securosys

White Paper

SECUROSYS

Optimally Secured Blockchain Environments

Address

Förrlibuckstrasse 70
8005 Zurich
Switzerland

Phone & Fax

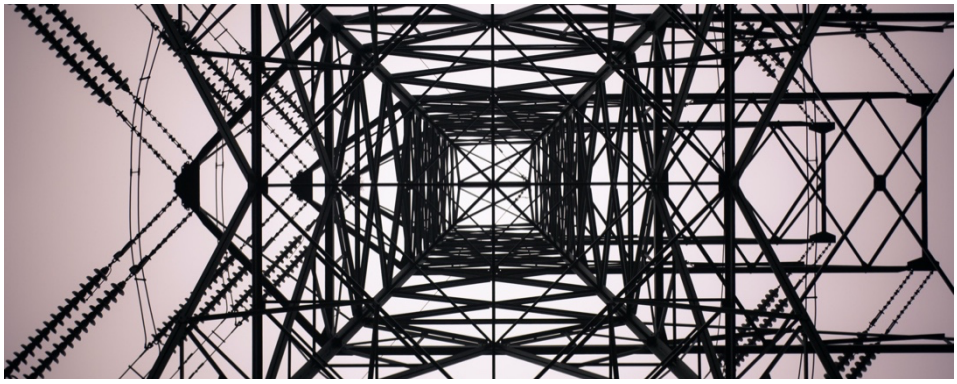
Phone: + 41 44 552 31 00
Fax: + 41 44 552 31 99

Email

Email 1: info@securosys.com
Website: www.securosys.com

Table of Content
Whitepaper

01. Introduction



Securosys is raising the bar for maximally secure asset management by introducing an advanced layer of blockchain-enhanced protection for execution of applications operating on separate, server-based enclaves.

Blockchain has the nearly unlimited potential to transform the ways in which organizations share data and transfer monetary values. Yet for all the promise that this futuristic technology holds, questions still linger surrounding its possible security and regulatory challenges.

If widespread adoption of blockchain for the transmission and settlement of financial payments is to occur, especially for organizations utilizing regulatory and compliance applications, its security must be impermeable.

While the blockchain technology underpinning distributed ledgers is already proven to be highly secure, concerns remain about how best to protect both the blockchain applications and the cryptographic keys that allow access to the ledgers themselves. For blockchain technology to reach its maximum potential, it must meet—or exceed—currently accepted security standards.

Definition of Blockchain

Blockchain technology is an undeniably forward-thinking invention, created in 2009 by the imagination of a mysterious person or group of people collectively known by the alias, Satoshi Nakamoto [i]. Since its inception, the technology is consistently evolving into something much more significant for use across a broad range of business and industrial applications. For organizations that have yet to take advantage of this innovative technology, the main question that often leaves them mired in unending procrastination seems to be: What is blockchain?

By allowing the distribution without direct duplication of digital information, blockchain technology is creating a new and revolutionary additional branch of the Internet. Initially devised for the cryptocurrency Bitcoin, the technology is now extremely popular within the high-tech community for its virtually unlimited potential involving maximized security and authentication of related financial

The management of assets and the individual asset owner

Whether an individual asset owner or a group of various co-managers within an organization are responsible for maintaining the financial portfolio, Blockchain technology allows the asset-controlling members to keep a detailed digital ledger containing all historical transaction data. Its use of private keys for signatory authentication further allows these members to update their digital ledgers with integrity and a significantly enhanced degree of nearly untouchable security. Because of blockchain technology, asset owners and managers are no longer dependent upon third-party authorization services.

A blockchain possesses unique, broker-free (P2P-based) characteristics, which allow the asset controllers to forego those often expensive and now-unnecessary fees related to P2P transactions requiring prior authorization by a third party. Since ownership of the transaction capabilities and their related data lies with the asset owner or multiple owners/managers, hacking and possible theft of assets from unknown attackers becomes increasingly more difficult.

An organization which assigns asset management and manipulation capabilities to multiple people saves additional money in security expenses and updates while also enhancing the speed, reliability, and efficiency of each financial transaction. Meanwhile, IT architects can implement, connect, and even expand blockchain systems with ease, and companies can make transaction records openly accessible to the public or pre-designated government agencies which also reduces regulatory costs[ii].

Blockchain Technology
Security Concerns

Blockchain technology is a highly structured platform with characteristics similar to a distributed database. But what exactly are the security concerns?

Blockchain is specifically designed to make arbitrary manipulation impossible because all network participants must verify and save the updated blockchain with each manipulation or transaction. Each block is a separate structure that contains the hash values of the previous and current blocks. Since the hash values stored within these blocks are directly affected by the values of the previous blocks, potential hackers find falsifying or altering the often enormous amounts of necessary signed data impossible.

A linked hash table combined with the use of public, key-based verification protocols is the basis of blockchain security. The Elliptic Curve Digital Signature Algorithm (ECDSA) verifies the digital signature generated during an asset transaction to essentially prove that the transaction data is reliable and unaltered.

While an anonymous public key can allow someone outside the participating group to determine the amount and the probable locations of the financial transactions, it does not allow the discovery of pertinent information related to the asset owner(s) or participating manager(s).

However, data alteration and even possible asset theft are conceivable in cases where controlling or stealing of 51% of the peers' private keys occur simultaneously. For this reason, owners and managers of digital assets are quickly learning a very valuable lesson. Regarding the prevention of digital financial manipulation, the security of the private keys is fundamentally more crucial than the protection of the digital assets themselves.

Smart Key Attributes (SKA)

When, it comes to digital assets, not having an additional blockchain security layer means death.

Smart Key Attributes (SKA) for optimal transaction security

In theory, conventional server environments utilize key generation and storage solutions where the asset keys never leave the hardware- or software-based infrastructure. However, if a hacker or other unauthorized person gains access to the server environment or even the related partition, the safety of the stored asset keys becomes immediately compromised. Not only can the hackers identify the individual keys, but they can also identify where to use them and with which assets.

The crypto currency is not the asset. The KEY is the asset.

The best practice resolution of these types of high-risk security challenges is the fundamental principle behind the revolutionary and patented Securosys SKA technology. Smart Key Attributes assignments involving secure rules and filters for authentication of company and compliance requirements help organizations safeguard their assets and financial transitions well beyond the capabilities of a conventional server-based infrastructure.

Application and use cases

Regardless of the business or industry, different applications typically require varying levels of security enforcement protocols. Therefore, some automatically require more complex key usage controls depending on the related business processes. Common use cases include individual signature keys, such as with electronic digital signature services, and multi-key access related to electronic seals, which typically require multiple signatures by two or more parties.

Other applications might include:

- **Digital signature** (signing service with authorization)
- **Digital seals**
- **Timed approvals**
- **Multiple signatory access for different timeframes** (for example, the acquiring of three out of five digital signatures within a four-hour timeframe or the acquiring of a single digital signature from a possible six different persons within a weekly timeframe)
- **Multiple signatory access for different departments** and/or groups within a single business entity (for example, the acquiring of digital signatures from the Board of Directors, the Chief Financial Officer, and perhaps the Purchasing Department Manager).
- **Signing payload comparisons** to prevent misuse of the signatory operation

02. Benefits of blockchain versus software-based security

Perhaps the best-known uses of blockchain technology include those related to the implementation, transaction, or realization of cryptocurrencies. However, even in these most common usages, various security issues still exist relating to the blockchain agreement, transactional capabilities, funding, withdrawing, wallet manipulation, and the associated software through which these manipulations occur. By assigning unique and customizable rules or filters to each associated private key, these security risks diminish substantially.

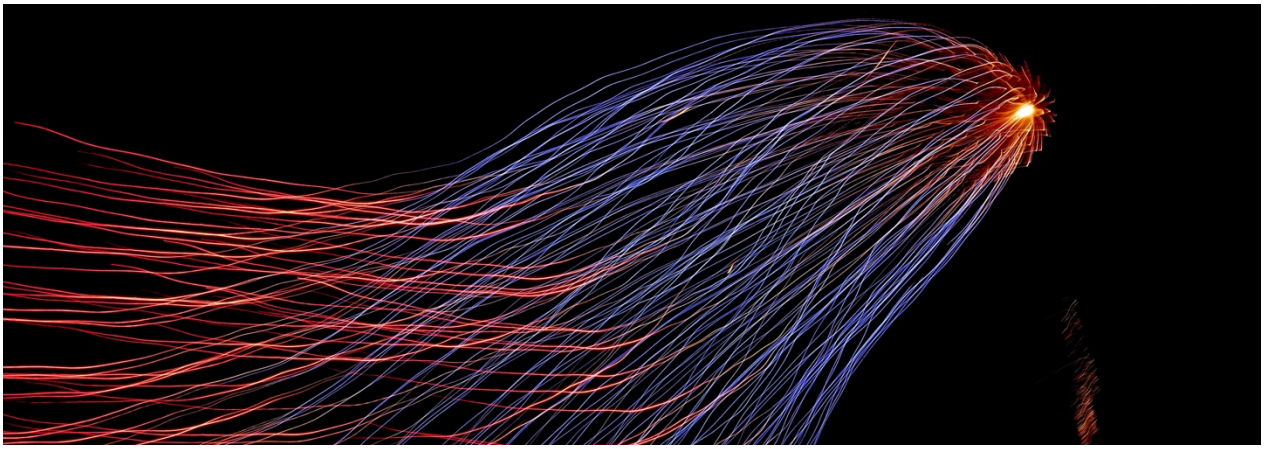
Here is a short list of advantages of SKA-enhanced blockchain technology.

Prevention of loss or theft of private keys

A Public Key Infrastructure (PKI) consists of a set of individual keys with various independent capabilities, such as data encryption, authentication, and other pertinent functions.

The most crucial individual key in the PKI hierarchy is the root key whose most common purpose is to authenticate and sign digital certificates, like a Certificate Revocation List or CRL.

However, requesting a new root key is a very labor-intensive process, especially if the connected digital assets are under the control of multiple signatories. Before the introduction of SKA technology by Securosys, all responsible co-signers would typically be required to meet physically in the same geographic location to manually sign a hardcopy agreement to revoke the stolen key. With the Securosys SKA multi-signatures feature, the entire process can take place virtually, instantaneously, and with maximum security.



Security of transactions

Regardless of whether the storage of assets takes place on virtual or hardware-based technology, every financial transaction requires two "addresses." The first address is that of the intended receiver. The second is that of the sender. An address is nothing more than a virtual location consisting of 26-35 alphanumeric characters, somewhat similar to an IP Address. No two wallet addresses are ever identical, and the deletion and regeneration of new cryptocurrency addresses take place with lightning speed.

Digital wallets systematically generate these numerous addresses through cryptographic operations, a software that relies heavily on an asymmetric signature algorithm to generate a public key or "address" that links back to a private key. The user essentially signs or authorizes the transaction to take place with the private key and verifies the signature with the public key.

Therefore, the locking script of a cryptocurrency transaction with an always-unique wallet address as output can be opened using an unlocking script that has the value signed with the personal key of the receiver and/or sender. The digital wallet stores pertinent information, such as the personal key of the address to be used for the generation of the unlocking script. Consequently, an unanticipated loss or corruption of digital wallet data (keys) usually translates to a loss of cryptocurrency wealth. Prime example include the hacking of the decentralised finance (DeFi) platform Polynetwork in August 2021, where hacker successfully stole 600 million USD. In February 2022, Hackers exploited vulnerabilities in the DeFi platform Wormhole that allows users to swap Solana directly for other cryptocurrencies—stealing Ether (Ethereum's native token) worth around USD 325 million. The network was then taken down to investigate the potential bugs and the resulting hack.

For these and many other reasons, digital wallets are increasingly becoming the targets of cybercriminals around the globe. To optimally enhance crypto wallet security, multi-signatory protocols involving multisig only go so far. By providing additional protection against theft or loss through the designation of customizable SKA rules and filters to the wallet's private keys, asset owners and managers achieve the highest possible levels of state-of-the-art security.

Wallets

Security of wallets

Regardless of whether the storage of assets takes place on virtual or hardware-based technology, every financial transaction requires two "addresses." The first address is that of the intended receiver. The second is that of the sender. An address is nothing more than a virtual location consisting of 26-35 alphanumeric characters, somewhat similar to an IP Address. No two wallet addresses are ever identical, and the deletion and regeneration of new cryptocurrency addresses take place with lightning speed.

Digital wallets systematically generate these numerous addresses through cryptographic operations, a software that relies heavily on an asymmetric signature algorithm to generate a public key or "address" that links back to a private key. The user essentially signs or authorizes the transaction to take place with the private key and verifies the signature with the public key.
Therefore, the locking script of a cryptocurrency transaction with an always-unique wallet address as output can be opened using an unlocking script that has the value signed with the personal key of the receiver and/or sender. The digital wallet stores pertinent information, such as the personal key of the address to be used for the generation of the unlocking script.
Consequently, an unanticipated loss or corruption of digital wallet data (keys) usually translates to a loss of cryptocurrency wealth. Prime example include the hacking of the decentralised finance (DeFi) platform Polynetwork in August 2021, where hacker successfully stole 600 million USD. In February 2022, Hackers exploited vulnerabilities in the DeFi platform Wormhole that allows users to swap Solana directly for other cryptocurrencies—stealing Ether (Ethereum's native token) worth around USD 325 million. The network was then taken down to investigate the potential bugs and the resulting hack.

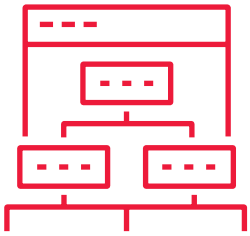
For these and many other reasons, digital wallets are increasingly becoming the targets of cybercriminals around the globe. To optimally enhance crypto wallet security, multi-signatory protocols involving multisig only go so far. By providing additional protection against theft or loss through the designation of customizable SKA rules and filters to the wallet's private keys, asset owners and managers achieve the highest possible levels of state-of-the-art security.

Security of Software

While architects purposefully design server environments to be tamper-resistant, the software that runs on these infrastructures is always at risk of attack by hackers, malicious malware, and ransomware. These conflicting security risks often cause architects to question whether to upload a legacy application or even a single piece of code to a new server structure when either has the potential of already being compromised. Unfortunately, this hypothetical can quickly become a stark reality for many organizations utilizing off-the-shelf hardware with built-in code that has already been hacked.

Security issues like these only prove further that the authenticity of an application must be secured outside of the server environment with a dedicated Smart Key Attest for the application operation. By augmenting systems with SKA technology, architects can implement a separate key store, or at least a hard-coded key within an isolated environment, where no other applications can engage other than the one assigned to and pre-authorized by the Smart private key. Not only will the financial transactions and digital wallets be maximally secure, so will the related software applications through which these transactions travel between two virtual wallet addresses.

Furthermore, even the core software behind the infamous Bitcoin is not entirely exempt from possible software attacks, corruption, and malfunctions. Perhaps the most notorious example is the August 2010 event relating to CVE-2010-5139 [iii] vulnerability. An integer overflow discrepancy allowed remote attackers to bypass economic restrictions on block 74638 and magically created 184 trillion Bitcoins for three different wallet addresses. Two of the addresses managed to secure a whopping 92.2 billion Bitcoins each. The third address and solver of the block received an additional 0.01 Bitcoin.



Enhanced authentication

Another critical aspect of blockchain security relates to the personal keys used in encryption. A typical example of associated cybercriminal behaviors involves a hypothetical attacker successfully gaining access to personal keys stored on an individual's smartphone, laptop, tablet, or personal computer. The hacker might easily acquire this valuable data by merely installing malware on a targeted Smart device.

Until the invention of Securosys Smart Key Attributes, two-factor authentication was considered a modestly effective tool for enhanced protection against unwanted attacks. Yet, cases of malicious codes and malware targeting digital assets are still occurring on a regular basis. Another popular prevention tool is the uploading of a comprehensive cybersecurity and detection software onto Smart technologies of identify attempted installations of malicious code in real time.

Unfortunately, hackers are much faster at creating new forms of malware and ransomware than the providers of these software products can generate and distribute their associated updates. SKA technology provides maximum security for Smart devices, too.

Many forward-thinking organizations are also taking advantage of biometric technologies, such as facial, fingerprint, and voice recognition software, to enhance the security and ease of authentication of various company services accessed via mobile devices. While biometrics is still a rather sensitive topic in some professional circles, the Securosys Smart Key Attributes solution adds an extra layer of security for personal identification metrics — especially when implemented via a personal signature identification software.

Whitepaper
Summary

By augmenting server infrastructures, mobile devices, and digital wallets with the Securosys Smart Key Attributes technology, individual investors, traders, and systems architects can allow strict separation of security and business application functionalities.

Meanwhile, companies gain many previously unavailable security advantages, such as an abundance of various multi-signature capabilities and the increased security of financial transactions, authentication, encryption, and wallet storage. By assigning unique and easily customizable rules and filters to private keys, organizations can even provide optimal protection against hacking attempts of pertinent software by malicious malware and ransomware.

[i] Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. Available online: https://bitcoin.org/en/bitcoin-paper (accessed on 2 September 2019).

[ii] Kaskaloglu, K. Near zero Bitcoin transaction fees cannot last forever. In Proceedings of the International Conference on Digital Security and Forensics (DigitalSec2014), The Society of Digital Information and Wireless Communication, Ostrava, Czech Republic, 24–26 June 2014.

[iii] Block 74638. Value overflow incident bad chain. 2010-08-15. Hash 0000000000790ab3f22ec756ad43b6ab569abf0bddeb97c67a6f7b1470a7ec1c

securosys

Whitepaper Optimally Secured Blockchain Environments

Get more information on our website www.securosys.com

Be digital. Be secure.