IsoWallet

Building a Safer Web3

March 1st, 2022

Abstract

Current blockchain wallets are inadequate. Users are effectively forced to choose between sacrificing on security, by using a hot wallet, or sacrificing on accessibility, by using a cold storage/multi-signature wallet. Hot wallets are highly susceptible to malicious attacks, and by simply clicking on a phishing link, the user can find the contents of their wallet emptied. Cold storage and multi-signature wallets on the other hand restrict the user's ability to move their assets, and often require an additional piece of hardware in order to secure the wallet. IsoWallet will provide users with a new option. By isolating the user's sensitive data from major attack vectors, IsoWallet will be the first software wallet that provides the same level of security as a cold wallet, without compromising on accessibility.

Table of Contents

Introduction **3**

State of Wallets **3**
- Software Wallets 3
- Hardware Wallets 4
- Multi-Signature Wallets 4

IsoWallet **5**
- Security Design 5
- Trustless Transactions 7
- Education 7
- Insurance 7
- User Experience 8

Business Landscape **8**
- Competition 8
- IsoWallet Advantage Matrix 10

Key Team Members **10**

Roadmap **10**

Conclusion **12**

Introduction

Blockchain technology is one of the safest technologies for ensuring legitimacy of data transference. It enables users to send information to trusted sources with records and assurance that, if the address one enters is correct, the blockchain will enable its safe arrival to the sender's target destination. Applications that interact with blockchains, however, are not necessarily safe. To hack and alter the Ethereum network would be immensely difficult. By contrast, to hack a device or application interacting with the Ethereum network is rather simple. One of the primary applications that interact with blockchain networks are wallets. Blockchain wallets are applications that allow users to store the public and private keys of their wallet, in order to access their digital assets, and effectively act as the gateway into Web3. A vast majority of DeFi and NFT market participants use wallets to store and access their assets, with the total number of blockchain wallets surpassing 80 million. As the Web3 market grows, the number of wallet users will as well. Additionally, the number of individuals who store a majority of their net worth in their wallets versus traditional bank accounts will grow as well. Wallets are also required in order to access many Web3 ecosystems. NFT marketplaces, DeFi exchanges, Metaverses, as well as a majority of NFT projects all require a blockchain wallet in order for one to gain access. As a result, blockchain wallets have become perhaps the most important application in Web3. Considering the importance of blockchain wallets, application security should be the top priority for developers. However, this has not been the case.

State of Wallets

Software Wallets

The most popular software wallets are browser extensions. A browser extension provides seamless accessibility for the user, however, its security architecture is tremendously lacking. The fundamental flaw with its design architecture is that the internet browser must be a trusted environment through which to access data. The browser, however, is the primary attack vector for black-hat hackers. While convenient,

browser extensions do not sufficiently isolate a user's sensitive data from the browser, and as a result leave wallets susceptible to compromise. Additionally, well-crafted, socially engineered phishing scams are a common threat to current software wallets. Social media is littered with seemingly innocent links which, if clicked on, will release malware that can result in complete loss of funds from a user's wallet. Even a novice hacker with little technical skill can penetrate a wallet by simply purchasing exploit kits on the web that enable software wallet theft. As a result of the lack of emphasis on security, a simple online search can present a plethora of social media posts by wallet users reporting that their wallets have been hacked, and their funds stolen.

Hardware Wallets

For those who prioritize security, the most popular wallets have been hardware wallets. Hardware wallets are designed to store the users' private keys offline and as a result reduce the risk of the wallet being hacked. However, there are trade-offs. The primary trade-off is that funds are not consistently accessible to the user. The user has to purchase an additional piece of hardware and must carry the hardware with them in order to access their funds. This is especially inconvenient for active market participants, and those who spend a significant amount of time outside of their home. Another trade-off is that hardware wallets operate on a trust model. The user must trust the environment with which they are interfacing in order to access their funds, or risk compromising the wallet's security. If the machine, browser, or application are compromised then the users' funds can be stolen, even with a hardware wallet. Lastly, the user must ensure the safety of the physical piece of hardware. If the hardware itself is physically damaged, defected, or misplaced, then the contents of the users' wallet are lost.

Multi-Signature Wallets

Multi-Signature wallets are blockchain wallets that require two or more private keys to sign and send a transaction. Since they require multiple private keys, they provide a higher level of security relative to browser based wallets. In order to utilize the

security benefits of a multi-signature wallet, the user must have multiple devices, each with a different private key. These wallets are often used by institutional investors and centralized exchanges due to their heightened level of security, however they are impractical for the average wallet user. They require the user to sign from multiple devices for each transaction, thereby requiring the user to sacrifice on speed and accessibility. Additionally, the average wallet user will find it onerous to have to sign on from multiple devices for each transaction. This is especially an issue for those who are active market participants. Another issue with multi-signature wallets is the lack of a backup mechanism. If the user loses a private key and the associated seed phrase, then the user loses access to the wallet entirely. These accessibility requirements make multi-signature wallets highly inefficient for the average wallet user.

In summary, there is currently no blockchain wallet which provides high accessibility for the user, without compromising on security.

IsoWallet

Security Design

IsoWallet follows the **Prevention**, **Detection**, and **Response/Recovery** model in order to provide best in class endpoint protection for Digital Assets.

Prevention: IsoWallet's security architecture philosophy is premised on security through isolation and compartmentalization. The benefit of isolating and compartmentalizing assets is that if one storage location is compromised, all is not lost. In computation, isolation is achieved through physical or virtual isolation. Physical isolation means having separate devices, like a hardware wallet. In physical isolation, if one device is compromised, the other device is less likely to be affected. Virtual isolation means having separate virtual environments that share one piece of hardware. Similar to physical isolation, if one virtual environment is compromised, the other is less likely to

be affected. IsoWallet achieves isolation by compartmentalizing the internet access point and key storage into separate environments. This ensures that if one clicks on a potentially malicious link in the IsoWallet browser, deactivating the malware will be as simple as closing and reopening the browser. Given that the browser environment is designed to isolate and dispose of any active malware, if used properly, your keys will be consistently safe.

Detection: Social engineering is hard to prevent without user education. IsoWallet aims to provide users with anti-phishing capabilities, natively within the app. This will include user prompts to recognize a non-whitelisted website to remind the user that the site they are interacting with might be malicious. IsoWallet's future updates will include Artificial General Intelligence implementation that would be able to detect malicious web pages natively in the IsoWallet web browser. We will be further implementing an intrusion detection system that will alert the user of any potentially suspicious activity on their application.

Response/Recovery: We have two plans for response and recovery. Firstly, we intend to enable users to backup their seed phrases and private keys in a zero-knowledge based cloud environment. This enables users to access their keys in the event of machine compromise or if they choose to use other blockchain wallets. Additionally, after extensive testing, we intend to offer private insurance for users' IsoWallet contents.

Trustless Transactions

IsoWallet's Trustless Transaction feature will enable users to trade any smart contract, blockchain-based digital asset through a middleman smart contract to facilitate ease of peer-2-peer trading. Without an intermediary smart contract, both parties have to trust that the other party will deliver on their terms of the trade. However, with IsoWallet's Trustless Transactions, parties can send their assets to a middleman smart contract and the assets will only be released when both parties have deposited the

required asset. IsoWallet users, who are not technical, will be able to set up and use their own Trustless Transaction smart contract natively, and with ease, from within the app.

Education

Along with an exceptional wallet, IsoWallet will also provide vast educational materials for its users. IsoWallet will have an Education Team whose task will be to create comprehensive educational materials to assist users in navigating Web3. Examples of these materials are:

- Introductory information on Blockchain; including Cryptocurrency, DeFi, and NFTs.
- Information on how to purchase digital assets.
- Best practices for security in Web3.
- How to spot potentially fraudulent projects in Web3.
- And much more.

As more people enter Web3, these kinds of educational materials will be necessary for them to make a smooth transition into this space. IsoWallet aims to assist in that transition by providing users with all the information necessary to make Web3 a fun and safe experience.

Insurance

IsoWallet plans to offer in-app insurance to its users. Users will have the ability to opt-in to an IsoWallet insurance policy that will reimburse the user for lost funds, should there be a coverage trigger. Details regarding the insurance feature offered by IsoWallet will be provided in future updates.

User Experience

IsoWallet's user experience will be highly intuitive and easy to use; great for newcomers and blockchain veterans alike. This user experience will also include dedicated User Support Teams that will be available 24/7 to ensure user satisfaction.

IsoWallet will also provide a variety of features to enrich user experience. Including:

- Support for all Ethereum Virtual Machine (EVM) compatible layer 1 networks.
- Support for layer 2 networks.
- Support for non-EVM compatible networks such as Bitcoin, Solana, Cardano and Terra Luna.
- The ability to trade on decentralized exchanges such as, UniSwap, SushiSwap, and PancakeSwap, natively in-app.
- Comprehensive NFT and DeFi token support.

Business Landscape

Competition

MetaMask: Metamask is a software wallet that is compatible with Ethereum Virtual Machine ("EVM") based blockchains. MetaMask protects its user's data through a single password. Hackers take advantage of this security design by sending phishing links to wallet users. If clicked on, these links enable remote access for the hacker. The hacker can then either find the user's password, guess the user's password, or release a key-logger that records and sends the user's password to the hacker. Once the hacker has successfully entered the MetaMask account, almost nothing can be done to protect the user's funds.

TrustWallet: TrustWallet is an exclusively mobile application that enables access to EVM compatible blockchains. TrustWallet suffers from the same threat profile as MetaMask due to its similar design.

Exodus: Exodus is a software wallet that lives outside of one's browser as a desktop and mobile application. However, its security architecture is limited to a single password which makes it highly vulnerable to password-cracking and phishing attacks.

Ledger: Ledger is a hardware wallet that allows users to store digital assets offline. It is the most popular hardware wallet on the market, however it suffers from all the same tradeoffs as other hardware wallets, including: low accessibility, and requiring the user the trust the ecosystem that Ledger is interacting with.

Trezor: Trezor is a hardware wallet that allows users to store digital assets offline. Although it provides increased security, it suffers from the same tradeoffs as Ledger and other hardware wallets.

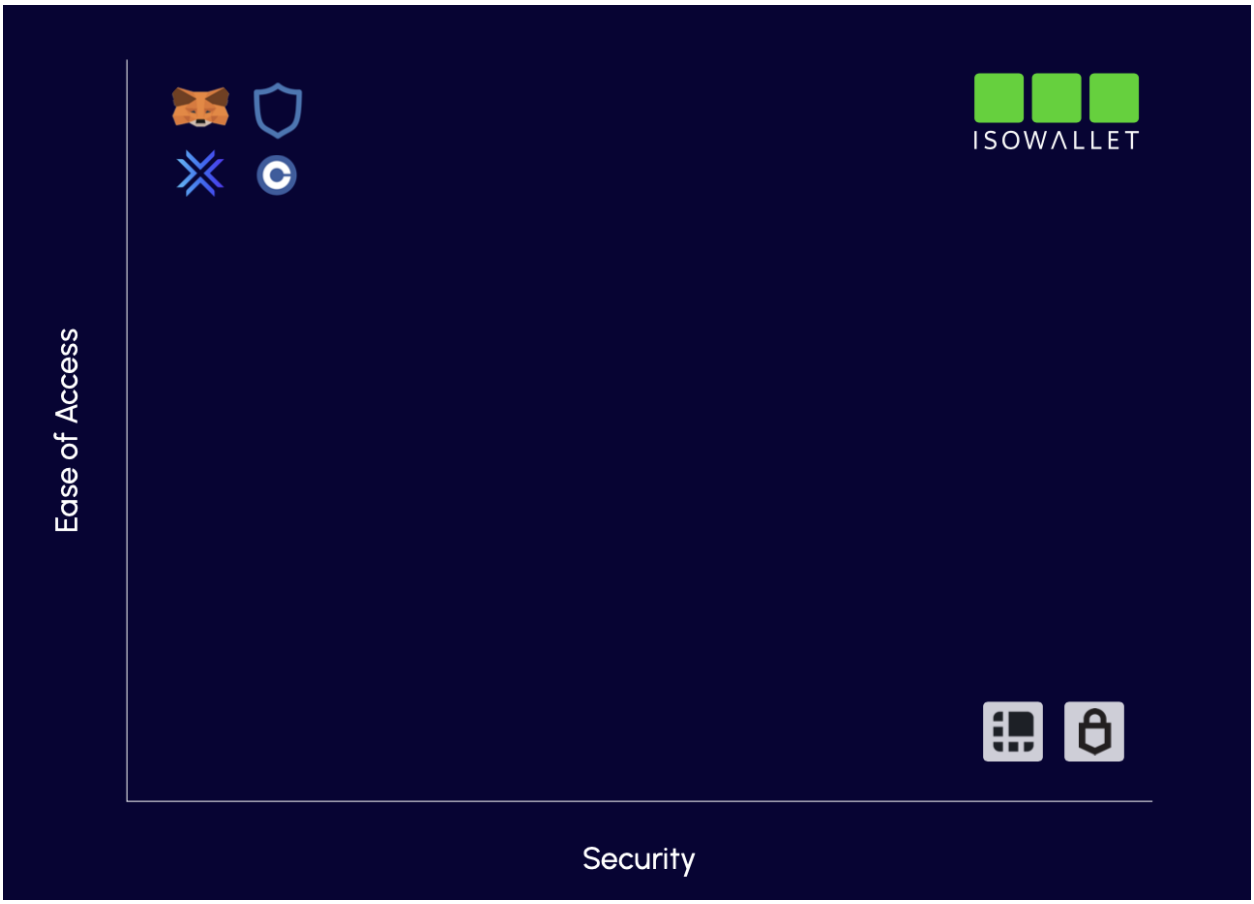

Figure 1. Competitive Matrix

IsoWallet Advantage Matrix

Present Wallet Ecosystem	IsoWallet
Lack of Security	Cutting-edge security
Low Accessibility	High Accessibility
Poor User Experience	Intuitive User Experience
Poor User Support	Dedicated Support Team for Users
Lack of Innovation	Continuous Innovation
No Options for Trustless Transaction	Trustless Transactions
No In-Wallet Insurance Offering	Will Offer In-Wallet Insurance
Lack of Education for New Users	Will Provide In-App Education Materials

Key Team Members

- David Elhadad, Partnerships. Law, Finance and Blockchain.
- Mike Feldman, Operations. Blockchain and Cybersecurity.
- Cullon Hecox, InfoSec. Lockheed Martin.
- Hartley Deare, Tech. Software Development. Google.
- Don Daskalo, Design. Founder of Don Daskalo Design.
- Rachel Lichtman, Advisor. Founder of Lichtman Law.

Roadmap

Phase 1 - Community Building

- ○ Build a passionate community that believes in the IsoWallet vision.

Phase 2 - Development

- ○ Team Expansion
- ○ Wallet Development

Phase 3 - Nearing Minimum Viable Product

- ○ Red teaming/infrastructure stress testing + security audit

- Strategic Partnerships

Phase 4 - Beta Release

- Bug bounty hunting program
- Implementing community feedback

Phase 5 - Official Launch

- Wallet launch
- Implement trustless transaction feature

Phase 6 - Development

- Improve wallet based on feedback
- Enterprise solution development

Phase 7 - Enterprise Solution Launch

- Continue to improve wallet
- Prepare insurance offering

Phase 8 - Insurance Launch

- Offer in-app insurance for users

Conclusion

Blockchain wallets are lacking. Current wallet options force users to choose between security and accessibility. By creating an isolated ecosystem for its wallets, IsoWallet is advancing an innovative software wallet that provides a similar level of security as a hardware wallet, without sacrificing accessibility. In addition, IsoWallet will provide novel features such as trustless transactions, in-app educational materials, and wallet insurance. In conclusion, IsoWallet not only aims to be the best wallet on the market, but to also act as a safe and efficient gateway for all to access Web3.