Warm Wallets: A Safer Design to Achieve Business Automation for Blockchain-Based Services

A Novel Wallet Implementation Strategy for Enhancing Blockchain-based Online Services Security

Filippo Bosi, Michele Cappelletti, Guido Ravagli, Lorenzo Manzoni, Stefano Monti, Emanuele Pagliara
Imola Informatica
Imola (BO), Italy
e-mail: {fbosi, mcappelletti, gravagli, lmanzoni, smonti, epagliara}@imolainformatica.it

***Abstract*—Blockchain wallets are the user-facing, public/private key storage and signing/verification part of blockchains. Different architecture styles and hardware/software components are available on the market, with different trust and accessibility levels. This paper presents a novel wallet approach that fuses the accessibility benefits of online wallets with the security of air-gapped, cold-storage based wallets.**

Keywords-Blockchain; wallet.

I. INTRODUCTION

Blockchains are rapidly gaining momentum as a revolutionary architecture style that opens up novel, fully decentralized, trusted interaction schemes and unprecedented, unexplored business opportunities.

Blockchains rely on asymmetric cryptography schemes to sign transactions, and to guarantee immutability (i.e., once written to the blockchain, transactions cannot be altered) and non-repudiability (i.e., transactions cannot be entitled to users other than the one that originally signed the transaction).

Blockchain wallets are software/hardware components that act on the user side and offer: 1) blockchain connection facilities, 2) storage of users private/public key pairs, and 3) signing and verification features via the above private/public keys.

Different wallet styles and offering are available on the market, with different degrees of trust, accessibility, and convenience [1]; however, the most diffused solutions usually require relevant tradeoffs for users: online wallet services are the most convenient and accessible type (with supposed always-online availability), but require users to trust third party providers to hold their private keys (hence virtually being able to act on behalf of users themselves). Offline, air-gapped software/hardware components are supposedly the most secure solutions [3], but pose accessibility and convenience limitations.

This paper highlights the main wallet architecture styles, and proposes a novel, hybrid approach – called warm wallet – that aims at maximizing trust, convenience, and accessibility.

The rest of the paper is organized as follows. Section II describes blockchains and wallet alternatives. Section II surveys the main requirements and principles in designing blockchain wallets. Section IV describes warm wallet architecture and relevant implementation insights. Section V concludes our work with some hints at future work and research directions.

II. BACKGROUND

A. Blockchain and wallets

A wallet in a digital money world has the same issues of a wallet in real life. First, it must be secured, as if anybody has access to it, all the money contained in the wallet is at his/her complete disposal. Conceptually speaking, blockchains and wallets are secured with a single private key. If someone knows the private key, they have fullcontrol on the amount of money it holds. It is the owner's responsibility to put in place good security practices in order to secure the money.

A digital coin wallet is like a wallet with cash: people would not keep a large amount of cash in their pocket if they do not need it. In general, it is good practice to keep on the server only the amount of digital money needed for everyday use, that is, the amount of money usually needed for running the service for a reasonably long amount of time. The rest of the funds should be kept in a safer place, moving them to the online service only when necessary to refill the wallet in order to run the service without interruption.

B. Wallet alternatives

Hot wallets [3] are the simplest form of wallet since the private key is kept directly within the software wallet itself. While conceptually simple to manage, hot wallets provide a low level of trust, since compromising them means having the same direct, complete access to information (wallet status and balance) and features (e.g., signing transactions) as the owner himself/herself.

Hardware wallets [3] rely on dedicated devices that a) store owner private key in a (supposedly) tamper-proof, confidential way, and 2) sign transactions that are candidate to be placed on a blockchain, hence making them non-repudiable by the owner himself/herself. Hardware wallets usually have no mechanisms to directly interact with

 ISBN: 978-1-61208-644-6

blockchains and limit themselves to return the signed transaction; other pieces of software are then in charge of actually interacting with the blockchain. Cold storage and removable media can be used as a stripped-down hardware wallet whose sole responsibility is to safely keep a copy of the private key, and that delegates signature features to other pieces of software.

Multi-signature [3] wallets are designed to sign a transaction with multiple private keys at the same time, thus raising the challenge for transaction forgery. Each private key can be managed with different privacy and visibility strategies, and with different hardware/software components.

Cold storage [2] wallets hold the private key on air-gapped storage, i.e., an offline device/software component that is meant to always remain physically disconnected from the Internet. Cold storage wallets are able to sign transactions with the private key, but need to rely on stripped-down, secondary wallets to interact with the blockchain to initiate and receive transactions. Passing a signed transaction from the offline cold wallet to its online counterpart requires some kind of physical interaction to cross the "air gap" between the two.

Custodial wallets and Web wallets [3] are usually online, third party services that are supposed to 1) maintain private keys on behalf of their owners, and 2) allow users to operate on the blockchain (e.g., signing transactions) by interacting with functionalities exposed by such services, e.g., Application Programming Interfaces (APIs) or Web interfaces.

Paper wallets are physically printed versions of private keys (and any other user-related information): paper wallets obviously have no signing feature, and can be physically stored safely offline.

III. PRINCIPLES AND REQUIREMENTS

Choosing the right wallet architecture style for a blockchain-based application largely depends on business requirements rather than strictly technical considerations. The main driver usually is accessibility and business continuity. Cold storage wallets represent the most tamper-proof kind of wallet, since physical access to the medium is required to conduct any kind of attack. However, physical network disconnection becomes cold wallets most relevant drawback when business automation and continuity are at stake. The other key driver in wallet choice is trust and reliability: third party providers offer users the key features to store public/private key pairs, and sign/verify transactions; this approach, however, let malicious sysadmins (or any other malicious user that could gain privileged access) surreptitiously register transactions on behalf or real users. Main Bitcoin blockchain frauds, such as Mt. Gox hacker attack that led to roughly 630,000 bitcoins stolen, and ultimately determined Mt. Gox bankruptcy [6], relied exactly on stolen public/private key pairs from the provider hot wallets.

The cornerstones of cold wallet superior [2] security mainly relate to:

- Separation between private and public key;
- Separation between signing and verification functions.

Cold wallets implement such separation via a physical segregation (air-gap) of hardware/software components, and relegate signing functions (together with the necessary private key) to offline components.

Relaxing the physical segregation principle challenges wallet security, since, depending on the degree of connection and intercommunications, opportunities arise to access the private key (and associated signing features) via the online-facing public key holder logic component.

In our vision, however, such relaxation can

- Lead to strong benefits in terms of accessibility and business continuity;
- Be mitigated via usual security countermeasures and isolation principles (such as firewalling network connections, and running least-privileged processes).

The next section presents a warm wallet architecture and a proof-of-concept implementation that demonstrate the viability of a cold storage wallet that abandons physical air-gapping, in favor of logical separation and technical isolation.

IV. DESIGN AND IMPLEMENTATION

A. Warm wallet architecture

Conceptually warm wallet architecture relies on two logical components:

- Signing Wallet: offline (i.e., disconnected from the blockchain) component that holds user private key and transaction signing feature;
- Watching Wallet: online component that retains user public key and operates against the actual blockchain of choice.

This design strategy is independent from the actual blockchain implementation used to implement the online service. The following subsection deepens the description of implementation details of a first proof-of-concept warm wallet for Bitcoin blockchain.

B. Warm wallet implementation

The first consideration to take into account when building a blockchain wallet relates to how this component interacts with the blockchain itself. In the case of a Bitcoin blockchain wallet, the most straightforward way is to leverage a full Bitcoin Core node – a fully functional Bitcoin node – and leveraging its native signing, verification, and transaction registration facilities. Bitcoin Core nodes, however, are resource-expensive, both in terms of dedicated hardware requirements, and of runtime memory and CPU consumption.

This ruled out this design choice from the beginning, and we had to design an alternative solution. Simplified Payment Verification (SPV) [4] is a means to implement a

 ISBN: 978-1-61208-644-6

lighter-weight Bitcoin blockchain node that downloads only minimal transaction information, and retrieves full transaction details from blockchain nodes when in need.

Specifically, SPV clients only download the headers of blocks, and then request transactions from full nodes as needed; this approach allows computation cost to scale linearly with the height of the block chain, hence resulting in a more viable option, cost-wise.

We implemented the wallet in Java language, via the BitcoinJ library [5].

V. CONCLUSION

This paper presented an architecture solution to mix online, hot wallet accessibility and convenience, with the trust and security of air-gapped cold wallets. We are adopting this approach in some real-world, business cases of blockchain adoption outside of the traditional finance/cryptocurrency area, and specifically related to the tracking of supply chain goods. This approach is proving itself beneficial in terms of business continuity, convenience, and accessibility. Future work will focus on defining tools and best practices to guarantee logical network disconnection (e.g., enforcing specific software firewall rules) from the online and offline wallets parts, so that adopters of warm wallets are not forced to implement their own solutions.

REFERENCES

[1] S. Eskandari, D. Barrera, E. Stobert, and J. Clark, “A First Look at the Usability of Bitcoin Key Management,” Proceedings of the NDSS, Workshop on Usable Security (USEC), 2015

[2] M. Draupnir, “Bitcoin cold storage guide,” Available: https://www.weusecoins.com/bitcoin-cold-storage-guide/, 2016

[3] M. Conti, S. Kumar E, C. Lal,S. Ruj. A Survey on Security and Privacy Issues of Bitcoin
https://arxiv.org/pdf/1706.00916.pdf

[4] Simplified Payment Verification [Online] Available from: https://bitcoin.org/en/developer-guide#simplified-payment-verification-spv. Accessed on 2018-05-29

[5] BitcoinJ [Online]. Available from: https://bitcoinj.github.io/ Accessed on 2018-05-29

[6] The Inside Story of Mt. Gox, Bitcoin's $460 Million. [Online] Available from: https://www.wired.com/2014/03/bitcoin-exchange/ Accessed on 2018-05-29

 ISBN: 978-1-61208-644-6