Wallet Governance, Policy and Key Management Study Report

bg in

blockchain governance initiative network

The Global Network for Blockchain Stakeholders™

This study is a work product of IAM, Key Management and Privacy Working Group of BGIN.

©2025 BGIN (Blockchain Governance Initiative Network) is registered as BN Association, a Japanese general association with its principal place of business at Shiba Building, 704, 4-7-6, Shiba, Minato-ku, Tokyo. All right reserved

© BGIN – All rights reserved

Executive Summary

The convergence of blockchain technology, digital identity, and decentralized governance has fundamentally transformed the role of digital wallets in our technological infrastructure. What began as simple cryptocurrency storage solutions have evolved into sophisticated platforms that manage financial assets, govern protocol decisions, and secure digital identities. This evolution brings both opportunities and challenges, as wallet systems become critical interfaces for participating in the decentralized digital economy.

This study report, produced by the IAM, Key Management and Privacy Working Group of BGIN (Blockchain Governance Initiative Network), examines the complex landscape of wallet governance, policy, and key management. The increasing centrality of wallets in digital interactions demands a thorough understanding of their security implications, implementation requirements, and regulatory considerations—crucial knowledge for all stakeholders in the digital ecosystem.

The evolution of "wallets" encompasses a broad spectrum of implementations, each with varying degrees of sophistication and security characteristics. We observe a progressive relationship between wallet complexity and the range of interactions they enable in blockchain ecosystems:

1. Financial transactions represent the original and most common wallet application, with established patterns for key management and security
2. Governance and reputation-based systems are increasingly integrated into wallet functionality, enabling participation in decentralized decision-making
3. Identity management is emerging as a critical wallet function, with implications for privacy, data control, and cross-chain interoperability

The report analyzes digital wallets across their complete lifecycle, from creation through decommissioning, providing a taxonomic framework for understanding different wallet types—from custodial and non-custodial to hardware, software, biometric, and smart contract implementations. Through examination of real-world security incidents and implementation challenges, we identify best practices and potential standardization opportunities, while analyzing respective security models, governance implications, and implementation trade-offs.

Throughout our analysis, we emphasize the critical balance between security, usability, and privacy. The convergence of financial, governance, and identity functions within single wallet interfaces introduces new security challenges and regulatory considerations. This convergence is accelerating as technologies like zero-knowledge

© BGIN – All rights reserved

proofs, account abstraction, and biometric binding enable more versatile and user-friendly implementations, but they require sophisticated approaches to security, privacy, and regulatory compliance.

By providing comprehensive insights into best practices, security frameworks, and emerging technologies, this report aims to establish a foundation for responsible wallet implementation and governance. Our goal is to equip stakeholders with the knowledge needed to navigate the complexities of wallet systems while maintaining the highest standards of security and user protection. As wallets increasingly serve as gateways to digital economies and decentralized societies, their proper implementation becomes essential for building trust in these systems while maintaining the sovereignty and privacy that underpin their value proposition.

The transformative potential of well-governed wallet systems comes with significant responsibilities. This report provides a framework for understanding and addressing these responsibilities while fostering innovation in wallet technology that balances security, usability, and privacy—ensuring that the convergence of wallet technologies ultimately empowers users and builds a more inclusive digital economy.

© BGIN – All rights reserved

Disclaimer: The views expressed in the document are personal views of the participating members of the BGIN community and should not be seen as the official views or recommendations of the institutions with which they are affiliated.

The technology described in this document was made available from contributions from various sources, including members of the BGIN and others. Although the BGIN has taken steps to help ensure that the technology is available for distribution, it takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any independent effort to identify any such rights. BGIN and the contributors to this document make no (and hereby expressly disclaim any) warranties (express, implied, or otherwise), including implied warranties of merchantability, non-infringement, fitness for a particular purpose, or title, related to this document, and the entire risk as to implementing this document is assumed by the implementer. The BGIN Intellectual Property Rights policy requires contributors to offer a patent promise not to assert certain patent claims against other contributors and against implementers. BGIN invites any interested party to bring to its attention any copyrights, patents, patent applications, or other proprietary rights that may cover technology that may be required to practice this document.

© BGIN – All rights reserved

Table of contents

© BGIN – All rights reserved

© BGIN – All rights reserved

© BGIN – All rights reserved

© BGIN – All rights reserved

1. Scope

This study report examines the governance, policy frameworks, and key management considerations for digital wallets across financial, identity, and decentralized systems. The scope encompasses the full lifecycle of wallet implementation, from creation through decommissioning, with particular focus on security, privacy, and regulatory compliance.

Intended Audience

This document is designed for:

- Developers implementing wallet technologies
- Businesses integrating wallet solutions
- Regulatory bodies overseeing digital assets and identity systems
- Academic institutions researching blockchain technology
- Security professionals evaluating wallet implementations
- Policy makers developing regulatory frameworks
- Industry practitioners seeking implementation guidance

Objectives

The paper aims to:

1. Analyze current challenges in wallet governance across different implementation types
2. Examine relationships between wallet sophistication and use case optimization
3. Provide implementation recommendations for various wallet applications
4. Address security and regulatory considerations for wallet lifecycle management
5. Explore convergence between financial, identity, and governance functions

Coverage

The study specifically addresses:

- Wallet types and their governance requirements
- Security frameworks and implementation standards
- Key management practices and protocols
- Regulatory compliance considerations
- Identity management integration
- Emerging technologies and future developments

© BGIN – All rights reserved

This comprehensive examination provides stakeholders with frameworks for understanding and implementing effective wallet governance strategies while maintaining security, privacy, and regulatory compliance.

2. Normative Reference

Terms and Definitions

The following terms and definitions are used in this document, with core definitions sourced from ISO and IEC terminology databases and supplemented with domain-specific references.

Core Wallet and Identity Terms

Wallet: application or mechanism used to generate, manage, store or use private keys and public keys or other digital assets. A wallet can be implemented in software, implemented as a hardware module, or written onto non-digital media such as paper or metal. Digital assets stored in wallets can include, for example, *non-fungible* tokens.

. [ISO 22739:2024]

Digital Asset: Asset that exists only in digital form or that is the digital representation of another asset. [ISO 22739:2024]

Decentralized Identifier (DID): Identifier that is issued or managed in a decentralized system and designed to be unique within a context. [ISO 22739:2024]

Identity: Set of attributes that distinguishes an entity in a context. [ISO 22739:2024]

Self-Sovereign Identity (SSI): Identity that is solely controlled by the entity that the identity distinguishes. [ISO 22739:2024]

Blockchain and DLT Terms

Distributed ledger: ledger that is shared across a set of distributed ledger technology nodes and synchronized between the DLT nodes using a consensus mechanism [ISO 22739:2024]

Blockchain: Distributed ledger with confirmed blocks organized in an append-only, sequential chain using hash links. [ISO 22739:2024]

© BGIN – All rights reserved

Smart Contract: Computer program stored in a distributed ledger technology system wherein the outcome of any execution of the program is recorded on the distributed ledger. [ISO 22739:2024]

Token: Asset that represents a collection of entitlements. [ISO 22739:2024]

Security and Cryptographic Terms

Private Key: Key of an entity's asymmetric key pair that is kept secret and that should only be used by that entity. [ISO/IEC 9798-1:2010]

Public Key: Key of an entity's asymmetric key pair that can be made public. [ISO/IEC 9798-1:2010]

Digital Signature: Data which, when appended to data to be signed, enable the user of the data to authenticate their origin and integrity. [ISO 14641:2018]

Additional References

Standards and Specifications

1. ISO/IEC 27001:2013 - Information security management systems
2. W3C Decentralized Identifiers (DIDs) v1.0
3. W3C Verifiable Credentials Data Model v1.1
4. FIDO Alliance Specifications
5. NIST Digital Identity Guidelines (SP 800-63-3)

Academic and Industry Sources

1. Buterin, V., Weyl, E.G., & Ohlhaver, P. (2022). "Decentralized Society: Finding Web3's Soul"
2. Antonopoulos, A. M. (2017). "Mastering Bitcoin: Programming the Open Blockchain"
3. Allen, C., et al. (2016). "The Path to Self-Sovereign Identity"

Technical Documentation

1. EIP-4337: Account Abstraction
2. BIP-39: Mnemonic code for generating deterministic keys
3. ERC-721: Non-Fungible Token Standard
4. DIDComm Messaging Specification

© BGIN – All rights reserved

Regulatory References

1. GDPR (General Data Protection Regulation)
2. eIDAS Regulation (EU) No 910/2014
3. FATF Recommendations on Virtual Assets
4. ISO/IEC 27701:2019 Privacy Information Management

Implementation Guidelines

1. OWASP Security Guidelines for Cryptographic Implementations
2. NIST Cryptographic Standards and Guidelines
3. Common Criteria Protection Profiles for Secure Elements
4. EMVCo Security Evaluation Process

4. Abbreviations and Symbols

In this document, the following abbreviations and symbols are used.

5. Current Problems and Risks

The rapidly evolving landscape of digital wallets, blockchain technology, and cryptocurrency has brought with it a myriad of challenges and risks. As these technologies become more integrated into our financial, governance, and identity systems, the stakes for proper management and security continue to rise. This section highlights several notable instances that underscore the potential risks involved in digital wallets.

These cases span a wide range of issues, from direct security breaches and hacks to more subtle problems involving smart contract vulnerabilities, key management failures, and governance shortcomings. By examining these real-world examples, we can gain valuable insights into the complexities and potential pitfalls of digital wallet systems. These instances not only illustrate the current state of risks in the field but also serve as crucial learning opportunities for improving the security, reliability, and functionality of digital wallets moving forward.

From multi-million dollar hacks to governance failures and user-facing scams, these examples demonstrate the diverse array of challenges faced by wallet providers, blockchain developers, and users alike. They highlight the critical need for robust security measures, clear and well-implemented policies, and ongoing education and vigilance in the face of evolving threats. As we delve into these cases, it becomes clear

© BGIN – All rights reserved

that the future of digital wallet technology depends on our ability to learn from past incidents and proactively address potential vulnerabilities.

The Bybit Triple-Tier Attack: A Case Study in Modern Wallet Vulnerabilities

In 2024, a sophisticated attack targeting Bybit revealed alarming vulnerabilities in multi-layered wallet security frameworks. The incident resulted in substantial losses across multiple cryptocurrency networks and demonstrated how advanced threat actors can simultaneously exploit social engineering, signature phishing, and smart contract manipulation.

Key aspects of the breach:

- The attackers compromised Safe Wallet's AWS infrastructure through sophisticated social engineering
- Malicious code was injected into Safe's web interface, deceiving users into signing fraudulent transactions
- Trojan smart contracts were deployed, enabling asset drainage without triggering security alarms
- The attack bypassed hardware wallets, multi-signature requirements, and standard security protocols

Security implications:

1. Blind Signing Vulnerabilities: The incident exposed how hardware wallets displaying only generic contract interactions remain vulnerable to deception attacks
2. Interface Trust: The compromise of trusted interfaces revealed critical weaknesses in the human-technology verification process
3. Multi-Layer Exploitation: The attack demonstrated how vulnerabilities across people, processes, and technology can be exploited simultaneously
4. Recovery Response Gap: A troubling divergence emerged between centralized entities (which responded quickly) and decentralized protocols (which struggled with philosophical and technical barriers to blocking illicit funds)

This case underscores the urgent need for standardized wallet governance frameworks addressing not just blockchain-specific vulnerabilities but the complex interplay between human, technical, and procedural security layers that sophisticated attackers target.

The result of this was 1.5 billion of stolen funds by a DPRK.

© BGIN – All rights reserved

Wallet Hacks

- Parity Wallet Hack (2017): An unidentified hacker managed to exploit a vulnerability in the Parity multi-sig wallet on the Ethereum network, stealing approximately 153,000 ETH, equivalent to $30 million at the time.

Custodial Wallet Hack

In January 2024, Wirex, a UK-based digital payment platform and custodial wallet provider, experienced a significant security breach. The incident resulted in unauthorized withdrawals from its hot wallets, with initial estimates suggesting losses of approximately $8.1 million in various cryptocurrencies including USDT, USDC, ETH, BTC, and MATIC.

Key aspects of the breach:

- The attack occurred through compromised private keys of Wirex's hot wallets
- Multiple blockchain networks were affected including Ethereum, Polygon, and Bitcoin
- Wirex temporarily suspended all cryptocurrency withdrawals to prevent further losses
- The company committed to fully reimbursing affected users

Security implications:

Hot Wallet Vulnerabilities: The incident highlighted risks associated with maintaining large balances in hot wallets for custodial services

Key Management: The compromise of private keys emphasized the critical importance of robust key management systems

Multi-Chain Risk: The attack demonstrated how vulnerabilities can impact multiple blockchain networks simultaneously in integrated wallet systems

Smart Contract Governance Failures

- The DAO Attack (2016): This case involved a governance failure where a user exploited a loophole in The DAO (Decentralized Autonomous Organization) smart contract, draining about 3.6 million ETH, equivalent to $50 million at the time.

© BGIN – All rights reserved

Bridge Exploits

- Poly Network Exploit (2021): In what's been dubbed the largest DeFi hack, a hacker exploited a vulnerability in the Poly Network interoperability protocol, stealing over $600 million in various cryptocurrencies. The event highlighted the potential risks inherent in cross-chain bridges.

Key Management Blunders

- QuadrigaCX Case (2019): The Canadian crypto exchange's CEO died unexpectedly, and he was the only one with access to the cold wallets that stored the firm's and customers' funds. The result was a loss of approximately $190 million in customer funds due to a lack of key management procedures.

Staking Key Recovery Issues

- Staking on Ethereum 2.0: Early participants faced the risk of permanent loss of their staked ETH if their keys were compromised.

Technology Challenges

- Mt. Gox Hack (2014): The now-infamous Bitcoin exchange hack, where 740,000 Bitcoin was stolen due to technology failure and lax security practices.

Governance Risks in Blockchain Governance

- YAM Finance Bug (2020): A coding error in a governance contract led to a bug that made it impossible for governance decisions to be executed, leading to the project's collapse.

Smart Contract Scams

- Uniswap Free Token Scams (2020): Fake websites and scam smart contracts were created, promising free tokens. Users were tricked into approving contracts that drained their wallets. Uniswap is a decentralised exchange, of which launched its token airdropping all existing users.

Key Phishing

- Electrum Wallet Attack (2018): Hackers launched a phishing attack against users of the Bitcoin wallet Electrum, stealing nearly 250 BTC. The attack involved creating fake versions of the wallet that stole users' private keys.

© BGIN – All rights reserved

Security

- Bitfinex Hack (2016): A significant security breach led to the theft of nearly 120,000 Bitcoin. Despite the use of multi-signature wallets, the hackers managed to circumvent security measures.

Terminology and Definitional Challenges

- Confusion over Wallet Definitions: There has been ongoing debate and confusion over the definition of "custodial" vs. "non-custodial" wallets, "hot" vs. "cold" wallets, and how these definitions impact the security and control over one's crypto assets.

6. Types of digital wallets

Introduction to Wallet Taxonomy

The evolution of digital wallets has expanded far beyond their original cryptocurrency-based implementations. As noted in the OpenWallet Foundation's Reference Architecture Whitepaper (2023), wallet technologies are converging across different domains, with a progression from physical wallets to sophisticated multi-purpose digital solutions. The whitepaper identifies this evolution through distinct stages: physical wallets (for in-person transactions only), mobile wallets (for payments, boarding passes, tickets), single-purpose digital wallets (for specific functionalities), and ultimately multi-purpose universal wallets that integrate identity, objects, and money in unified systems.

This convergence necessitates a comprehensive taxonomy of wallet types that considers both technical implementation and functional capabilities. The OpenWallet Foundation describes the ideal future state as one where "multi-purpose digital wallets provide users with the ability to carry their digital identity credentials, payment credentials, and digital objects across boundaries, ecosystems, and physical and digital environments." This vision aligns with our classification approach, which examines wallets across multiple dimensions including policy mechanism, security implementation, and control methodology.

Within this broader ecosystem of universal wallets, blockchain wallets represent a critical subset that has pioneered innovative approaches to key management, security,

© BGIN – All rights reserved

and user sovereignty. While the OpenWallet Foundation architecture presents a technology-agnostic framework for wallet interoperability, blockchain wallets have developed distinct implementations to address the unique security requirements of decentralized systems. These blockchain-specific solutions—particularly in areas like non-custodial control, multi-signature authorization, and secure key recovery—offer valuable insights that can inform the development of universal wallet standards. As noted in the OWF whitepaper, "Where we want to get to is a place where we have multi-purpose digital wallets," and the security models pioneered in blockchain environments will likely play a significant role in shaping these future universal implementations.

Our focus on blockchain wallet types acknowledges both their current practical importance and their influence on emerging wallet architectures.

While the OpenWallet Foundation architecture provides an excellent comprehensive framework for universal wallets encompassing channels, policy engines, interfaces, digital items, storage, communication, and networks, the Blockchain Governance Initiative Network (BGIN) focuses specifically on blockchain wallet implementations and their unique governance considerations. Our taxonomy examines the implementation variations currently deployed in blockchain ecosystems, with particular attention to decentralized control, cryptographic security, and on-chain governance mechanisms. It is worth noting that as wallet technologies continue to converge, the distinctions between blockchain-specific wallets and broader digital wallet implementations may diminish, with technology-agnostic approaches becoming increasingly important. The BGIN's work complements the broader OWF framework by providing specialized guidance for blockchain-specific contexts while recognizing the value of cross-domain wallet standardization efforts.

Blockchain Wallets

A blockchain wallet is a tool for securely storing and sending/receiving cryptocurrency and NFTs. Digital signatures are used to prove the authenticity of asset transactions and other operations. The user's verification key functions as a wallet address and is linked to assets like an account number. On the other hand, the signing key functions like a password, proving ownership of the assets and is used when performing transactions such as sending assets. Loss or leakage of the signing key can lead to permanent loss of assets, so key management is a common challenge for wallets. According to the definition in ISO 22379:2024, wallets are supposed to manage not only signing keys but also verification keys, digital assets, NFTs, etc., but in this section, we focus only on the

© BGIN – All rights reserved

method of storing signing keys for the reasons mentioned above.
This section begins with an overview of digital signatures and outlining the key management issues for wallets. We then list representative forms of wallets and organize them mainly from the key management perspective. In general, there is a trade-off between security and convenience, so an appropriate combination of wallet forms should be selected according to the required security level and use case.

Digital Signatures

Digital signatures are used to prove the authenticity of cryptocurrency transactions. Digital signatures are a type of public-key cryptography that can be used to verify the sender of a document and that the contents have not been tampered with. During key generation, a pair of keys is generated, consisting of a signing key and a verification key. The signing key is kept private by the owner, while the verification key is registered as a public key. The sender uses the signing key to sign the document and sends them. The receiver can mathematically verify that the signature was generated using the signing key associated with the sender's verification key, thereby verifying the validity of the signature-document pair.
In cryptology, security is defined in terms of two aspects: the level at which signatures can be forged and the ability of the attacker. The ideal security ensures that even highly capable attackers cannot forge a document within a practical timeframe. Signature schemes widely used in blockchain such as ECDSA and EdDSA are mathematically proven to satisfy the desired level of security under certain mathematical assumptions.

Key Management Issues

Digital signatures are based on the premise that only the signer knows the signing key that corresponds to a particular verification key. If this assumption is violated through key exposure, the security of the entire system is undermined. Therefore, depending on how the signing keys are managed, security may be lower than cryptological security. Security is determined by taking into account all factors, including which entity manages the keys, in which medium, and how key access control is performed.
In addition, there are cases where keys become inaccessible due to loss or damage of the device, or termination of service by the provider, as illustrated in Subclause 6.4. Digital signatures are based on the premise that the signer possesses the signing key. In such situations, temporary or permanent loss of access to assets can occur, making availability a critical element of key management. Leakage of keys or loss of access in wallets can lead to permanent loss of assets, making proper key management

© BGIN – All rights reserved

essential. Thus, in addition to cryptographic security, ensuring operational security and availability becomes a key consideration in key management.

Wallet Policy mechanisms

Software Wallet

This is a type of wallet that manages signing keys on a computer. It can take the form of desktop applications, browser extensions or mobile applications for smartphones. The term "software wallet" is often used to refer to non-custodial wallets that store signing keys in software, but as mentioned in 7.2.3.1, it is not limited to non-custodial wallets.This type of wallet requires no special hardware and is convenient to use.

Security is highly dependent on the key management method and the level of access control. Physical risks include theft of the computer or mobile device, which could lead to signing key leakage. There are also risks of malware, keyloggers or user error compromising the signing key due to application vulnerabilities.

There are several potential single points of failure. If the wallet application provider ceases service, the wallet may become unusable. The reliance on internet connectivity means that communication disruptions can render the wallet inaccessible. In addition, loss or damage to the storage medium containing the signing key, such as a mobile device, can render the wallet unusable. Some software wallets can synchronize keys between smartphone and desktop applications using QR codes or cloud services, which improves availability.

Hardware Wallet

This is a type of wallet that stores the signing keys on a dedicated, robust physical device.It is less convenient in that it requires a dedicated device, but it is suitable for long-term storage and management of large quantities of assets.

There is still a physical risk of the dedicated device being stolen and the private keys being misused. However, because the dedicated device is isolated from Internet-connected computers, the risk of malware infection is greatly reduced. Hardware wallets are generally considered more secure than software wallets, but the devices can be tampered with during the manufacturing and distribution process. Users need to trust the vendor about the integrity of the product.

© BGIN – All rights reserved

There is a single point of failure. If the dedicated device fails or is lost, access to private keys is lost. Unlike software wallets, the rugged design of hardware wallets makes them more resistant to damage from water or other elements. It is suitable for long-term storage and management of large asset holdings.

Implementation Security Framework

Security considerations vary significantly across different wallet implementations.
Implementation Security Framework

Wallet Type	**Security Considerations**	**Threat Vectors**	**Mitigations**	**Standards/Compliance**
Software Wallets	- Application security -Storage protection -Network security	- Malware injection -Memory attacks -Man-in-the-middle	- Code signing -Secure enclaves - TLS/SSL	- OWASP guidelines - ISO 27001 - NIST standards
Hardware Wallets	- Physical security -Side-channel protection -Firmware security	- Physical tampering -Power analysis -Firmware manipulation	-Secure elements -Anti-tampering -Secure boot	- Common Criteria - FIPS 140-2 - EMVCo
Smart Contract Wallets	-Contract security -Upgrade mechanisms -Access controls	-Contract exploitation -Front-running -Access control bypass	- Formal verification -Time locks -Role-based access	- Smart contract standards - ERC specifications - Audit requirements

© BGIN – All rights reserved

Wallet Control mechanism

Custodial Wallet

This is a type of wallet where the service provider stores the signing keys. The provider's key management methods vary. They may manage the signing keys on online servers, store them on dedicated offline devices, or use cloud HSMs.

Security is highly dependent on the provider's key management methods, user authentication, and the provider's level of authentication for key activation. Online key management carries the risk of hacking. Using a hardware wallet can reduce these risks. User authentication can vary from ID/PW, biometrics and OTP, to a combination of these. Strict measures such as mandatory two-factor authentication are implemented for user authentication. Some keys are activated by user authentication, while others require another level of authentication on the operator's side. However, there is still a risk of the provider misusing the keys. Since the provider has effective control over the assets, users must trust the provider.

There is a single point of failure. If the provider's service is disrupted, users may temporarily lose access to their assets. If appropriate action is not taken before the service is terminated, users risk losing access permanently.
With user keys centralized at the provider, a successful attack could result in massive losses. Typically, in such cases, the provider that controls the assets is responsible for compensating users. To mitigate these risks, and in line with the idea of self-sovereign control over assets, non-custodial wallets have emerged, where users manage their own signing keys.

With user keys centralized at the provider, a successful attack could result in massive losses. Typically, in such cases, the provider that controls the assets is responsible for compensating users. To mitigate these risks, and in line with the idea of self-sovereign control over assets, non-custodial wallets have emerged, where users manage their own signing keys.

Non-custodial Wallet

This is a type of wallet where users manage their own signing keys. Users have various methods for key management. They can store signing keys in applications on their

© BGIN – All rights reserved

devices or on external devices like USB drives.

Security is highly dependent on the user's key management method and level of access control. Hardware wallets may be used to reduce hacking risks. Strict measures like two-factor authentication are implemented for key access control.

There is a single point of failure. Availability varies greatly depending on the user's management method. Loss or damage of the storage medium containing the signing key can result in loss of access to assets. If the user dies without leaving a means of accessing the assets, the assets may be permanently lost.

Multi-sig Wallet

This is a type of wallet where redundancy is introduced to the signing keys, with multiple pairs of signing keys and verification keys associated with a single wallet address. Multiple signing keys are generated, and approval is granted when a threshold number of signatures are collected. Here, we assume that out of n keys distributed for storage, approval is granted when k or more keys provide signatures.
In addition to personal use by a single user, Multi-sig wallets are also used in use cases where multiple individuals or entities share signing authority and jointly authorize it. The management of multiple signing keys can either be distributed between users and custodians or solely distributed by the custodians. For example, multi signatures can be used to reduce the risk of internal fraud in the custodial model. By setting (k, n) appropriately, various operational scenarios can be accommodated. However, the configuration of (k, n) is not flexible. If (k, n) is to be changed by adding or removing managers, a new wallet needs to be created and each manager notified.

Cryptographically, the wallet is secure as long as fewer than k keys are compromised. Setting a higher value for k allows for stricter account management. In addition, since the corresponding signatures for each signing key are recorded in the chain, in the event of an attack, the specific keys that were targeted can be identified.

If $k < n$, the single point of failure problem is solved, and availability increases as k becomes smaller. Setting $k = n$ increases the number of single points of failure. Availability also depends on where the signing key is managed.

In cases where there is a single piece of secret information per wallet address, the entity managing the signing key has effective control over the assets, leading to the classification of custodial and non-custodial wallet types. For Multi-sig wallets, multiple entities manage the secret information, so it is necessary to consider which entity has

© BGIN – All rights reserved

the authority to transfer assets. The authority to transfer assets is determined by how much secret information each entity manages and how much is required for the transfer. Here we classify the authority to transfer assets in the context of a single user Multi-sig wallet. In this case, the entity that manages k or more private keys has the right to transfer assets. There are four possible patterns of asset control:
(1) Only the user can transfer assets, and the assets can be transferred only by the user.
(2) Only the custodian can transfer assets, and the assets can be transferred only by the custodian.
(3) Neither the user nor the custodian can transfer assets individually; asset transfer requires the cooperation of both parties.
(4) Both the user and the service provider can transfer assets independently, without the other party's cooperation.
The transfer authority is granted based on the setting of (k, n) and the number of private keys managed by the user and the service provider, as shown in the Figure X:

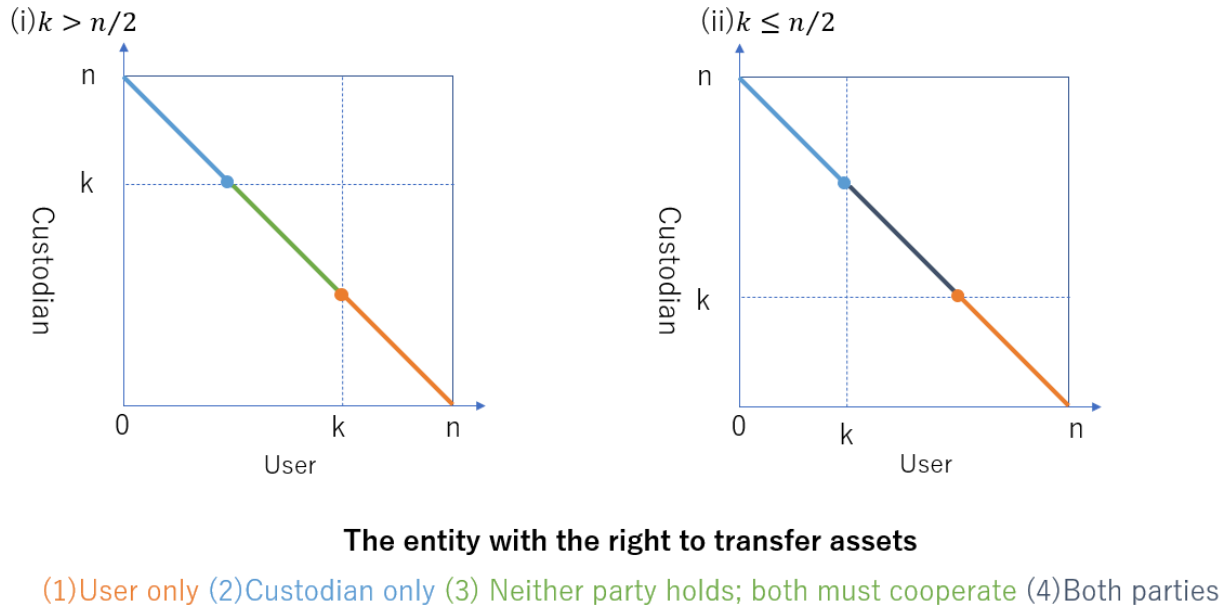

Figure X -The pattern of the entity with the right to transfer assets

- If k > n/2
    - If the user manages k or more keys, it falls under case (1).
    - If both the user and the service provider manage less than k keys, it falls under case (3).
    - If the service provider manages k or more keys, it falls under case (2).

- If k <= n/2

© BGIN – All rights reserved

- If the user manages n-k or more keys, it falls under case (1)
- If both the user and the service provider manage k or more keys, it falls under case (4).
- If the service provider manages n-k or more keys, it falls under case (2)

MPC Wallet

This type of wallet has a single key pair associated with the wallet address, but the shares of that key are held by multiple parties. There are two main methods of generating the key pair and shares. One method is to first generate a key pair and then split the signing key into multiple shares that are distributed to each party. The other method is for multiple parties to generate shares independently and then derive a single verification key corresponding to the set of shares. Signature verification is only successful if a threshold number of shares are used. Unlike Multi-sig wallet, which generates n separate signing keys, in MPC wallet the n independently generated shares correspond to a single signing key. By using k or more of these shares in communication, signatures can be generated without reconstructing the signing key.

In addition to personal use by a single user, MPC wallets are also used in use cases where multiple individuals or entities share signing authority and sign together. They can also be used for distributed key management between the user and a custodian, or distributed management by a service provider alone. By appropriately setting (k, n), different operational scenarios can be accommodated. Unlike Multi-sig wallets, it is easier to change the (k, n) setting.

Similar to Multi-sig wallets, cryptographically, it is secure as long as fewer than k key shares are stolen. By setting k to a larger value, the account can be managed more strictly. Unlike Multi-sig wallets, since the signature generation computation process is performed off-chain, third parties cannot identify which shares were used to generate the signature.

Similar to Multi-sig wallets, when k < n, the single point of failure problem is solved, and availability increases as k becomes smaller. Setting k = n increases the number of single points of failure. Availability also depends on where the key share is managed.

Transaction fees can be kept low because the computation to generate the signature takes place off-chain and only the final signature is recorded on the blockchain.
Unlike multi-sig, MPC wallet is more difficult to implement due to the use of advanced cryptographic techniques.

© BGIN – All rights reserved

Biometric wallet

This is a generic term for wallets that use biometric information. There are two types of Biometric wallet: one in which biometric information is used for key activation and the other in which biometric information is used as a signing key. The former is called a Biometric-locked wallet and the latter a Biometric-bound wallet. Since these are not mutually exclusive concepts, it is possible to conceive of wallets that are compatible with both.

First, we describe the features common to both.

Unlike keys and passwords, biometric information is inherently tied to the individual and cannot be lost, forgotten, or deliberately shared with others in the same way traditional credentials can be. However, biometric data can be stolen through data breaches or compromised through sophisticated spoofing attacks. Biometric wallets make use of the unique binding properties of biometric information to strengthen the connection between the signing key and the owner, and are expected to prevent the use of the signing key by anyone other than the legitimate owner. This binding varies in strength between Biometric-locked wallet and Biometric-bound wallet as noted below.

Biometric information also has the potential to realize hands-free use of wallets in shops, as it does not require conscious storage or remembering of credentials. Biometric wallets, which are device-independent, could enable a world in which any user can use a wallet without having to own a modern smart device or dedicated hardware with secure element functionality. This provides the concept that all a user needs to have in order to perform a transaction is their own 'biometric', which allows them to use the blockchain in a 'hands-off' format, without the need for a physical device.

On the other hand, there are fundamental issues concerning privacy, security and availability. Since biometric information is essentially immutable personal data, once compromised through data breaches or sophisticated attacks, the system may become permanently unusable for that individual. Therefore, both the entity managing the biometric information and the entity presenting the biometric information need to consider the privacy aspects and implement robust security measures.

These wallets are secure under the assumption that biometric information cannot be replayed without the genuine user; security depends on the accuracy of the biometric authentication. In practice, however, there is a risk of impersonation through copied photos or videos. Preventing this requires system-level enhancements such as

© BGIN – All rights reserved

presentation attack detection, digital injection mitigation and AI-based threat detection. In addition, there is also the issue of availability. If biometric information input is mandatory, there is a single point of failure. Biometric information cannot be used in some situations due to damage caused by accidents or injuries, or environmental factors such as darkness for a face captured without additional lighting.

Biometric-locked wallet

This is a type of wallet that uses biometric information for key activation. The wallet stores the key and biometric template. It can take various forms with regard to its storage location and authentication location. The key here also includes the distributed key share of the signing key. See ISO/IEC 24745 Table 5 for the forms of biometric template storage and biometric authentication locations. For the key storage location, it could be software, hardware or a combination of these.

Operational security depends to a large extent on how the keys and biometrics are managed and how the biometric authentication is performed. In the case of key escrow in a custodial wallet, the key management operator could in principle skip biometric authentication and use the key if no additional security measures are in place. In this sense, the biometric-locked wallet is considered as a weak binding between the key and the owner if there is no other strong security measure to mitigate misuse, for which the user would need to trust the operator. The following forms of enhanced biometric-locked wallet may be taken, where the operator is unable to use the key:
- combination with MPC wallet where part of the key is under control of the operator and part is locally unlocked by the biometric data.
- storing biometrically locked encryption keys locally and depositing the encrypted signature key with the operator.

Biometric-bound wallet

This is a type of wallet that uses biometric information as a signing key. Several such signature schemes have been studied [Dodis et.al, 2008, Takahashi et al, 2015, Higo et al, 2023].
Since biometric information only needs to be captured each time a signature is generated, it can be considered similar to a hardware wallet in the sense that keys are not stored on a computer. However, biometric wallets offer greater convenience than hardware wallets because the biometric information does not require conscious possession.

© BGIN – All rights reserved

There are cases where the user manages the secret information and cases where the user and a custodian manage it together: If the biometric information replaces the signing key and is not stored anywhere, or if the user manages secret information other than the biometric information, it falls into the first case. If there is secret information other than biometric information that needs to be stored and entrusted to another party, it falls under the latter case.

The key to generate the signature itself is not stored anywhere, so the binding is strong in the sense that the signature cannot essentially be generated without the person in question. Some signature schemes generate a temporary signature key during key generation or use biometric information to temporarily recover the signature key at the time of signing, at which point there is a risk of compromise.

Unlike digital keys, biometric information is difficult to transfer, which prevents unauthorized delegation of authority. This can prevent misuse of the service through malicious attribute transfer by users. Some signature schemes use their own verification algorithms and are therefore unsupported by the public chain.

Bureaucratic Bound Wallet

The Bureaucratic Bound Wallet represents an emerging category that combines biometric authentication with government-issued identification, creating a wallet system where the user's digital identity is cryptographically tied to their officially recognized physical identity. This model bridges the gap between traditional identity verification systems and blockchain technology.

Core Characteristics

In a Bureaucratic Bound Wallet, biometric data (such as fingerprints, facial recognition, or iris scans) is cryptographically linked to government-issued identity documents like passports, national ID cards, or driver's licenses. This creates a multi-factor authentication system with several key features:

- Government Attestation: The wallet incorporates cryptographic proofs that a government authority has verified the user's identity and biometrics
- Revocable Credentials: Unlike pure biometric systems, credentials can be revoked or updated by the issuing authority if necessary
- Cross-verification: Multiple sources of verification (biometric data, document data, and issuer attestation) create a robust identity foundation

© BGIN – All rights reserved

- Compliance Integration: Built-in compliance with regulatory requirements like KYC/AML that require government-verified identities

Implementation Approaches

Bureaucratic Bound Wallets can be implemented through several technical approaches:

1. Verifiable Credential Model: Government authorities issue digital credentials attesting to the relationship between a person's identity and their biometrics, which can be stored in the wallet and selectively disclosed
2. Biometric Binding with Official Database: The wallet implements a secure protocol to verify biometrics against government databases in real-time without storing the actual biometric data
3. Chip Integration: For countries with chipped identity documents (like biometric passports), the wallet can interface with the secure element on these documents to verify the user's identity

Security and Privacy Considerations

This wallet type introduces unique considerations:

- Cross-Border Validity: Government attestations may only be recognized within certain jurisdictions
- Revocation Concerns: If a government revokes identity verification, users may lose access to assets
- Surveillance Risks: The connection to official identity systems could enable enhanced tracking if not implemented with strong privacy protections
- Geopolitical Implications: Users from countries with problematic human rights records may face additional risks

Wallet-related biometrics threats and mitigations

Biometric systems in general face number of threats that are well summarized in the standard ISO/IEC 19792. Those threats include performance limitations, presentation attacks, modification of biometric characteristics, difficulty of concealing biometric characteristics, similarity due to blood relationship, special biometric characteristics, synthesised wolf, hostile environment, procedural vulnerabilities around the enrolment process, leakage and alteration of biometric data, etc.

Some of those threats have to be taken into account when designing and using a biometric wallet. Wallets leveraging biometrics need to follow the best practices for

© BGIN – All rights reserved

integrating biometric-specific security mitigations and general security mitigations to protect the wallet and the user against those threats. A comprehensive list of requirements and recommendations have been developed by ISO in the context of mobile-based biometric authentication for online services (see ISO/IEC 27553-1 and ISO/IEC 27553-2) that can be adapted to biometric wallets in order to ensure the appropriate level of security.

Overall there are tradeoffs between the level of security of a biometric wallet and the kind of assets and operations to be handled via the wallet, similarly to the choice of specific hardware wallets for instance (simple hardware vs tamper resistant hardware vs fully secure and certified hardware). It is important for the mitigations to be adapted to the context, and for the user to be educated about it. Technologies exist to secure a biometric wallet against presentation attacks or deep fake injection attacks but the cost of operating the wallet will be higher in that case, and thus the cost-benefit/security tradeoff.

Smart Contract Wallets

Smart contract wallets represent an evolution in blockchain technology, extending beyond traditional key-pair management to provide programmable accounts through on-chain smart contracts. These wallets enable advanced features like multi-signature requirements, spending limits, recovery mechanisms, and automated transaction handling while maintaining robust security.

Account Abstraction and EIP-4337

Account abstraction, formalized in Ethereum Improvement Proposal 4337 (EIP-4337), introduces crucial capabilities without requiring consensus-layer changes to the underlying blockchain:

- Custom transaction validation logic: Enabling policy-based controls beyond simple cryptographic signatures
- Batched transactions and atomic operations: Allowing multiple operations to be executed as a single transaction
- Gas fee abstraction and sponsorship: Permitting third parties to pay transaction fees on behalf of users
- Simplified user onboarding: Supporting social recovery and gradual security models

© BGIN – All rights reserved

The standard establishes a unified entry point contract for validation and standardized interfaces for chain-agnostic implementations.

Security Model

Smart contract wallets introduce a fundamentally different security architecture compared to traditional EOA (Externally Owned Account) wallets:

- Code-based security: Security rules enforced by immutable or upgradeable smart contract code
- Separation of ownership and execution: Distinction between wallet ownership and transaction execution
- Programmable authorization: Flexible permission systems that can adapt to different contexts
- On-chain recovery mechanisms: Built-in processes for account recovery that don't rely on seed phrases

Major Implementations

Coinbase Smart Wallet:

- Focuses on user-friendly key management and institutional-grade security
- Provides integrated DApp interactions with simplified user experience
- Supports cross-chain compatibility through standardized interfaces
- Implements tiered security with customizable policy controls

Safe (formerly Gnosis Safe):

- Industry-standard for organizational treasury management
- Supports highly customizable multi-signature arrangements
- Provides modular architecture with pluggable security features
- Enables programmable spending limits and transaction rules

Argent:

- Consumer-focused smart wallet with social recovery
- Implements guardians for account recovery without seed phrases
- Features daily transfer limits and approved address lists
- Integrates with popular DeFi protocols with security guardrails

Privy:

- Emphasizes developer-first integration with customizable authentication
- Features OAuth integration and email-based recovery systems
- Abstracts blockchain complexity for mainstream users
- Supports gradual progression from custodial to non-custodial control

© BGIN – All rights reserved

Technical Considerations

Smart contract wallets must address several key technical challenges:

- Contract security: Implementing formal verification and comprehensive audit processes to prevent vulnerabilities
- Upgrade mechanisms: Balancing immutability with the need for security upgrades and feature enhancements
- Key management: Providing flexible approaches to key storage, rotation, and recovery
- Transaction validation: Optimizing gas costs while maintaining robust validation rules
- Cross-chain functionality: Supporting assets across multiple blockchain networks

Future Developments

The evolution of smart contract wallets continues through several important directions:

- Enhanced cross-chain integration: Unified wallet interfaces that seamlessly operate across multiple blockchain networks
- Trust score implementation: On-chain accountability mechanisms inspired by the Accountable Wallet framework
- Privacy improvements: Zero-knowledge proof implementation for confidential transactions and interactions
- Advanced identity management: Integration with verifiable credentials and decentralized identity systems
- WebAuthn and passkey integration: Leveraging platform authentication standards for improved security and usability
- Hardware security integration: Combining smart contract logic with hardware security module protections

Accountable Wallet Framework

The concept of smart contract wallets aligns well with the "Accountable Wallet" framework proposed by Yamanaka et al. (2024), which introduces a comprehensive approach to proving wallet legitimacy across three critical dimensions:

1. Legitimacy of Wallet Holders: Verifying that the wallet is not controlled by sanctioned entities
2. Legitimacy of Wallet Conducts: Confirming the wallet has not engaged in illicit activities

© BGIN – All rights reserved

3. Legitimacy of Crypto Asset Provenances: Ensuring assets held in the wallet were acquired through legitimate channels

Smart contract wallets are uniquely positioned to implement these accountability features directly at the protocol level. For example, they can enforce transaction rules that prevent interaction with blacklisted addresses, integrate with "Chained Credentials" systems that track asset provenance, and calculate on-chain "Trust Scores" based on transaction history and verification proofs.

This accountability framework provides a trust model that could potentially address significant security and compliance challenges in decentralized finance by enabling legitimate wallets to actively prove their trustworthiness to counterparties. Smart contract wallets can enforce these accountability features programmatically, making them particularly valuable for institutional and regulated use cases.

Smart contract wallets represent an important bridge between blockchain's technical capabilities and mainstream user requirements. By abstracting complex cryptographic operations behind programmable interfaces and incorporating accountability frameworks, they balance advanced functionality with security requirements. As standards like EIP-4337 mature and adoption increases, these wallets will continue to evolve, offering increasingly sophisticated features while maintaining security and usability.

Account recovery

If a key is lost in the form of a wallet where the user manages the key, the assets associated with that wallet address will no longer be accessible. In such cases, it is recommended to recover the key and transfer it to another wallet address. An account recovery method to recover the key must therefore be ensured. A straightforward approach would be to store a copy of the key as backup information, but it should be noted that this increases the attack surface. The risk of key leakage from the backup information requires a secure recovery method. We shall choose methods that do not compromise the security of normal use. In addition, if the user manages the backup information by memorizing or storing it on a physical medium, there is a risk of forgetting the information or losing the medium. For this reason, a recovery method with high convenience is necessary. From the above, it is necessary to choose a recovery method that maintains the security of normal use and is highly convenient.

General recovery methods are to manage keys or mnemonic phrases or key share by

© BGIN – All rights reserved

memorization or possession.

Management location:
Like normal use wallets, they are managed by software or hardware devices. Other methods often use paper, metal or brains (memory). Paper is easy to use, but it can be wet, torn or erased. Metal is more durable than paper.

Object to be stored

Key

Store the key or the hexadecimal representation or QR code of the key. Paper or metal storage or memorisation is often used. QR codes have an error correction function and are resistant to partial damage.

Mnemonic Phrase

It is also called seed phrase or recovery phrase. It is basically a set of 12 or 24 words generated when a wallet is created; a 128-bit seed is generated for 12 words and a 256-bit seed for 24 words, from which the key is generated.They are selected from the 2048 words defined in the BIP-039 (Bitcoin Improvement Proposals) standard. The order of the words is also fixed, so they must be written down in the correct spelling and order. When stored by the user, paper, metal are often used. Words are easier to memorize than keys, so brain memory can also be used. Some services encrypt mnemonic phrases and further manage them using a secret sharing scheme.

Key share

The key is divided by a secret sharing scheme, and its share is managed by multiple administrators. Management entities can be users only, multiple operators, distributed among users and operators, or people designated by users, such as family members or friends. Note that there is a risk that the collusion of administrators may result in the collection of the number of shares required for recovery. The security is highly dependent on the trust relationship between the user and administrators. In order to prevent the collusion, for example, each share is encrypted with the user's encryption key and sent to each entity.

Social recovery is easy with smart contracts. The user designates guardians to manage the key shares. In the case of strict accounts, it is desirable for the guardian to authenticate users not by email or chat, but by video calls or face-to-face meetings.

© BGIN – All rights reserved

User also needs to set up the guardian appropriately. It is desirable to choose between different communities, which should be sorted out if the guardian can no longer be contacted or if the trust relationship has broken down. Users can add or remove guardians using their own signing keys, but the guardians are limited to Ethereum users.

Community recovery based on SBT has been proposed as a broader concept of social recovery [cite Weyl et al, 2022]. In [Ref], it is proposed to use SBT to set the guardians as the most recently connected people from each community to which the user belongs at the time of loss.This eliminates the need for conscious management of guardians by the user and improves convenience. Specific selection methods and operations have not yet been studied.

Multi-sig wallets and MPC wallets have redundancy in terms of keys and key shares. The redundant parts can be regarded as for recovery, and the wallets can be considered as wallets with recovery methods as well.

Biometric wallets differ from other wallets regarding recovery considerations, which are discussed below.

In Biometric-locked wallets, the keys themselves can be backed up in the same way as described above. On the other hand, there may be cases where the biometric information to activate the key cannot be used. For example, due to damage caused by accident or injury, or environmental factors such as darkness. Although the probability of the biometric information becoming unusable may be lower than the loss of a key, it is necessary to ensure other methods of authentication as a backup. For example, authentication by ID/PWD could be considered as an option, but it is less secure than normal use, resulting in a reduction in the security of the entire system. Therefore, biometric authentication using a modal different from the main biometric authentication is recommended.

Biometric-bound wallets do not store the keys themselves, so there is no concept of key backup. However, as with biometric-locked wallets, it is necessary to prepare for cases where biometric information cannot be used.

Recommendations for Core Implementation Standards

© BGIN – All rights reserved

As wallet technologies continue to evolve and converge, establishing robust implementation standards becomes increasingly critical. Based on our analysis of various wallet types and their security models, we propose several key recommendations for core implementation standards that should be considered by developers, organizations, and standards bodies.

Support for Zero-Knowledge Proofs

Zero-knowledge proof (ZKP) technology should be standardized as a core component of wallet implementations for several critical reasons:

- Privacy-Preserving Verification: ZKPs enable verification of credentials, transactions, and identity claims without revealing underlying data, balancing privacy with accountability
- Selective Disclosure: Standards for implementing selective disclosure using ZKPs allow users to reveal only necessary information for specific transactions
- Ownership Proof: ZKPs can verify asset ownership without exposing sensitive information about wallet balances or history
- Transaction Validation: Standardized ZKP implementations can enable private yet verifiable transaction validation across different blockchain networks

We recommend the development of interoperable ZKP libraries and protocols that can be consistently implemented across wallet types. Standards should specify minimum requirements for ZKP implementations, including performance benchmarks, security validation procedures, and privacy guarantees.

BGIN-ZKPdoc.docx

DID/VC/SBT Composable Outcomes

The intersection of Decentralized Identifiers (DIDs), Verifiable Credentials (VCs), and Soulbound Tokens (SBTs) represents a powerful framework for identity and reputation management in wallet systems. Standardization in this area should focus on:

- Interoperability: Establishing clear standards for how DIDs, VCs, and SBTs can interoperate across different wallet implementations and blockchain networks
- Credential Exchange Protocols: Standardizing secure methods for exchanging and verifying credentials between wallets
- Revocation Mechanisms: Developing consistent approaches to credential revocation that work across ecosystems

© BGIN – All rights reserved

- Binding Mechanisms: Standards for cryptographically binding DIDs to wallet addresses and credentials
- Cross-Chain Resolution: Protocols for resolving DIDs and verifying credentials across different blockchain networks

To achieve truly composable outcomes, we recommend:

1. Common Data Models: Standardizing data formats across DIDs, VCs, and SBTs to ensure consistent interpretation
2. Standard Verification Methods: Establishing common verification procedures that work consistently across implementations
3. Trust Registry Interoperability: Creating standards for how different trust networks and registries interact
4. Privacy-Preserving Presentation: Unified approaches to credential presentation that protect user privacy

Reference: (Soulbound Tokens (SBTs) Study Report Part 1: Building and Embracing a New Social Identity Layer? - Study Report at IKP WG, Blockchain Governance Initiative Network (BGIN): https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4449592

Recovery Standards and Best Practices

Building on the account recovery methods discussed previously, we recommend standardizing:

- Social Recovery Protocols: Establishing standard protocols and interfaces for implementing social and community recovery
- Backup Format Standards: Creating common formats for key and credential backups to ensure portability
- Recovery Attestation: Standardized methods for verifying the legitimacy of recovery attempts
- Cross-Wallet Recovery: Protocols enabling recovery across different wallet implementations

Secure Enclave Integration

For hardware-based security components:

- Secure Element APIs: Standardized interfaces for interacting with hardware security elements

© BGIN – All rights reserved

- Attestation Protocols: Common approaches to verifying the integrity of hardware elements
- Key Isolation Standards: Requirements for proper isolation of cryptographic keys in hardware

Implementation Security Frameworks

We recommend the development of comprehensive security evaluation frameworks specifically for wallet implementations:

- Security Levels: Defined security levels based on implementation characteristics
- Threat Modeling Standards: Common approaches to threat modeling for wallet implementations
- Penetration Testing Guidelines: Standardized methodologies for security testing
- Certification Processes: Independent certification standards for wallet security

These recommendations aim to establish a foundation for secure, interoperable, and privacy-preserving wallet implementations that can support the diverse and evolving needs of users across financial, identity, and governance applications. By adopting these standards, the industry can move toward a more cohesive ecosystem where wallets function as secure gateways to digital value and identity while preserving user sovereignty and privacy.

7. Wallets as a Financial Technology

Modern wallets are predominately digital and play a crucial role in modern financial systems by providing a secure, convenient, and efficient means for conducting financial transactions. They allow users to store, manage, and transfer funds electronically, eliminating the need for physical cash and traditional banking methods. With advanced security features like encryption and biometric authentication, digital wallets offer enhanced protection against fraud and unauthorised access. Their seamless integration with various financial services, including banking and online shopping, streamlines financial operations and enhances user experience.

Moreover, digital wallets promote financial inclusion by offering an alternative to traditional banking, particularly benefiting individuals in remote or underserved areas. They support innovative financial solutions, such as cryptocurrency storage and integration with emerging technologies like blockchain. By reducing transaction costs

© BGIN – All rights reserved

and providing real-time access to account information, digital wallets empower consumers to make informed financial decisions and manage their finances more effectively. Digital wallets transform the financial landscape, drive financial innovation, and pave the way for a cashless economy.

To date, most of the adoption of digital wallets has been through FinTech and now emerging blockchain and decentralised finance industries; however, there is a need for more education both among builders and consumers as to the trade-offs these wallets have in use. We are seeing a trend whereby digital wallets now use 'smart wallet' technologies (account abstraction), to bridge the gap between the user experiences of traditional finance, FinTech and digital currency wallets. What is notable about this trend is that centralised providers are abstracting blockchain-based wallet key management and security issues away. We hope this study report uplifts education among all types of wallets.

Types of Wallets in Digital Finance

As a financial application, wallets come in various forms, each designed to cater to different user needs and preferences. Here, we explore the primary types of digital wallets, highlighting their key features and functionalities and the challenges and risks associated with each type.

Mobile Wallets

Key Features and Functionalities:

- Convenience: Mobile wallets such as Apple Pay, Google Wallet, and Samsung Pay allow users to make payments using their smartphones. Transactions can be completed with a tap at contactless payment terminals.
- Security: These wallets employ advanced security measures like tokenisation, which replaces sensitive card information with a unique identifier, and biometric authentication, including fingerprint or facial recognition.
- Integration: Mobile wallets often integrate with other financial services and apps, providing seamless access to banking, shopping, and loyalty programs.
- Peer-to-Peer Payments: Many mobile wallets offer peer-to-peer (P2P) payment options, enabling users to send and receive money instantly.

Challenges and Risks:

- Security Vulnerabilities: Despite advanced security measures, mobile wallets can still be susceptible to hacking, malware, and phishing attacks.

© BGIN – All rights reserved

- Technology Adoption: Not all merchants accept mobile payments, limiting the usability of mobile wallets in specific regions or establishments.
- Dependence on Devices: Loss or theft of a mobile device can temporarily prevent access to funds until the wallet is restored on a new device.

Online Wallets

Key Features and Functionalities:

- Web-Based Access: Online wallets such as PayPal and Skrill are accessible through web browsers and mobile apps, allowing users to manage their funds from various devices.
- Multi-Currency Support: These wallets often support multiple currencies, making them ideal for international transactions and e-commerce.
- Linked Accounts: Users can link their online wallets to bank accounts, credit cards, and other payment methods, facilitating easy fund transfers.
- Merchant Services: Online wallets frequently offer merchant services, including invoicing, payment processing, and integration with e-commerce platforms.

Challenges and Risks:

- Regulatory Compliance: Online wallets must comply with varying regulatory frameworks across different regions, which can be complex and costly.
- Fraud and Scams: Online wallets are targets for fraud and scams, requiring continuous monitoring and robust security measures.
- Service Disruptions: Technical issues or cyber-attacks on the wallet provider's infrastructure can lead to service outages, affecting users' ability to access their funds.

Prepaid Wallets

Key Features and Functionalities:

- Preloaded Funds: Prepaid wallets, such as those provided by Starbucks or Amazon, require users to preload funds, which can then be used for purchases within the specified ecosystem.
- Ease of Use: These wallets are straightforward, making them popular for specific purposes like gifting or budgeting.
- Rewards and Discounts: Many prepaid wallets offer rewards programs, discounts, and special promotions to incentivise usage.

Challenges and Risks:

© BGIN – All rights reserved

- Limited Usability: Prepaid wallets are often restricted to specific merchants or ecosystems, limiting their versatility.
- Unused Funds: Users may end up with unused balances that are difficult to recover or transfer.
- Security Concerns: Paid wallets can be vulnerable to fraud and unauthorised use like other digital wallets.

Wearable Wallets

Key Features and Functionalities:

- Wearable Devices: Wearable wallets are integrated into devices like smartwatches and fitness trackers, enabling quick and convenient payments on the go.
- Contactless Payments: Similar to mobile wallets, wearable wallets use NFC technology for contactless payments, enhancing user convenience.
- Health and Fitness Integration: Often linked with health and fitness apps, these wallets can provide a holistic view of the user's lifestyle, combining financial and wellness data.

Challenges and Risks:

- Device Dependency: The functionality of wearable wallets depends on the wearable device, which may have limitations in terms of battery life and durability.
- Security Risks: Wearable devices can be lost or stolen, posing security risks if not adequately secured with authentication measures.
- Adoption Barriers: The adoption of wearable wallets may be slower due to higher costs and the need for consumers to adapt to new technology.

Cryptocurrency Wallets

While the prior sections of this paper include many of the types of cryptocurrency wallets available, it is important to note their application, functionality, and challenges in the specific use for financial transactions when analysing the overall digital wallet ecosystem.

Key Features and Functionalities:

- Blockchain Integration: Cryptocurrency wallets interact with blockchain networks to facilitate transactions and update the distributed ledgers they support. The most common type of cryptocurrency wallets interact with either Bitcoin or Ethereum and EVM (Ethereum virtual machine) based blockchains.

© BGIN – All rights reserved

- Private Key Management: These wallets manage private and public keys, which are crucial for securely signing transactions and accessing cryptocurrency holdings on-chain.
- Security: Cryptocurrency wallets emphasise security, offering features such as multi-signature support, hardware wallet integration, and secure recovery phrases. As seen in the section Types of Wallets, there are trade-offs regarding the security of different wallets.
- Decentralised Applications (DApps): Some cryptocurrency wallets provide access to DApps, enabling users to participate in Decentralised Finance (DeFi) activities and other blockchain-based services.

Challenges and Risks:

- Market Volatility: The value of cryptocurrencies can be highly volatile, posing financial risks to users.
- Security Risks: The loss or theft of private keys can permanently cause cryptocurrency funds to be lost. Additionally, cryptocurrency wallets are frequent targets for cyber-attacks.
- Regulatory Uncertainty: The regulatory landscape for cryptocurrencies is constantly evolving, creating uncertainty and compliance challenges for wallet providers and users.

As a financial technology, wallets come in various forms, each with unique features and functionalities tailored to different user needs. However, they face numerous challenges and risks, including security vulnerabilities, regulatory compliance issues, and technology adoption barriers. As digital wallet technology evolves, addressing these challenges will be crucial to enhancing their security, usability, and overall impact on the financial landscape.

We aim for this paper to support those who choose to build digital wallets in considering identifying the numerous iterations of blockchain-based wallet technology as alternatives to improve the security and self-sovereignty of existing digital wallets in the financial system.

Blockchain Wallet Recommendations Table

Policy Recommendations:

Wallet Type	Primary Users	Key Benefits	Best For	Typical Applications

© BGIN – All rights reserved

Custodial	- New users - Regular traders	- Managed security - Easy access - Simple interface	- Daily transactions - High-volume trading - Beginner users	- Crypto exchanges - Payment platforms - Retail transactions
Non-custodial	- Experienced users -Privacy-focused individuals	- Complete control - Enhanced privacy - Direct asset access	- Long-term holding - DeFi participation - Private transactions	- Investment portfolios - DeFi platforms - P2P transactions
Cold wallets	- Long-term investors -Security-focused users	-Maximum security -Offline storage -Physical backup	-Large holdings -Cold storage -Backup solutions	-Long-term storage -High-value assets -Security backups
Multi-signature	-Organizations -Joint accounts	-Shared control -Enhanced security -Governance support	- Corporate funds - Shared accounts - DAO governance	- Treasury management -Joint investments -DAO operations
MPC	-Institutions -Large enterprises	-Distributed security -Flexible control -Fraud prevention	-Institutional funds -Complex operations -High-security needs	- Asset management - Fund administration - Security solutions
Biometric	-Retail users -Consumer applications	-Easy authentication -User friendly -Quick access	-Regular payments -Consumer apps -Daily use	-Mobile payments -Consumer apps -Personal finance
Smart Contract	-DeFi users -Automated traders	-Programmable -Automated -Integration ready	-DeFi operations -Complex trades -Automated systems	-DeFi platforms -Automated trading -Token management

© BGIN – All rights reserved

8. Wallets as Governance Tools

In blockchain ecosystems, wallets serve as crucial instruments for governance, enabling participation in protocol decisions, DAO management, and network security through staking. The integrity of these governance actions relies on cryptographic signatures, making wallet security and management essential for maintaining trust in decentralized systems.

Core Governance Functions

Staking Governance

Staking governance allows token holders to secure blockchain networks by locking assets as stake. Key elements include:

- Validator participation and delegation
- Reward distribution and slashing mechanisms
- Protocol change voting rights
- Network security maintenance

Protocol Governance

Protocol governance enables stakeholders to influence network parameters and rules through:

- Governance token voting
- Protocol upgrade proposals
- Parameter adjustments
- Implementation oversight

DAO Governance

DAOs utilize smart contracts for organizational governance, featuring:

- Autonomous rule execution
- Token-based voting systems
- Proposal submission and review
- Collective decision-making

Transactional Governance

Management of transaction rules and policies includes:

© BGIN – All rights reserved

- Fee structures and priorities
- Dispute resolution mechanisms
- Transaction validation rules
- Network upgrade coordination

Oracle Governance

Oracle systems require governance for external data integration:

- Data provider management
- Validation mechanisms
- Incentive structures
- Decentralization maintenance

Governance Implementation by Wallet Type

Wallet Type	Primary Governance Use	Security Level	Key Benefits	Main Risks
Custodial	Basic participation	Low to Moderate	Easy access	Third-party dependence
Non-custodial (Software)	Direct control	Low to High	Full autonomy	User responsibility
Cold	Secure signing	High to Very High	Offline security	Limited accessibility
Multi-sig	Collective decisions	Hight to Very High	Distributed control	Coordination overhead
MPC	Institutional governance	High to Very High	Flexible control	Implementation complexity
Smart Contract	Automated governance	Moderate to High	Programmable rules	Smart contract risks

Advanced Governance Technologies

Account Abstraction

- Simplified user experience
- AI-assisted participation

© BGIN – All rights reserved

- Enhanced transaction management

Soulbound Credentials

- Identity verification
- Governance rights management
- Participation tracking

AI Integration

- Predictive governance analytics
- Automated participation
- Dynamic security adaptation
- Oracle optimization

Future developments in wallet governance will likely focus on:

1. Enhanced privacy through confidential computing
2. AI-driven decision support
3. Cross-chain governance coordination
4. Improved user experience through abstraction

Success in wallet governance requires balancing security, accessibility, and user experience while maintaining the decentralized nature of blockchain systems.

9. Wallets as Identity

Digital wallets have evolved significantly beyond their original purpose of cryptocurrency storage and transaction management. They now serve as comprehensive identity management platforms, enabling users to securely store, manage, and selectively disclose various aspects of their digital identity. This convergence of financial and identity functions presents both opportunities and challenges for security, privacy, and user sovereignty.

Core Identity Components and Technology Framework

As shown the fundamental components of identity-enabled wallets encompass various technologies and security considerations:

© BGIN – All rights reserved

Component	Technical Implementation	Key Features	Security Aspects	Standards/Protocols
Decentralized Identifiers (DIDs)	- Blockchain anchoring -Public key infrastructure -Resolution systems	- Globally unique -Persistent -Cryptographically verifiable	- Private key management -Revocation mechanisms -Recovery protocols	-W3C DID spec -DID Methods -DID Resolution
Verifiable Credentials	- JSON-LD format -Digital signatures -Merkle proofs	-Tamper-evident -Privacy-preserving -Selective disclosure	- Issuer authentication - Credential encryption -Revocation registries	- W3C VC Data Model -JWT/JSON-LD - ZKP protocols
Self-Sovereign Identity	- Identity hubs - Peer-to-peer protocols - Credential agents	- User control - Portability - Interoperability	- Edge computing security - Data encryption - Access management	- DIDComm - KERI - Aries protocols

Identity Wallet Applications and Use Cases

Identity wallets serve various purposes across different sectors:

Healthcare Applications

- Medical record management
- Insurance verification
- Treatment authorization
- Provider credentials

Government Services

- Digital identification
- Public service access
- Voting systems
- Regulatory compliance

Corporate Identity

- Employee credentials

© BGIN – All rights reserved

- Access management
- Supply chain verification
- Contractor management

Privacy and Data Protection

Identity wallets must implement robust privacy protection mechanisms:

Data Minimization

- Selective disclosure protocols
- Purpose limitation
- Storage minimization
- Processing restrictions

Privacy-Enhancing Technologies

- Zero-knowledge proofs
- Fully homomorphic encryption
- Secure multi-party computation
- Ring signatures

Governance and Best Practices

User Control

- Granular consent mechanisms
- Clear terms of service
- Data access revocation
- Identity portability

Security Measures

- End-to-end encryption
- Multi-factor authentication
- Regular security audits
- Incident response planning

Standards Compliance

- Technical standards adherence
- Regulatory compliance

© BGIN – All rights reserved

- Industry best practices
- Security certifications

Future Developments

Emerging Technologies

- AI integration for identity verification
- Quantum-resistant cryptography
- Enhanced biometric systems
- Cross-chain identity solutions
- Identity binding

Ecosystem Evolution

- Standardized protocols
- Improved interoperability
- Enhanced privacy controls
- User experience optimization

The evolution of wallets into identity management platforms represents a significant advancement in digital infrastructure. Success in this domain requires careful balance of security, privacy, and usability while maintaining compliance with evolving regulations and standards. Organizations implementing identity wallets must consider both current requirements and future developments to create sustainable, user-centric solutions.

Organizations must particularly focus on:

1. Robust security implementation across all wallet types
2. Comprehensive privacy protection mechanisms
3. Clear governance frameworks and best practices
4. Preparation for emerging technologies and threats

The future of identity wallets lies in their ability to provide secure, private, and user-controlled identity management while maintaining interoperability across different systems and use cases.

10. Lifecycle of Wallets

Digital wallet lifecycles encompass complex interactions between technical implementation, security requirements, governance mechanisms, and regulatory compliance. Understanding these lifecycles is crucial for developers, operators, and users of wallet systems, particularly as

© BGIN – All rights reserved

wallets evolve from simple key storage solutions to sophisticated platforms managing financial assets, identity credentials, and governance rights.

Core Lifecycle Stages

As outlined in the Lifecycle of Wallets: Stages and Components table, wallet lifecycles comprise five primary stages, each with distinct requirements and considerations for different wallet types.

Creation and Initialization

The creation phase establishes the foundation for wallet security and functionality. For non-custodial wallets, this involves secure key generation using high-entropy sources and implementing appropriate backup mechanisms. Custodial wallets must additionally establish robust authentication systems and operational procedures.

Key considerations during initialization include:

- Implementation of cryptographic protocols appropriate to wallet type
- Establishment of governance mechanisms and access controls
- Integration with existing identity and security systems
- Setup of monitoring and compliance frameworks

Hardware wallets require additional steps to verify device integrity and establish secure communication channels. MPC wallets must coordinate distributed key generation ceremonies among participants while maintaining security throughout the process.

Active Operations

During active use, wallets must balance security, usability, and compliance requirements. Modern wallets increasingly handle multiple functions simultaneously:

- Financial Operations: Modern wallets process various transaction types, from simple transfers to complex smart contract interactions. Each transaction type requires appropriate security measures, fee management, and compliance checks.
- Identity Management: Wallets increasingly serve as identity management platforms, storing and managing verifiable credentials, DIDs, and authentication mechanisms. This requires sophisticated access control and privacy-preserving mechanisms.
- Governance Participation: Many wallets now facilitate participation in DAOs, protocol governance, and other decentralized decision-making processes. This requires secure voting mechanisms and delegation capabilities.

Maintenance and Updates

Wallet maintenance encompasses both routine operations and critical updates. This phase requires careful balance between security, availability, and user experience:

© BGIN – All rights reserved

System Updates:

- Security patches must be deployed promptly while maintaining wallet accessibility
- Protocol upgrades require careful coordination, especially for non-custodial wallets
- Feature additions must undergo thorough security review

Policy Updates: Changes to governance parameters, security policies, or compliance requirements must be implemented without disrupting wallet operations or compromising security.

Recovery Scenarios

Recovery mechanisms represent a critical component of wallet lifecycle management. Different wallet types require specific recovery approaches:

1. Custodial Wallets: Focus on operational recovery procedures and business continuity planning.
2. Non-custodial Wallets: Emphasize user-controlled recovery mechanisms like social recovery or secure backup systems.
3. Hardware Wallets: Require specific procedures for device failure or replacement scenarios.
4. MPC or multi-sig Wallets: Must handle scenarios where multiple participants or key shares are involved in recovery.
5. Smart Wallets: Leveraging smart contract capability (e.g. account abstraction on Ethereum) to embed on-chain dedicated recovery functionalities
6. Communal Recovery: A recovery mechanism that leverages a trusted community or collective entity to restore wallet access, potentially through shared responsibility models within a defined group or organization.
7. Social Recovery: A non-custodial wallet recovery approach where trusted individuals ("guardians") are designated to help restore access when a user loses their primary key, distributing recovery authority across a personal network.

Decommissioning

The final lifecycle stage requires careful management to ensure security and compliance:

- Planned Decommissioning: Involves systematic transfer of assets, credentials, and governance rights while maintaining security and regulatory compliance.
- Emergency Decommissioning: Requires rapid response capabilities while preserving necessary records and maintaining security.

With the emergence of new technologies, namely quantum computing, we must remain agile for the framework of wallet use and governance long term, decommissioning as a lifecycle stage needs to be considered upon creation.

© BGIN – All rights reserved

Considerations and Concerns Throughout the Lifecycle of a Wallet

Several factors impact all lifecycle stages:

Security Considerations

Security remains paramount throughout the wallet lifecycle. Key aspects include:

- Cryptographic protocol implementation
- Access control mechanisms
- Monitoring systems
- Vulnerabilities management
- Incident response capabilities

Governance Requirements

Governance mechanisms must be established early and maintained throughout the lifecycle:

- Access control policies
- Update procedures
- Recovery authorization
- Decommissioning protocols

Regulatory Compliance

Compliance requirements affect all lifecycle stages:

- Initial registration and licensing
- Ongoing monitoring and reporting
- Update management
- Decommissioning procedures

Privacy Protection

Privacy considerations include:

- Data minimization practices
- Consent management
- Information sharing controls
- Cross-border data flows

Future Considerations

The evolution of wallet technology, together with advanced on-chain functionalities, drives changes in lifecycle management:

© BGIN – All rights reserved

Technological Advancement

Emerging technologies affecting wallet lifecycles include:

- Quantum resistance preparation
- AI integration
- Cross-chain compatibility
- Layer 2 solutions
- User binding
- Proof of personhood

Enhanced Privacy

Privacy-preserving technologies increasingly important:

- Zero-knowledge proofs
- Full homomorphic encryption
- Selective disclosure mechanisms
- Multi-Party Computation

Regulatory Evolution

Evolving regulatory landscape requires:

- Flexible compliance frameworks
- Adaptable technical infrastructure
- Enhanced reporting capabilities

Lifecycle of Wallets: Stages and Components

Lifecycle Stage	**Component**	**Key Elements**	**Security Considerations**	**Governance Requirements**
1. Creation and Initialization	Key Generation	- Secure random number generation - Key derivation protocols - Support for multiple key types (single, multi-sig, MPC) - HSM integration	- Entropy source quality - Key generation environment security - Protection against side -channel attacks	- Key generation ceremony documentation - Audit trail requirements - Compliance verification

© BGIN – All rights reserved

	Initial Setup	- User authentication setup - Backup procedures - Identity system integration - Security parameter configuration	- Secure initial configuration - Protection of setup parameters - Access control implementation	- Policy documentation - User agreement establishment - Regulatory compliance checks
	Verification	- Cryptographic operation testing - Recovery procedure validation - Security configuration audit	- Testing environment security - Verification process integrity - Independent audit requirements	- Compliance documentation - Audit report requirements - Verification standards
2. Active Usage	Transaction Management	- Financial transaction processing - Identity credential handling - Governance participation - Smart contract interaction	- Transaction signing security - Replay attack prevention - Rate limiting implementation	- Transaction approval policies - Voting rights management - Multi-signature requirements
	Key Management	- Key rotation procedures - Backup maintenance - Multi-signature coordination - MPC share management	- Key usage monitoring - Access control enforcement - Key compromise detection	- Key rotation policies - Access control policies - Backup verification requirements
	Security Monitoring	- Transaction pattern analysis - Anomaly detection - Security event logging - Access tracking	- Real-time monitoring systems - Incident response readiness - Audit log protection	- Security policy enforcement - Incident reporting requirements - Compliance monitoring
3. Maintenance	Software Updates	- Security patches - Feature upgrades - Protocol compatibility - UI improvements	- Update verification - Rollback capability - Testing requirements	- Change management policies - Update approval process - Testing requirements

© BGIN – All rights reserved

	Policy Updates	- Governance revisions - Security policy updates - Privacy policy changes	- Policy enforcement mechanisms - Change impact assessment - User notification systems	- Policy approval process - User consent management - Regulatory alignment
	Key Rotation	- Scheduled rotations - Certificate renewals - Backup updates	- Secure key transition - Old key destruction - New key validation	- Rotation schedule compliance - Audit requirements - Documentation standards
4. Recovery	Lost Access	- Social recovery implementation - Hardware failure recovery - Biometric backup procedures	- Recovery verification - Identity validation - Timeout mechanisms	- Recovery approval process - Documentation requirements - Time lock policies
	Compromise Recovery	- Security breach response - Key revocation - Asset recovery	- Immediate containment - Evidence preservation - New key generation	- Incident response policies - Stakeholder notification - Recovery authorization
	Disaster Recovery	- Backup restoration - Alternative access - Business continuity	- Secure recovery environment - Data integrity verification - Access control maintenance	- Recovery plan compliance - Stakeholder communication - Audit requirements
5. Decommissioning	Planned	- Asset transfer - Credential migration - Key destruction	- Secure data erasure - Transfer verification - Access revocation	-Decommissioning approval - Documentation requirements - Compliance verification
	Emergency	- Rapid asset securing - Credential revocation - Immediate suspension	- Immediate access termination - Evidence preservation - Forensic considerations	- Emergency procedures - Notification requirements - Legal compliance

© BGIN – All rights reserved

	Legacy Planning	- Inheritance procedures - Long-term access - Historical records	- Access transition security - Long-term storage security - Data preservation	- Succession policies - Legal requirements - Documentation standards

Digital wallets are undergoing a fundamental transformation, evolving from single-purpose tools into integrated platforms that manage money, identity, and data. This convergence means a single wallet might now handle everything from complex financial transactions and identity verification to everyday activities like paying for public transport. Understanding how these wallets function throughout their lifecycle - from creation to eventual retirement - has become crucial for everyone from financial institutions managing billions in assets to individual users making daily transactions.

The stakes of this convergence are significant. A wallet that stores both financial assets and identity credentials requires more sophisticated security measures and careful lifecycle management than one that simply holds funds. Yet these same wallets must remain accessible and user-friendly enough for routine transactions. Whether used by a hedge fund executing complex trading strategies or a commuter tapping into a transit system, proper wallet lifecycle management ensures security, reliability, and appropriate functionality across all use cases.

This convergence represents both an opportunity and a challenge. While integrated wallets offer unprecedented convenience and functionality, they also introduce new complexities in security, privacy, and usability. Understanding these tradeoffs and managing wallet lifecycles effectively has become essential for developers, businesses, and users navigating this evolving digital landscape.

11. Convergence of Wallets

A Unified Framework and Future Outlook

Digital wallets are evolving from single-purpose tools into integrated platforms that combine financial operations, governance participation, and identity management. This convergence enables users to manage cryptocurrencies, participate in DAO voting, and control digital identities through a single interface, fundamentally changing how users interact with blockchain ecosystems.

Principles of Universal Wallet Architecture

Drawing from the OpenWallet Foundation's reference architecture, the future of convergent wallets should be guided by these core principles:

© BGIN – All rights reserved

1. **Multi-purpose**: Designed to handle diverse capabilities across identity, objects, and money rather than serving a single use case
2. **Privacy-preserving**: Built with user privacy as a foundational requirement, not an afterthought
3. **Interoperable**: Leveraging open standards to ensure data can be used across different systems
4. **Portable**: Enabling users to move between wallet implementations without lock-in
5. **Equitable**: Ensuring accessibility without discrimination
6. **Open**: Utilizing open-source approaches, collaboration, and standards

Architectural Components for Convergence

A comprehensive architecture for converged wallets includes:

User-Facing Components

- **Administrative UI**: Interfaces for wallet setup, login, and management
- **SDK and API Layer**: Developer tools for building on wallet capabilities

Core Service Components

- **Agents**: Services that act on behalf of wallet owners for issuance, presentation, P2P interactions, and policy enforcement
- **Wallet Services**: Core functions including consent management, profile management, inventory management, and transaction processing
- **Secure Storage**: Specialized storage for keys, credentials, and data with appropriate security controls

Network Interaction Components

- **Network Services**: Capabilities for connecting to networks via indexers, connectors, and trust registries
- **P2P Services**: Direct wallet-to-wallet communication capabilities

Implementation Challenges and Considerations

Security Considerations

- **Expanded Attack Surface**: The integration of multiple functions increases potential vulnerabilities
- **Complex Security Requirements**: Different functions require varied security approaches

© BGIN – All rights reserved

- **Key Management Complexity**: Robust systems for key generation, storage, recovery, and rotation
- **Multi-factor Authentication**: Balancing security with usability in authentication mechanisms

Privacy Implications

- **Cross-linking of Data**: Risk of correlating financial and identity information
- **Selective Disclosure**: Need for granular control over what information is shared
- **Zero-Knowledge Capabilities**: Implementation of advanced privacy-preserving technologies
- **Consent Management**: Robust systems for obtaining and tracking user consent

Technical Framework Requirements

- **Interoperability Standards**: Development of common protocols for cross-wallet interactions
- **Scalability Solutions**: Architectures that can handle increasing transaction volumes
- **Cross-chain Compatibility**: Support for multiple blockchain networks and technologies
- **Offline Capabilities**: Functioning without continuous network connectivity

Critical Questions for the Future

Power and Control

- **Digital Autonomy**: Are we creating new digital gatekeepers through wallet convergence?
- **Standards Governance**: Who controls the evolution of wallet interoperability standards?
- **Centralisation Risks**: Does convenience inevitably lead to centralization, and what safeguards can prevent wallet providers from becoming too powerful?

Privacy and Identity

- **Personal Data Management**: Can privacy truly be maintained in converged systems?
- **Digital Rights**: How do we ensure user sovereignty over their digital presence?
- **Context Separation**: How can users maintain separate identities for different contexts?

Social Implications

- **Digital Divide**: Will wallet convergence widen or narrow technology gaps?
- **Financial Inclusion**: How can converged wallets promote greater financial inclusion?
- **Economic Power Shifts**: How might this technology reshape economic power structures?

© BGIN – All rights reserved

12. Standards and Implementation Path Forward

As this study has demonstrated, digital wallets have evolved dramatically from their origins as simple cryptocurrency storage solutions to become sophisticated multi-purpose platforms that integrate financial operations, governance mechanisms, and identity management systems. Throughout this paper, we have examined the complex landscape of wallet types—from custodial and non-custodial implementations to hardware, software, biometric, and smart contract wallets—each offering distinct advantages and trade-offs for specific use cases.

Synthesis of Key Findings

Our analysis reveals several critical insights that must inform future wallet development and standardization efforts:

Security and Risk Management

The examination of current problems and risks in Section 6 highlighted significant vulnerabilities in wallet implementations, from direct security breaches to key management failures and governance shortcomings. Notable incidents like the Bybit Hack, Parity Wallet Hack, QuadrigaCX case, and Wirex breach underscore the importance of robust security architectures. These events demonstrate that security cannot be an afterthought but must be integrated throughout the wallet lifecycle—from creation and initialization through active operations, maintenance, decommissioning, and recovery scenarios.

Wallet Type Optimization

Section 7's detailed analysis of wallet types revealed that different implementations serve distinct purposes with varying security profiles. Non-custodial wallets provide maximum user control but place significant responsibility on users, while custodial solutions offer convenience at the cost of third-party dependency. Hardware wallets provide high security for long-term storage, while MPC and multi-signature implementations offer institutional-grade protection with distributed control. As explored in Section 8, these implementations must be matched appropriately to their use cases, with consideration for the specific security, usability, and regulatory requirements of each application.

Beyond Financial Applications

Our exploration of wallets as governance tools in Section 9 and identity systems in Section 10 demonstrated the expanding utility of wallet technologies beyond simple financial transactions. Governance implementations enable participation in decentralized decision-making through staking, protocol governance, and DAO management. Identity wallets support verifiable credentials, selective disclosure, and self-sovereign identity models that fundamentally transform digital trust architectures. This convergence creates powerful new capabilities but also

© BGIN – All rights reserved

introduces complex security and privacy challenges that must be addressed through thoughtful standardization.

Lifecycle Management

The comprehensive lifecycle analysis in Section 11 emphasized the importance of understanding wallets as complete systems with distinct phases—creation, active operations, maintenance, recovery, and decommissioning—each requiring specific security considerations and governance mechanisms. This lifecycle approach is essential for developing standards that address the full spectrum of wallet implementation concerns, from initial key generation to emergency recovery scenarios and eventual decommissioning.

The Case for Standardization

The convergence of wallet functionalities outlined in Section 12 presents both tremendous opportunities and significant challenges. The integration of financial, governance, and identity functions within single interfaces enables powerful new user experiences but also introduces complex security, privacy, and regulatory considerations that cannot be addressed through ad hoc approaches.

Drawing from the OpenWallet Foundation's reference architecture, we see a compelling framework for standardization based on core principles:

1. **Multi-purpose Design**: Standards must accommodate diverse capabilities across identity, objects, and money while maintaining security boundaries between functions.
2. **Privacy Preservation**: Privacy must be treated as a foundational requirement rather than an add-on, with standards for data minimization, selective disclosure, and consent management.

3. **Interoperability**: Open standards for data exchange, credential formats, and protocol interactions are essential for ensuring wallets can interoperate across different systems and ecosystems.
4. **Portability**: Standards must enable users to move between wallet implementations without lock-in, ensuring long-term data accessibility and ownership.
5. **Equitable Access**: Standardization efforts must prioritize accessibility and avoid creating systems that exclude or discriminate against users based on geography, ability, or socioeconomic status.
6. **Open Development**: Standards development should follow open processes with broad stakeholder participation, ensuring that critical infrastructure isn't controlled by a single entity or closed group.

© BGIN – All rights reserved

Recommendations for Standards Development

Based on this study's findings, we propose the following priority areas for standards development:

1. Security Framework Standardization

Develop comprehensive security standards for different wallet types, addressing key management, authentication, secure storage, and cryptographic operations. These standards should include:

- Certification criteria for hardware security elements and TEEs
- Implementation guidelines for multi-party computation and threshold signatures
- Security requirements for biometric-based wallets
- Standardized security audit methodologies for wallet implementations

2. Lifecycle Management Standards

Create standards that address the complete wallet lifecycle, providing implementation guidance for:

- Secure key generation and initialization procedures
- Backup and recovery protocols, including social and communal recovery mechanisms
- Key rotation and update management
- Secure decommissioning procedures with proper data sanitization

3. Identity and Credential Standards

Advance standards for identity credentials and selective disclosure that enable privacy-preserving verification:

- Credential format standards compatible with verifiable credentials
- Selective disclosure protocols that minimize data sharing
- Zero-knowledge proof implementations for privacy-preserving verification
- Cross-chain identity resolution mechanisms

4. Governance Participation Standards

Develop standards for secure governance participation through wallet interfaces:

- Voting mechanism standards for on-chain governance
- Delegation protocols for representative participation
- Secure multi-step approval processes for critical governance actions
- Transparency and auditability standards for governance activities

© BGIN – All rights reserved

5. Regulatory Compliance Standards

Establish standards that address regulatory requirements across jurisdictions:

- KYC/AML compliance frameworks that preserve privacy where possible
- Data protection standards aligned with GDPR and similar regulations
- Cross-border transaction compliance mechanisms
- Standardized approaches to travel rule compliance

Implementation Considerations

Standardization alone is insufficient without thoughtful implementation strategies.

Organizations implementing wallet systems should consider:

Phased Implementation Approach

Organizations should adopt a phased approach to implementing converged wallet systems:

1. **Assessment Phase**: Evaluate existing systems against emerging standards and identify gaps
2. **Foundation Phase**: Implement core security and key management capabilities
3. **Integration Phase**: Add specialized functionality for identity and governance
4. **Optimization Phase**: Enhance user experience while maintaining security boundaries

Security-First Development

As demonstrated throughout this study, security compromises in wallet implementations can have catastrophic consequences. Organizations should:

- Implement secure development lifecycles with threat modeling
- Conduct regular security audits and penetration testing
- Establish bug bounty programs for continuous improvement
- Develop incident response plans for security breaches

User-Centric Design

The usability challenges highlighted in our analysis of various wallet types must be addressed through:

- Progressive security models that match security levels to transaction risk
- Intuitive recovery mechanisms that balance security and accessibility
- Clear consent mechanisms for data sharing and credential presentation
- Appropriate education and support for users transitioning to new systems

© BGIN – All rights reserved

Future Research Directions

While this study provides a comprehensive overview of wallet governance, policy, and key management considerations, several areas require further research:

1. **AI Integration**: What governance frameworks are needed for AI agents operating through wallet interfaces?
2. **Cross-Chain Identity**: How can identity be maintained consistently across multiple blockchain environments?
3. **Biometric Binding**: What standards are needed for secure biometric-bound wallets that preserve privacy?
4. **Quantum Resistance**: How can wallet implementations prepare for post-quantum cryptography requirements?
5. **Recovery Evolution**: How might social and communal recovery mechanisms evolve with technologies like Soulbound Tokens?

13. BGIN's Role

The Blockchain Governance Initiative Network (BGIN) is uniquely positioned to facilitate the critical dialogue around wallet governance and standardization. As a multi-stakeholder forum bringing together technologists, businesses, regulators, academics, and civil society representatives, BGIN provides a neutral space for addressing the complex challenges that arise from wallet convergence across financial, governance, and identity domains.

The role of BGIN in advancing wallet governance includes:

1. **Fostering Cross-Domain Collaboration**: BGIN bridges traditional siloes between financial services, identity management, and governance communities, enabling holistic approaches to wallet standards that address the full spectrum of use cases.
2. **Promoting Open Standards Development**: By supporting open, transparent, and inclusive standards development processes, BGIN ensures that wallet governance frameworks reflect diverse stakeholder needs rather than narrow commercial interests.
3. **Facilitating Knowledge Exchange**: Through working groups, research initiatives, and public documentation, BGIN enables the sharing of best practices, security insights, and implementation experiences across different blockchain ecosystems.
4. **Engaging Policymakers**: BGIN's inclusive approach creates opportunities for constructive dialogue between technical communities and regulatory bodies,

© BGIN – All rights reserved

helping to shape policy frameworks that balance innovation with appropriate safeguards.

5. **Addressing Global Perspectives**: By incorporating voices from different regions and jurisdictions, BGIN helps develop wallet governance approaches that respect diverse regulatory, cultural, and social contexts.

Conclusion

The convergence of wallets represents a fundamental transformation in how we interact with digital assets, manage our identities, and participate in decentralized governance. This transformation offers unprecedented opportunities for user empowerment and efficiency but also introduces complex security, privacy, and regulatory challenges that must be addressed through thoughtful standardization and implementation.

By developing comprehensive standards based on the principles outlined in this study and the architectural framework provided by initiatives like the OpenWallet Foundation, we can create wallet systems that balance security, usability, and innovation. These standards must be developed through open, collaborative processes that engage diverse stakeholders—from technical experts and businesses to regulators and end users.

The future of digital wallets lies not just in their technical capabilities but in how effectively they serve human needs while protecting fundamental rights. Through carefully considered standards and responsible implementation, we can ensure that the convergence of wallet technologies empowers users, enhances security, and builds a more inclusive digital economy.

As wallet technologies continue to evolve, ongoing dialogue between technologists, businesses, regulators, and society will be essential for addressing emerging challenges and opportunities. This study represents a step toward that dialogue, offering a framework for understanding and implementing effective wallet governance while maintaining security, privacy, and regulatory compliance. Through BGIN's continued engagement with these issues, we can collectively shape the evolution of wallet technologies in ways that preserve their transformative potential while addressing legitimate concerns about security, privacy, and inclusion.

© BGIN – All rights reserved

Appendix A – Acknowledgement

(Informative)

A.1 Editors and Co-editors

- Mitchell Travers (Soulbis)
- Saki Otsuki
-

A.2 Contributors

- BGIN IKP Working Group Participants
- Julien Bringer
- Nikita Kent
- Ken Katayama
- Masato Yamanaka
- Bruno Martins
- Takaya Sugino

© BGIN – All rights reserved

Appendix B – Informative reference

(Informative)

- Nakamoto, Satoshi. 2008. “Bitcoin: A Peer-to-Peer Electronic Cash System” Available: https://bitcoin.org/bitcoin.pdf (last viewed on January 18, 2023)
- Sovrin Foundation. December 6, 2018. “What is self-sovereign Identity?” Available: https://sovrin.org/faq/what-is-self-sovereign-identity/
- Szabo, Nick. 1996. “Smart Contracts: Building Blocks for Digital Markets.” Available: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html.
- Weyl, Eric Glen and Ohlhaver, Puja and Buterin, Vitalik, 2022. “Decentralized Society: Finding Web3's Soul.” Available at SSRN: https://ssrn.com/abstract=4105763
- Kei. July 21st, 2021. “A Prehistory of DAOs.” Available: https://gnosisguild.mirror.xyz/t4F5rItMw4-mlpLZf5JQhElbDfQ2JRVKAzEpanyxW1Q.
- Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, “Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data,” SIAM Journal on Computing, vol. 38, no. 1, pp. 97–139, Jan. 2008.
- K. Takahashi, T. Matsuda, T. Murakami, G. Hanaoka, and M. Nishigaki, “A Signature Scheme with a Fuzzy Private Key”, in International Conference on Applied Cryptography and Network Security, 2015.
- H. Higo, T. Isshiki, S. Otsuki, and K. Yasunaga, “Fuzzy Signature with Biometric-Independent Verification,” 2023 International Conference of the Biometrics Special Interest Group (BIOSIG), pp. 1–6, 2023.
- https://github.com/openwallet-foundation/architecture-sig/tree/main
    - https://github.com/openwallet-foundation/architecture-sig/blob/main/docs/papers/architecture-whitepaper.md
- **Kshetri, N. (2017).** *Blockchain's Roles in Strengthening Cybersecurity and Protecting Privacy*. *Telecommunications Policy, 41*(10), 1027-1038
- **Chuen, D. L. K. (Ed.). (2015).** *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data*. Academic Press.
- https://soulsync.substack.com/p/lessons-from-the-bybit-hack-smart

© BGIN – All rights reserved

Appendix C

Additional details on specifically impactful biometric wallet threats

Biometric Resets and Physical Modifications

A significant challenge for biometric wallet systems is addressing permanent or semi-permanent changes to a user's biometric characteristics. Plastic surgery, severe injuries, or medical conditions can alter facial features, fingerprints, or other biometric identifiers used for authentication. This creates a unique challenge:

- Identity Continuity: Systems must maintain identity verification capabilities despite physical changes while preventing fraudulent "reset" attempts
- Verification Procedures: Some implementations require medical certification or plastic surgery documentation to authorize biometric resets
- Multi-modal Authentication: Advanced systems use multiple biometric factors to reduce dependency on any single characteristic that might change
- Step-up Authentication: Transitional verification using additional factors during periods of physical change

These measures must be carefully balanced—too strict, and legitimate users may lose access after medical procedures; too lenient, and attackers could exploit the reset process.

Deepfake and Synthetic Biometric Attacks

Advances in AI have created increasingly sophisticated methods to generate synthetic biometric data that can fool authentication systems:

- Deepfake Videos: AI-generated videos can potentially defeat facial recognition systems by simulating liveness
- Synthetic Fingerprints: Machine learning models can now generate artificial fingerprints capable of matching multiple real fingerprints
- Voice Synthesis: Voice cloning technology can produce convincing replicas of a target's speech patterns

Mitigation strategies include:

- Multimodal Verification: Requiring multiple biometric factors simultaneously
- Neural Analysis: Advanced systems that detect synthetic patterns in presented biometrics
- Challenge-Response Mechanisms: Unpredictable interactive challenges that are difficult for synthetic systems to anticipate

© BGIN – All rights reserved

- Hardware Attestation: Verification that biometric data comes from trusted sensor hardware

The arms race between attack and defense technologies in this domain continues to accelerate, requiring biometric wallet implementers to maintain vigilance and regularly update security measures as new threats emerge.

Appendix D

BGIN Layer2Meetup@Tokyo Meeting Report_Wallet Governance

Presentation of Wallet Governance and Policy Study Report by BGIN

1. Convergence of Wallet Use Cases:

- **Question**: One of the key questions raised was whether financial and non-financial use cases for wallets should come together in a single wallet or remain separate.
- **Discussion**: Several participants pointed out that from a user experience perspective, separating financial and non-financial functions would be detrimental, as it would complicate adoption. This sparked a discussion about whether identity and financial transactions would converge naturally, as trust and reputation systems evolve.

2. AI Integration in Wallets:

- **Question**: A question was raised about whether AI agents will become primary users of blockchain wallets in the future and what the implications might be for **AML/CFT** compliance.
- **Discussion**: Participants considered how AI agents might impact financial transactions and whether AI could be held accountable for its actions. The discussion explored how AI-driven transactions could complicate KYC/AML processes, and whether there would be a need for signatures proving that a human authorized an AI transaction.

3. Governance Wallets and Voting:

- **Question**: The discussion touched on whether wallets should be used for governance activities, such as voting, and what security considerations should be taken into account.
- **Discussion**: Some participants argued that governance wallets might sit at the intersection of finance and identity, but there was debate about whether wallets should have a specific governance function or if existing wallets (used for finance and identity) could be adapted for governance. Concerns about anonymity and security in voting were also raised, especially in governance systems where cryptographic signatures are essential.

4. On-Chain vs. Off-Chain Wallet Governance:

© BGIN – All rights reserved

- **Question**: Should wallet governance take place on-chain, or is there a need for off-chain solutions to manage governance use cases more effectively?
- **Discussion**: The debate focused on the pros and cons of on-chain governance, which offers transparency but comes with challenges such as vulnerability to attacks. Off-chain governance, on the other hand, might offer more flexibility but could sacrifice transparency. Participants discussed the potential for using zero-knowledge proofs and decentralized storage solutions to protect data while maintaining the security of wallets used for governance.

5. Identity and Privacy in Wallets:

- **Question**: Should wallets be focused solely on identity, or should identity be a starting point for integrating other use cases (such as finance and governance)?
- **Discussion**: This sparked a conversation about whether identity and reputation drive financial transactions, or if finance leads to the creation of reputation and identity. Suggestions included using wallets to store and manage identity information securely, with features like granular consent and selective disclosure to protect privacy. There was agreement that privacy-enhancing technologies, like zero-knowledge proofs, could be crucial in the future of identity wallets.

Presentation about Biometric Key Management

- **Question**: One of the participants asked if splitting a transaction into two stages (ordering and authorizing with a fingerprint) could be considered similar to a biometric-bound wallet.
- **Answer**: The presenter clarified that biometric-locked wallets activate a stored key with biometrics but do not directly generate signatures from the biometric data, as biometric-bound wallets do.

Appendix E

BGIN Block#11

BGIN Block#11 MR Wallet Governance

Wallet Governance

Date: Monday, October 22, 2024

Location: Washington DC, United States

Duration: Approx. 90 minutes

Summary

Biometric Key Management

© BGIN – All rights reserved

Question 1:
What are biometric schemas, and is it possible to read them?

Answer:
Biometric schemas are specific files designed for secure storage of biometric data. The technology to read these schemas is typically proprietary, making it challenging to access or use them outside of their intended systems. Even if the schema data were leaked, it would be difficult to interpret or use effectively without the proprietary technology.

Question 2:
How is a biometric different from data like a Social Security number?

Answer:
Unlike data such as a Social Security number, which is standalone, biometric data relies on physical traits like fingerprints. Even if the biometric data were leaked, linking it back to an individual is more complex, adding a layer of security.

Question 3:
Does using biometric security decrease the convenience of wallet use?

Answer:
Yes, using biometric data can reduce convenience, as users must go through additional verification steps. However, biometric-bound wallets do not store the biometric data directly but rather derive public information from each interaction, which is not stored anywhere. This setup reduces privacy risks but can impact usability.

Question 4:
Could biometric authentication alone achieve complete security?

Answer:
Biometric authentication cannot completely eliminate error rates, so alternative solutions like multi-factor authentication should be considered for critical systems. Relying solely on biometrics may not be sufficient due to the inherent limitations in biometric data accuracy.

Question 5:
Do you use only fingerprint data to generate the signing key, or is additional information required?

Answer:
This depends on the biometric signature scheme in use. Some systems, like Hitachi's, use only fingerprint data, while others might incorporate additional "helper data." This helper data does

© BGIN – All rights reserved

not contain confidential information and cannot reconstruct the original biometric information, serving only to enhance security.

Question 6:
What about the potential risks of losing biometric data or parts of the body associated with it?

Answer:
If someone loses the part of the body used for biometric authentication (like a fingerprint), they could lose access to the wallet. Biometric security represents both a strength and a weakness, as it is unique to the individual. Future technologies, including generative AI, may potentially reconstruct biometrics, which would be a security challenge if biometrics are the only form of authentication.

Question 7:
How is entropy managed in biometric-based signature schemes to maintain security?

Answer:
Maintaining high entropy in biometric signatures is essential for security, and although biometric systems have some entropy loss, it is necessary to have alternative systems or multi-factor authentication to reinforce security.

Question 8:
Could biometric-locked wallets be combined with other key management methods?

Answer:
Yes, biometric-locked wallets could support additional key management methods. For instance, a wallet could use biometrics for low-value transactions while requiring multiple authentication factors for higher-value transactions. This tiered approach could balance security and convenience.

Question 9:
How do biometric systems handle minor alterations in biometric data, like slight changes in fingerprints?

Answer:
To account for variations, biometric systems use "helper data" that compensates for minor differences in biometric information. This helper data adjusts for small discrepancies in features, allowing the biometric data to match without needing exact replication.

Question 10:
Is there any need for external storage in biometric-bound wallets to handle data fuzziness?

© BGIN – All rights reserved

Answer:
Typically, external storage for keys is unnecessary because biometric-bound wallets incorporate procedures like activation and matching stages. These processes align registration data with real-time biometric data, enabling secure key generation without storing extra data externally.

Accountable Wallet

Question 1:
Will the accountable wallet concept create a duality in the ecosystem, possibly affecting fungibility, like pricing differences between accountable and non-accountable Bitcoin?

Answer:
Yes, introducing accountable wallets could lead to a division in the ecosystem between accountable and non-accountable systems. This has raised concerns about potential differences in the pricing of accountable versus non-accountable tokens, such as Bitcoin. This impact on fungibility was a major topic at the Bitcoin Tokyo event.

Question 2:
How can we build incentives for using accountable wallets?

Answer:
Positive ecosystem inclusion may serve as an incentive, as users often want to participate in trusted environments. This could create a "snowball effect," making accountable wallets essential for accessing certain financial opportunities, thus encouraging their use.

Question 3:
What role could accountable wallets play in decentralized finance (DeFi), specifically in compliant, walled gardens?

Answer:
Accountable wallets could be instrumental in creating compliant, walled gardens within DeFi. By using block filters, transactions from sanctioned ecosystems could be identified, supporting reputation-based incentives, reducing business risks, and benefiting individual investors.

Question 4:
Will accountable wallets ease or increase user responsibility for privacy management?

Answer:
Expanding privacy management responsibilities onto users does add to their burdens. However, accountable wallets could mitigate this by offering incentives to users who take ownership of their data, potentially shifting privacy management to a beneficial, positive-sum outcome where users gain from their data control.

© BGIN – All rights reserved

Question 5:
Could accountable wallets benefit validators in addition to Virtual Asset Service Providers (VASPs)?

Answer:
Yes, users and validators could benefit if transactions are validated using accountable wallets. However, there are concerns around centralization, as seen with F2Pool's decision to exclude flagged transactions based on sanctions, which was criticized for its centralized approach. Accountable wallets should ideally support decentralized, individual decisions rather than relying on centralized control.

Question 6:
Is there a way to avoid centralization issues when implementing accountable wallets?

Answer:
One potential solution is creating an association set where accountable wallets only interact with transactions mined by particular relayers compliant with sanctions like OFAC. This decentralized approach could combine accountable wallets with privacy pools and compliance-focused tools, such as NEV (non-extractive value) bots, rather than relying on centralized entities.

Question 7:
Will users voluntarily adopt accountable wallets to avoid association with harmful activities?

Answer:
Voluntary adoption may be challenging, as many users don't prioritize privacy, and avoiding illegal involvement may not be a strong enough motivator. Some believe enforcement may be necessary to ensure widespread adoption, although the concept could gain acceptance over time by providing a whitelist for exclusive opportunities, such as airdrops or new token access.

Question 8:
How complex would it be to implement accountable wallets, and what compliance measures would be needed?

Answer:
Implementing accountable wallets might require extra steps, like signing an additional transaction or querying an on-chain registry for compliance verification. Although this could increase development complexity, these steps could be worthwhile for enhancing user security and preventing negative interactions.

Question 9:
Can an accountable wallet be revoked, and would monitoring be necessary?

© BGIN – All rights reserved

Answer:
Revocation does not necessarily require monitoring. Accountability could decay over time, with recent transactions holding higher legitimacy. Wallet holders could refresh their legitimacy through continued control. If a bad actor takes over, a trusted third party could revoke the wallet's attestation, isolating the issue to that specific instance.

Question 10:
How would the system handle the steady state of an accountable wallet, especially if a bad actor later misuses it?

Answer:
The system would need real-time reputation decay, allowing users to refresh their reputation through control retention. If a bad actor assumes control, a third party could revoke the wallet's token, possibly impacting related attributions and discouraging misuse over time.

© BGIN – All rights reserved

Appendix F- suggested (mitchell) furtherance of the paper and study.

AI Agents and Sovereign AI: The Critical Role of Wallet Governance

The Emerging Landscape of Autonomous Digital Actors

As AI systems become increasingly autonomous, we are witnessing the emergence of "Sovereign AI" agents capable of independent decision-making, transaction execution, and digital asset management. These systems represent a fundamental shift in digital identity and governance participation, creating unprecedented opportunities alongside complex accountability challenges.

AI agents are already operating within blockchain ecosystems through automated trading, DeFi optimization, DAO participation, and cross-chain operations. The trajectory toward Sovereign AI involves agents controlling substantial portfolios, making complex decisions, and operating across multiple domains with minimal human oversight.

Wallet Governance Implications

Authentication and Authorization Challenges

Traditional wallet governance assumes human users with predictable patterns. AI agents introduce new complexities:

Identity Verification: New frameworks must address cryptographic proof of AI agent authenticity, verification of authorization to act on behalf of principals, and mechanisms to distinguish authorized operations from system compromises.

Delegation Frameworks: Clear structures must define the scope of AI authority, human override mechanisms, time-bound limitations, and procedures for updating permissions.

Risk Management and Accountability

Operational Risk: AI agents introduce unique risks including algorithm malfunction, adversarial attacks, market manipulation, and cascade failures when multiple agents respond to identical signals.

© BGIN – All rights reserved

Legal Accountability: Current frameworks struggle with determining liability for AI decisions, KYC/AML compliance for AI-initiated transactions, cross-jurisdictional enforcement, and insurance mechanisms for AI-related losses.

Enhanced Governance Participation

AI agents could revolutionize governance through continuous monitoring, rapid response to time-sensitive decisions, complex multi-criteria analysis, and coordination across multiple systems. This enables new governance models including AI-mediated consensus, hybrid human-AI governance, and real-time policy adaptation.

Technical Framework Requirements

Multi-Layer Security Architecture

Effective AI agent governance requires:

1. **Human Authorization**: Cryptographic proof of principal authorization
2. **Scope Limitation**: Technical enforcement of authority boundaries
3. **Audit Trails**: Comprehensive logging of decisions and actions
4. **Emergency Controls**: Fail-safe mechanisms for immediate intervention

Interoperability Standards

AI agents operating across networks require:

- Universal identification standards
- Cross-chain permission verification
- Standardized delegation protocols
- Interoperable audit frameworks

Privacy and Transparency Balance

AI agents need protection of operational parameters while maintaining accountability through zero-knowledge proofs of compliance, selective disclosure to authorized parties, privacy-preserving audits, and standardized public reporting without revealing sensitive strategies.

Suggested Roadmap

© BGIN – All rights reserved

Phase 1 (Current-2025): Basic authentication standards, simple delegation frameworks, monitoring tools, regulatory dialogue

Phase 2 (2025-2027): Cross-chain identity standards, advanced risk management, governance participation protocols, liability frameworks

Phase 3 (2027+): Fully sovereign operations within bounds, AI-native governance systems, global oversight standards, advanced privacy-preserving accountability

Critical Success Factors

Success requires technical excellence in security architectures and interoperable standards, regulatory alignment through proactive engagement and clear liability structures, and community acceptance through education and transparent development processes.

The Sovereign AI Network will need good wallet governance

The emergence of Sovereign AI represents one of the most significant developments in digital economies. As AI agents gain capability to manage substantial resources and make consequential decisions, today's wallet governance frameworks will determine whether this transformation enhances human prosperity or creates systemic risks.

Effective governance requires reimagining digital identity, authorization, and accountability with AI-native frameworks that scale with advancing capabilities while maintaining human oversight. Well-governed AI agents could democratize sophisticated financial strategies and enhance governance participation. Poorly governed agents could concentrate power and undermine decentralized principles.

The convergence of AI and blockchain is inevitable. Our task is ensuring governance frameworks harness benefits while protecting against risks through cooperation between technologists, regulators, and society. The wallet governance decisions we make today will shape tomorrow's digital economy, requiring us to prioritize security, accountability, and human agency to create a future where Sovereign AI enhances rather than replaces human decision-making.

© BGIN – All rights reserved

Appendix G - Key Artefacts List and References:

1. BGIN Block #9 Panel Discussions
    a. Wallet Governance and Key Management
2. Interviews
    a. MPC Technology Providers
    b. Zero-knowledge technology providers
    c. Digital asset custody
    d. Wallet and DAO governance
    e. Standards setting Foundations
3. Working Group discussions.

Links and References

https://www.coinbase.com/blog/digital-asset-management-with-mpc-whitepaper

https://vitalik.eth.limo/general/2023/06/09/three_transitions.html
https://vitalik.eth.limo/general/2023/02/28/ux.html

https://openwallet.foundation/
https://identity.foundation/working-groups/wallet-security.html
https://medium.com/@identitywoman-in-business/exploring-approaches-to-digital-wallets-c1824c90480a

Footnotes (wallet hacks section)

1. https://www.coindesk.com/parity-unfreezes-ethereum ↩
2. https://www.coindesk.com/understanding-dao-hack-journalists ↩
3. https://www.coindesk.com/tech/2021/08/10/poly-network-hacker-returns-260m-in-funds-following-610m-exploit/ ↩
4. https://www.coindesk.com/quadrigacx-creditors-are-owed-190m-court-filing-shows ↩
5. https://www.coindesk.com/eth-2-0-staking ↩
6. https://cointelegraph.com/news/crypto-wallets-where-to-start ↩
7. https://www.coindesk.com/mark-karpeles-mt-gox ↩
8. https://www.coindesk.com/yam-finance-defi ↩
9. https://cointelegraph.com/news/uni-scams-net-criminals-340k-in-defi-boom ↩
10. https://www.coindesk.com/electrum-wallet-attack-may-have-stolen-as-much-as-245-bitcoin ↩
11. https://www.coindesk.com/bitfinex-bitcoin-hack-know ↩

© BGIN – All rights reserved