Soverance: An Anonymous Hardware Wallet Solution

soverancelabs.com

Abstract:
Soverance presents an innovative downloadable hardware wallet solution tailored for the secure cold storage of digital assets. The core breakthrough lies in the development of our system, designed to breathe new life into outdated mobile devices by seamlessly integrating the SoveranceOS, effectively superseding the Android operating system. This integration serves a dual purpose: it isolates the device from the internet, thereby mitigating potential vulnerabilities, and eradicates the Android framework, which had previously hosted data harvesting functionalities.

Our approach leverages an anonymous transaction script, in conjunction with a Zero Knowledge protocol, wherein recipient wallets function as unique access codes to discreetly acquire the Soverance package. This innovative methodology circumvents the necessity for Know Your Customer (KYC) procedures, a requirement imposed by prominent competitors in the hardware wallet domain, which often inadvertently expose sensitive user information such as usernames, addresses, emails, and financial details.

Notably, we refrain from storing user data in databases, ensuring a robust shield against third-party compromises. This transactional paradigm effectively erects a wall of anonymity between any external entity, including Soverance itself, and the user. Consequently, Soverance establishes an exclusive wallet management solution that operates beyond the purview of any entity other than the user, thus ensuring the utmost privacy and security.

Introduction:
Know Your Customer (KYC) procedures have stirred debate within the cryptocurrency community, primarily due to their perceived intrusion into users' privacy. The very essence of Bitcoin's inception was to usher in a decentralized, peer-to-peer transactional paradigm that empowers individuals to maintain their privacy while executing transactions, eliminating the need for intermediaries. However, the current trajectory in the hardware wallet arena entails an unnecessary accumulation of user data, encompassing government-issued identification, physical addresses, names, email addresses, and even photographic records, thus steering humanity toward a critical juncture. This trajectory risks compromising the fundamental principles upon which the digital realm was established, inadvertently providing malicious actors with potentially sensitive information.

As any seasoned cryptocurrency enthusiast understands, KYC stands in direct contrast to the ethos of the crypto space, where privacy is paramount. Soverance's software solution has been

meticulously crafted with a singular goal in mind: to afford every individual the means to securely safeguard their assets, all while prioritizing affordability and sustainability.

The linchpin of our security paradigm is anonymity. By ensuring that the existence of the device remains concealed beyond the user's realm of comprehension, we preemptively mitigate liability from the very moment of conception, well before utility is even a consideration. This foundational principle is central to our mission, and we invite you to delve deeper into the innovative world of Soverance as we embark on this journey toward redefining digital asset security.

Problem Statement:
The existing hardware wallet market, though crowded with numerous players, suffers from fundamental deficiencies in three crucial dimensions: **security**, **accessibility**, and **ethics**.

Security is the paramount concern when it comes to hardware wallets. Historically, the practice of connecting a hardware wallet to a hot device, such as a commonly used smartphone, computer, or tablet, poses severe risks to user security. Shockingly, a staggering 75% of all Internet of Things (IoT) devices are infected with keylogging malware, including devices linked to major data accumulators like Google, Facebook, AWS, iCloud, and home routers. This alarming statistic highlights the dire vulnerability of private data to potential breaches, compromising the very essence of cryptocurrency security. The gravity of the situation is further exacerbated by the exploitation potential of devices tied to cell phone numbers, exemplified by the NSO Group's notorious software package, Pegasus, utilized by state-run intelligence organizations globally.

Accessibility to secure hardware wallets is another pressing issue. Currently, the price range for such devices spans from $39.99 to a whopping $400 per unit, with an average price point hovering around $120. To put this into perspective, the average global monthly salary stands at $1,480. However, in the bottom 129 countries, the average monthly income falls below the $120 mark. This means that the majority of the world's population, including countries like India ($2,150 per year), Pakistan ($1,470 per year), Nigeria ($2,080 per year), Bangladesh ($2,570 per year), and Ethiopia ($940 per year), cannot realistically afford even the median hardware wallet cost on a monthly salary after factoring in basic living expenses. This poses not just a challenge for economically disadvantaged individuals, but a systemic risk for all stakeholders in the burgeoning Web3 space. As hot wallets become increasingly vulnerable and subject to security breaches, cryptocurrency assets may inadvertently flow back into exchanges, triggering a detrimental chain reaction that depresses prices and jeopardizes the security of digital assets for everyone.

Moreover, **ethical** concerns loom large over the hardware wallet industry. Purchasing these devices necessitates users to surrender personal information such as their name, address, email, and bank account details to secure their device. This data, in the hands of sellers, creates a digital ledger connecting users' identities, financial institutions, and residences, presenting a treasure trove of information to potential malicious actors. Given that the user base of these devices often comprises individuals seeking refuge from failing fiat-based regimes and advocating for decentralization, these users could potentially become targets of retroactive scrutiny by authoritarian governing bodies. The methods employed by every hardware wallet manufacturer on the market not only fail to address the inherent issues of security, global accessibility, and ethical considerations but actively counteract the very purpose they purportedly serve – providing a secure means to safeguard decentralized wealth.

At the core of the cryptocurrency movement lies the aspiration to decentralize global power structures by establishing a trustless medium of exchange, free from the influence of monolithic, privacy-invading, centrally-aligned governments and institutions. However, when governments and private industry entities collaborate to consolidate control, offering the means to achieve their respective objectives where legal avenues fall short, the specter of fascism looms. Placing one's wealth on a cold storage wallet that collects user data, including their name, address, date of birth, email, and bank details, effectively strips individuals of their most critical asset – anonymity. Inaccessibility further compounds the problem, preventing the majority of the world's population from securely holding their wealth in a rational format. Compounding these issues, vulnerabilities in current hardware wallet solutions far outweigh their utility. The imperative of providing an anonymous cold storage solution that encompasses security, global accessibility, and ethical principles is not only viable but encapsulated in Soverance. We are committed to delivering sovereignty to all.

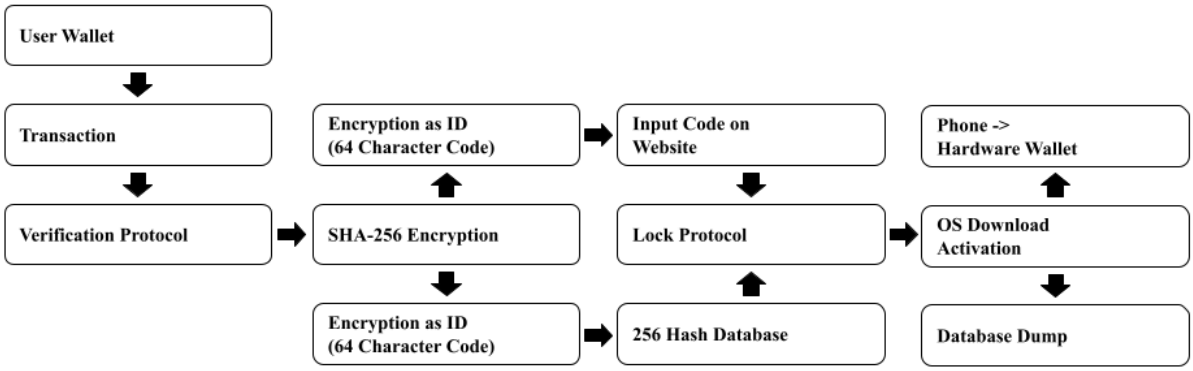
Soverance Anonymous Transaction Protocol:
The Soverance transaction protocol has been meticulously designed to ensure the absolute preservation of user anonymity. It commences with the user initiating the initial transaction, which serves the dual purpose of procuring a software license. Upon receipt of the transaction, the protocol proceeds to record the wallet details while concurrently converting the associated amount into USD for reference.

The wallet data then undergoes a transformation through a robust SHA-256 hash function, creating an encryption referred to as the "output" or "code." This code is systematically logged within the system. To facilitate the download process, the user undertakes a verification step where they copy and paste their wallet into a SHA-256 calculator, generating an identical code.

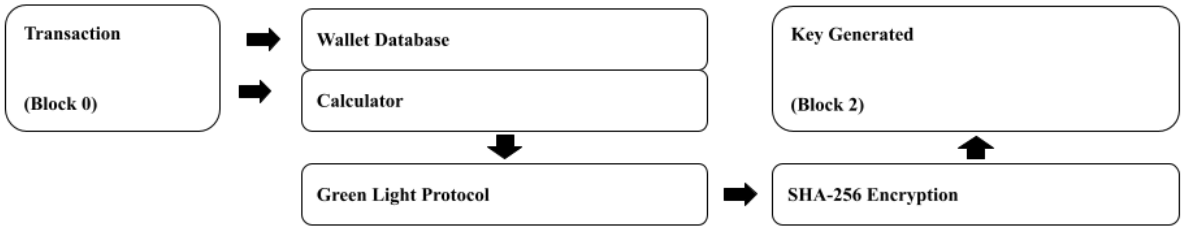
The user subsequently submits this output code through the designated website interface. The protocol meticulously scrutinizes the provided code, verifying two crucial conditions. First, it

confirms that the token value aligns precisely with the USD price. Second, it ensures that the wallet encryption log perfectly matches the code input on the website. Only when both criteria are met does the download process commence, ensuring the utmost security and accuracy in the transaction process.

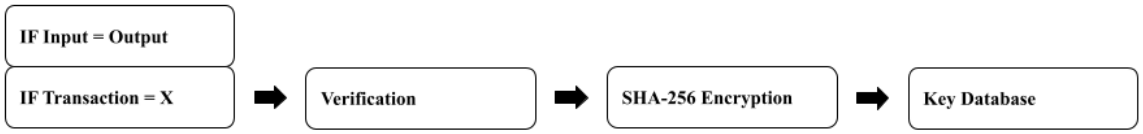
Visualized Transaction Script:



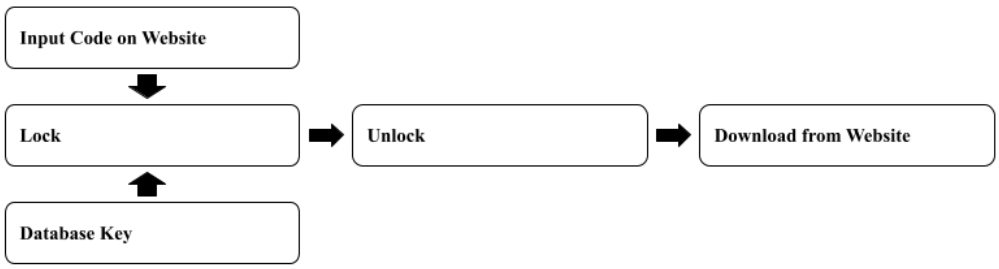
Verification Protocol:



Green Light Protocol:



Lock Protocol:



Soverance Transaction Process - Website & User Steps:

1. **[User]:** The transaction is initiated by the user.
2. **[Website Script]:** The verification process is initiated.
    a. **[Website Script]:** Payment information is logged in the database.
        i. **[Website Script]:** The payment calculator verification system is engaged.
            1. **[Website Script]:** The Green light protocol validates the transaction.
    b. **[Website Script]:** Wallet details are recorded in the database.
        i. **[Website Script]:** Wallet address undergoes SHA-256 encryption to generate a unique key.
        ii. **[User]:** The user copies their wallet address and applies SHA-256 encryption to generate a matching key on the website.
        iii. **[Website Script]:** An active database is subjected to the lock protocol.
        iv. **[User]:** The user inputs their generated key into the lock protocol.
            1. **[Website Script]:** The lock protocol verifies the key for single-use validity.
    c. **[SoveranceOS Script]:** The SoveranceOS commences the download process.
        i. **[Website Script]:** The SHA-256 key is securely disposed of.
        ii. **[User]:** The user selects their preferred platform for download, either iOS or Android.
        iii. **[SoveranceOS Script]:** The SoveranceOS completes the download process.
3. **[User]:** The user proceeds to utilize the SoveranceOS device for secure cryptocurrency management.

SoveranceOS:

The Soverance operating system represents a distinct Android-derived stack, downloadable with the primary objective of transforming your device into an anonymous wallet management platform. The prevailing issue in the current hardware wallet landscape revolves around the integration of these wallets with hot devices, typically daily-use cell phones or internet-connected computers. These hot devices are predisposed to a plethora of data-tracking services, encompassing entities such as Google, Facebook, and even potential surveillance by government agencies like the FBI. Furthermore, mobile phones, in particular, are susceptible to a gamut of privacy-infringing services, including cellular triangulation, GPS tracking, and the notorious PEGASUS exploit, among others, which not only trace your digital footprint but also your physical whereabouts.

By erasing the pre-existing software and installing the SoveranceOS, which intentionally lacks any internet connectivity, we achieve a state of absolute data security. The SoveranceOS is a highly customized system that achieves anonymity by stripping away all extraneous

functionalities, leaving only the essential components necessary for the device to function as a wallet manager while completely eliminating internet access.

From this juncture, it is important to note that the user assumes responsibility for any vulnerabilities associated with their chosen hardwired synchronization method. For enhanced security, we recommend employing an external node, ideally a second-hand computer procured from a reputable source, and connecting it to a privately-owned modem. This setup ensures a higher degree of control and mitigates the risks associated with internet-based vulnerabilities, thereby providing a more secure environment for managing your digital assets.

Soverance Base Code and Compatibility:
The foundation of the Soverance codebase is drawn from Android Studio, specifically utilizing the Android OS 8 for its core functionality. This choice stems from the desire for a neutral and adaptable codebase that can be easily manipulated to suit our unique requirements.

One notable advantage of our system is the ability to access reversion capabilities directly through the SDK (Software Development Kit) tools. These tools have been thoughtfully updated to accommodate the reversion of the latest Android OS releases. It's important to emphasize that while compatibility with new Android OS releases may necessitate periodic updates, the fundamental Soverance base code remains resilient and unaffected by these Android updates. This distinction ensures that the core principles of security and anonymity inherent to Soverance remain intact, irrespective of the evolving Android landscape.

Soverance Marketplace:
Soverance stands as the definitive privacy wallet solution, meticulously designed to address the prevailing security vulnerabilities within the hardware wallet ecosystem. Empowering individuals to securely store their cryptographic assets is the foundational step in our mission to extend Sovereignty to all. However, facilitating secure and anonymous asset trading represents the logical progression in achieving this goal.

The Soverance marketplace is conceived as an internal software update, distinguishing itself from the conventional decentralized exchange (DEX) model. Instead of establishing a DEX, our approach centers on the implementation of a cutting-edge Zero-Knowledge (ZK) peer-to-peer trading system, operating within a framework of end-to-end security. This innovative marketplace solution not only enhances the privacy and security of asset trading but also ensures that the Soverance ecosystem remains at the forefront of technological advancements in the blockchain space.

Definitions:

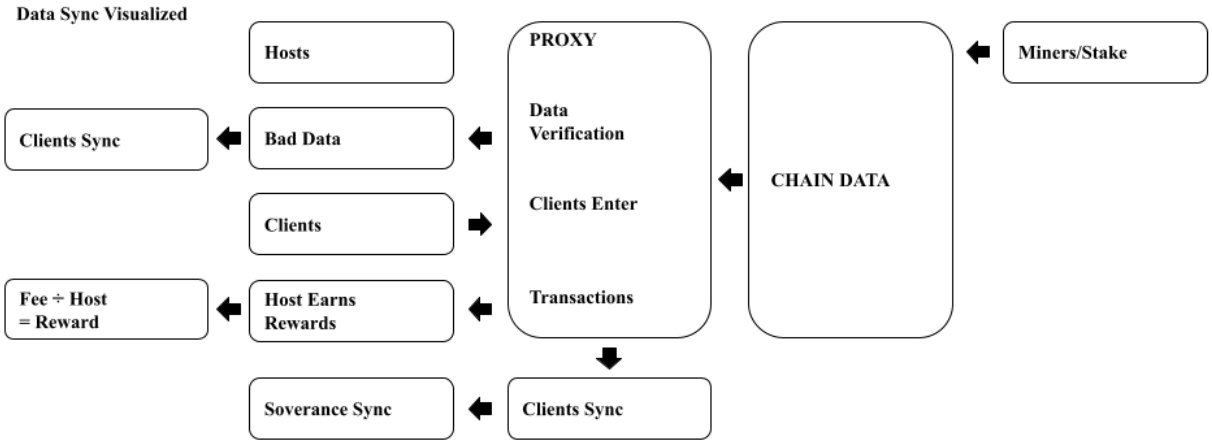
Wallet 0 refers to the main, cold storage wallet for long term digital assets holdings. The main function of Wallet 0 is to deep freeze your holdings which would disable movement to other wallets. These wallets are designed to operate within an internal KYC-free cold storage system, prioritizing the utmost security and privacy of digital assets, requiring a password prior to movement.

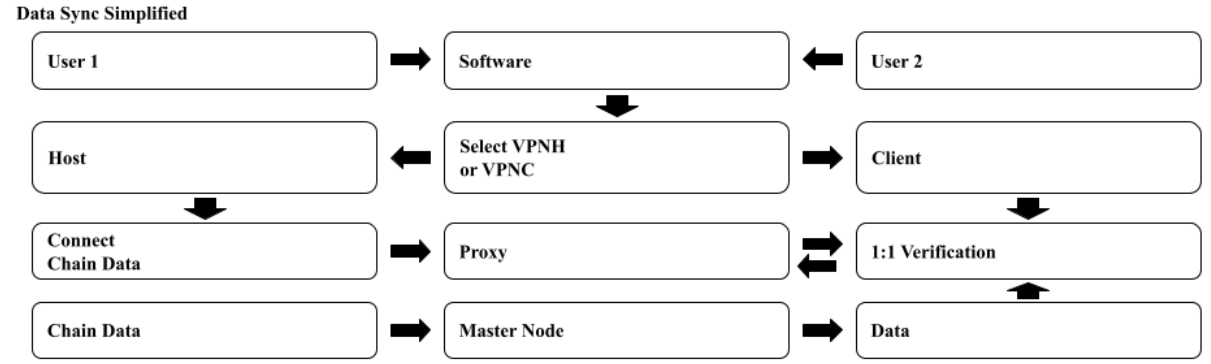
Wallet 1 represents a hot wallet, which is a generic type of cryptocurrency wallet. Hot wallets are typically connected to the internet and offer quick access to digital assets for everyday transactions. Comparatively, to wallet 0, wallet 1 allows for a gateway into and out of the Soverance system.

T-Wallet, Short for Temporary or Tachyon Wallet, is a specialized wallet characterized by timer-based functionality. These wallets are specifically designed for the purpose of facilitating key exchanges within a predetermined time frame, offering a unique and time-sensitive approach to enable inter-wallet trades similar to a marketplace. Through facilitating the desired parameters, without on chain data recording the swap since no assets appear to change hands.

SoveranceVPN:
In order to guarantee the online safety and privacy of Soverance users, we introduce SoveranceVPN—a decentralized Virtual Private Network service meticulously designed to preserve 100% anonymity for our users. This innovative VPN service operates as a multi-computer node chain, offering participants the opportunity to earn yield by hosting synchronization data and collecting transaction fees within an anonymous proxy server. Importantly, this system ensures the verification of chain data without the exposure of users' IP addresses to the public.

The core functionality of SoveranceVPN operates in synergy with both mining data and on-chain data. Relay nodes integrated within the VPN infrastructure are cross-referenced with external blockchain data to provide secure and anonymous transactional data. This intricate interplay ensures that SoveranceVPN remains at the forefront of safeguarding user privacy while enabling users to actively participate in the network and earn rewards for their contributions.





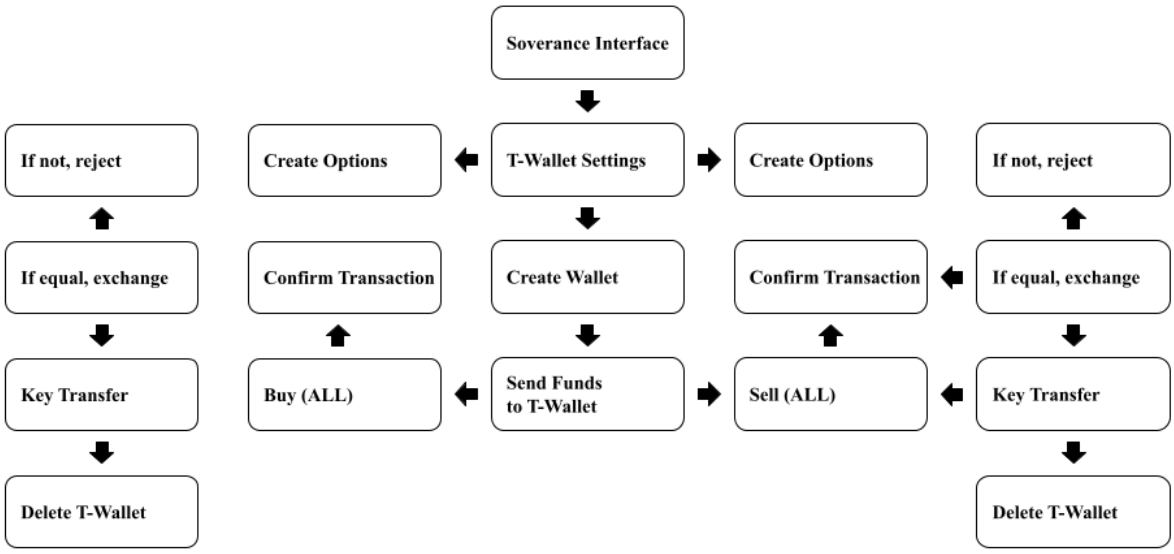
How It Works - Host:

1. Users download the VPN software via the anonymous transaction script accessible at soverance.org.
2. The node system is initiated through the software, effectively creating a VPN infrastructure.
3. The software provides users with the option to act as either a host (VPNH) or a client (VPNC).
4. Hosts initiate the setup process, either by creating a new proxy or joining an existing one. The proxy is responsible for managing chain data synchronization. Users can select the protocol of the listed blockchain chains they wish to synchronize with.
5. Hosts launch the VPNH (VPN Host) module, marking their participation in the network.
6. To become a VPNH and earn rewards, the host must engage in tasks such as mining the blockchain and directly transmitting data or having a means to relay data in real-time.
7. VPNHs with similar tasks are interconnected, forming a collaborative proxy server.
8. The VPNs act as gateways to the proxy, providing a tunnel that shields users from ISP detection.
9. The proxy breaks down data into smaller bits for transmission through the network of nodes, ultimately reaching their designated endpoints.

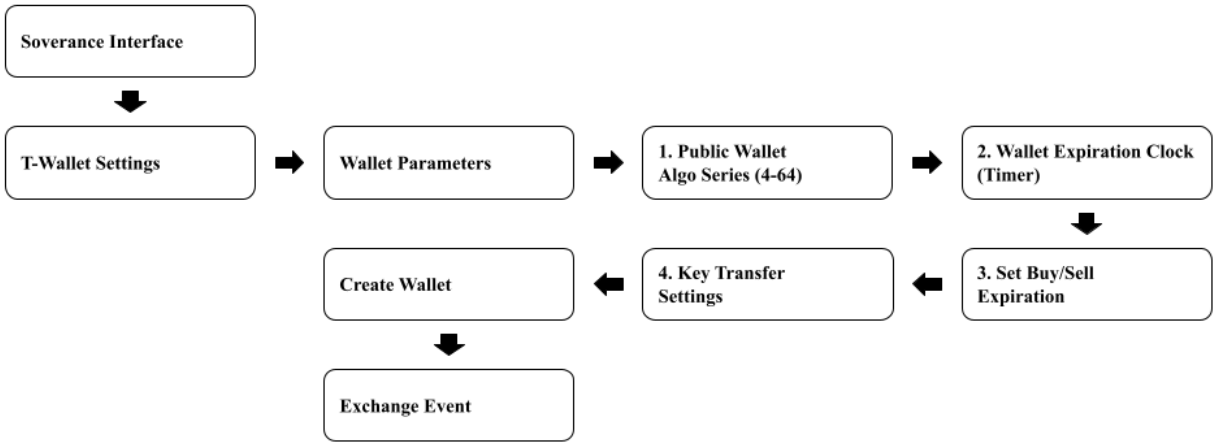
How It Works - Client:

1. The client configures an encryption cipher for secure data transmission through the software portal.
2. The client activates the VPNc (VPN Client) module and selects the desired proxy for connection.
3. Two or more nodes combine to form an "anonymous bitproxy."
4. Upon connection, a key exchange takes place using the Diffie-Hellman key exchange method, securing the connection between the client and the proxy.
5. The client establishes a secure connection to the selected proxy.
6. When a search is initiated by the client, the request is sent into the bitproxy.
7. The bitproxy divides the search request into nodes, and VPNP (VPN Proxy) hosts retrieve the requested data.
8. Data retrieved by VPNP hosts returns to the bitproxy, where it is assembled correctly using the corresponding encryption key.
9. The data then exits the bitproxy and enters the VPNp (VPN Proxy) for decryption.
10. Finally, the software decrypts the data, making it accessible to the user who can view the results.

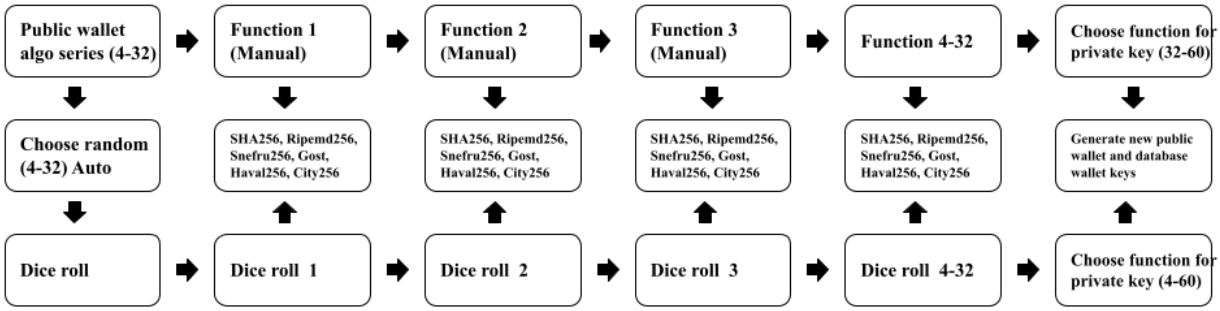
Temporary Wallet Creation & Transfer Mechanism:



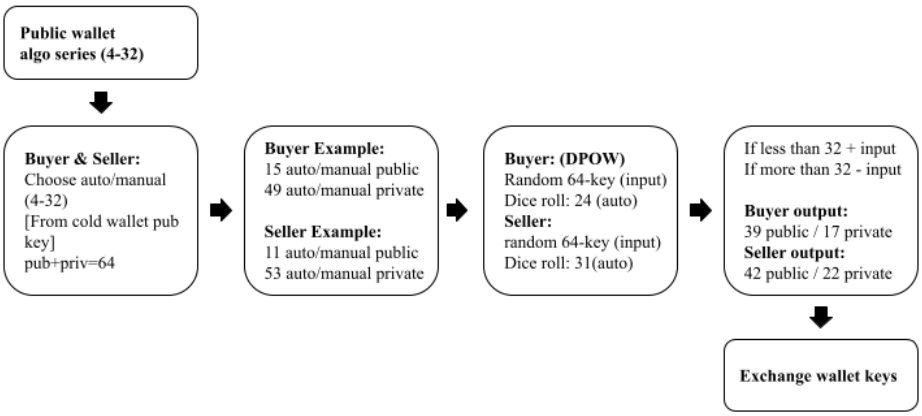
Wallet Settings:



Public Private Wallet Algorithm Series:



Key Transfer Settings:



Ensuring True Chain Data:
To maintain the integrity of chain data synchronization, the proxy is connected to live chain data whenever feasible. Data that is inaccurate or unreliable is systematically filtered out, and any IP addresses associated with misleading or incorrect data are banned from the server. This meticulous process fosters the development of a decentralized synchronization system that enhances the trustworthiness and reliability of the network.

Conclusion:
The SoveranceOS package represents the ultimate, completely anonymous endpoint for safeguarding an individual's sovereign digital wealth. With a foundation rooted in the use of anonymous transaction scripts fortified by Zero-Knowledge (ZK) protocols, the Soverance package remains exclusively known to the user. It not only offers unparalleled versatility, outperforming any manufactured hardware device in the cryptocurrency space, but also possesses core competencies that surpass any market share holder, both past and future.

Through the integration of the SoveranceVPN and the Soverance marketplace, this decentralized finance (De-Fi) ecosystem achieves full anonymity, encompassing the entire spectrum from cold storage security to secure trading. Privacy and data security are the central pillars of our product, a design philosophy that aligns with the earliest principles of the cypherpunk movement.

As the cryptocurrency space gradually faces regulatory scrutiny, the imperative for a system like Soverance becomes undeniably clear. Instances of government overreach and mounting evidence of corruption have reached unprecedented levels. In this landscape, Soverance stands as the indispensable solution for safeguarding your digital net worth, ensuring the utmost security, anonymity, and sovereignty in the ever-evolving world of digital assets.

SoveranceOS Derivative OSS Stack:
https://developer.android.com/studio
https://developer.android.com/tools
https://github.com/CalyxOS
https://github.com/GrapheneOS
https://github.com/mycelium-com/wallet-android
https://github.com/horizontalsystems/unstoppable-wallet-android
https://github.com/Blockstream/green_android/
https://github.com/EdgeApp/edge-react-gui
https://github.com/cypherstack/stack_wallet
https://github.com/secretkeylabs/xverse-web-extension
https://github.com/LedgerHQ/OUTDATED_ledger-wallet-android
https://github.com/DcentWallet
https://github.com/Okx

https://github.com/keepkey/keepkey-firmware
https://github.com/trezor/trezor-firmware
https://github.com/Blockstream/Jade
https://github.com/LedgerHQ/nanos-nonsecure-firmware-releases