reviewing your guardians once a year, like updating emergency contacts.

Q: What happens to my NFTs and tokens during recovery?

A: Recovery transfers your identity (your soulbound NFT) to your new address. Your other assets remain at your old address. After recovery, you can transfer them to your new address using your restored access.

Security Questions

Q: What if someone forces me to approve a recovery?

A: Consider adding a "duress guardian"—someone who knows to deny any request if you're under pressure. You can also set up a secret signal with your guardians (e.g., a specific word that means "deny everything").

Q: What if an attacker gains access to my email AND phone?

A: This is why we require multiple guardians or a waiting period. Even if an attacker compromises your notifications, the 7-day waiting period for timelock recovery gives you time to notice through other means (checking your wallet, friends mentioning it, etc.).

Q: Is the arbitration system really fair?

A: Jurors stake their own money. If they vote dishonestly (against the majority), they lose their stake. This creates strong incentives for honest evaluation. Additionally, jurors are randomly selected, preventing coordination.

Technical Questions

Q: How is this different from a regular multisig?

A: A multisig requires multiple parties to approve every transaction. Our system only involves guardians for recovery—your day-to-day transactions work normally with just your wallet. It's security when you need it, freedom when you don't.

Q: What if VibeSwap goes out of business?

A: The recovery contracts are deployed on-chain and are immutable. They'll continue working as long as Ethereum exists. No company, including VibeSwap, can modify or shut them down.

Q: Can I use this for any wallet?

A: Currently, this system works with VibeSwap identities (soulbound NFTs). We're working on standards that could apply to any smart contract wallet.

The Future of Wallet Security

We believe wallet recovery should be:

1. **Human-centered**: Working with how people actually live, not against it
2. **Layered**: Multiple backup options so no single failure is catastrophic
3. **Social**: Leveraging trusted relationships, not just technology
4. **Resistant**: Prepared for threats that don't exist yet (including advanced AI)
5. **Accessible**: Understandable by anyone, not just crypto experts

This is version 1.0 of our standard. As technology evolves and we learn from real-world usage, we'll continue improving. Our goal is a world where losing access to your digital assets is as rare as losing access to your bank account—possible, but with multiple safety nets to catch you.

Glossary

Term	Definition
Guardian	A trusted person who can help recover your wallet
Timelock	A waiting period before recovery can complete
Dead Man's Switch	Automatic recovery after prolonged inactivity
Arbitration	A jury-based dispute resolution system
Bond	Money deposited as collateral for recovery attempts
Soulbound	A token that can't be transferred (tied to your identity)
Seed Phrase	The traditional 12-24 word backup for crypto wallets
Quantum-Resistant	Encryption that future quantum computers can't break
Behavioral Score	A measure of your wallet's historical legitimacy

---

Conclusion

You shouldn't have to be perfect to keep your money safe. The VibeSwap Wallet Recovery Standard acknowledges that humans forget, lose things, and eventually pass away—and builds a system that handles all of these gracefully.

With five recovery methods, seven AI-resistance layers, and a focus on human relationships over technical perfection, we're building a future where "not your keys, not your coins" doesn't mean "lose your keys, lose everything."

Your crypto. Your people. Your safety net.

This whitepaper describes the VibeSwap Wallet Recovery Standard version 1.0. For technical implementation details, see the accompanying technical documentation. For the latest updates, visit our GitHub repository.