WHY BLOCKCHAIN FOR BLOKSEC?

Executive Summary

Blockchains, in general, allow us to keep an auditable, indisputable record of information that is more secure than any centralized record-keeping system.

BlokSec leverages a blockchain to provide auditable, indisputable proof of an authorization record's integrity and identity of origin.

Why is this proof important? If we are to build the next generation of online security, we need overcome the shortcomings of current technology. One of those shortcomings is the vulnerability of centralized data stores to tampering. It is not possible to prove, without a doubt, that the data in a centralized database has not been tampered with because someone with administrative privileges (including hackers who gain that level of access through exploits) could alter data and then remove all traces of having done so. Therefore, when it comes time to prove that someone did authenticate to a system or, more importantly, provided their consent for an important transaction, the current generation of authentication services fall short. All we can do is *trust* that the security practices of authentication providers are strong enough – hence the term "trusted 3rd party".

The most profound quality of blockchains is that they are trustless – a distributed network of nodes leveraging cryptography and consensus protocols can prove unequivocally (in an auditable way that would stand up in court) that data has not been tampered with. This allows BlokSec to provide indisputable records of not only authentication, but also user consent (authorization) for important transactions without needing the reputation nor the massive overhead of companies like Facebook, Google, or Okta. *The technology asserts the security - trust is not required as the system itself is immutable and incorruptible.*

Motivation

When we set out to develop the next generation authentication solution, we knew that we needed a data store that provided much better security than what was traditionally available. What do we mean by security? There are a couple of ways we can think about security of online records: who owns them, who can read them, and who can modify them.

Ownership: whose records are they – who created them?

- Ownership of the record must be maintained in a way that is transparent and immutable, not in a log or table that can be tampered with by system administrators

- Ideally this information is stored alongside the record (in the same datastore) and tamper-proof

Read Access: are records open for all to read, or kept privately? If records should be private, how is access control enforced?

- We do not need to be concerned about this and the system can remain open for all to read so long as no personally identifiable information (PII) is stored within the system, or so long as any such information is sufficiently encrypted that it remains private

Modify Access: how does the datastore ensure that only authorized actors are able to modify data?

- Record modification should be strictly controlled, and the rules about who can write records must be clearly understood and strictly enforced. If it becomes necessary to use records as legal evidence, it must be possible to prove that all modifications were authorized, and to have an auditable and indisputable history of the data (who, what, when)
- This involves proving the identity of those actors as well as the integrity of the records to show that there has been no tampering

Traditionally, centralized databases have been used to store online information. However, they suffer from a glaring problem: if you want to trace the history of a record, you must trust the steward of that centralized database. There is no way to PROVE that the record has not been tampered with. This is one of the main problems that motivated the development of blockchains. In a blockchain, each record carries cryptographic breadcrumbs of the record that came before it, and no change can be made to a record in that chain without breaking the dependencies among records. In this way, it can be proven that records have not been tampered with after being recorded because for such a thing to happen, all records that come afterwards would also need to be modified (and their hashes recomputed) in order to accept the tampered data.

If the cryptography behind blockchain proves this for us, why do blockchains require a network of distributed nodes? By spreading identical copies of the data amongst many nodes and requiring **consensus**, we eliminate the possibility that a single centralized party who has stewardship over the blockchain could manipulate the data to “change history” by re-writing blocks all the way down the chain. If any single node attempted to do this, the cryptographic signatures of its blocks would not match those of the rest of the network, and it would be removed from the set of trusted nodes. With this decentralized stewardship of data, there is no single party who can defeat the preservation of the integrity of the data.

So that takes care of making sure that records are not tampered with, but what about controlling access to who *can* write to records? How do we prove unequivocally the source of these modifications? The answer has two parts. The first part is knowing the identity of the source of the modification; this is called authentication. Once this identity has been established,

the second part is ensuring that they have permission to modify the record; this is called authorization.

For **authentication** we can rely on the service provided by the blockchain itself. Based on digital signatures, it is able to provide cryptographic / mathematical proof that a transaction (that is, a request to modify a record) originated from a particular private key. This cryptographic proof is executed by every node in the decentralized blockchain and consensus of correct signature is required before the record is accepted. This provides proof of possession – only a person in possession of the private key could have correctly signed the message. BlokSec augments this security with an additional check – by securely encrypting the private key with the user's biometry or secret PIN, it provides proof of presence; having possession of the device is not enough – only the person whose fingerprint was originally recorded or who knows the PIN could have created the signature. These two proofs (or factors of authentication) give us assurance of the particular person's identity.

For **authorization** we need to augment the innate logic of the blockchain, which natively accepts transactions from any source. BlokSec creates records of user consent (user consenting to prove their identity, user consenting to having a transaction performed on their behalf, and possibly more in the future), and therefore we need to ensure that only the specific person whose consent has been requested has permission (authorization) to do so. We do this by way of smart contracts – the rules of BlokSec Personal Consent smart contracts state that only specifically allowed identities are allowed to create records of consent. And because the rules of these smart contracts are contained within the distributed ledger of the blockchain, their content and integrity are auditable and indisputable just like all the other records the blockchain contains. Combining the positive identity verification described above with the rules of the Personal Consent smart contract give us a third proof: proof of permission. The proof of permission states that this operation was permitted for this person, and only this person. Any attempts to create or alter records controlled by the smart contract which are not signed by the private key associated with the consenting user are rejected, and all modifications are audited and persisted for the lifetime of the blockchain.

Together, these three proofs – the proof of possession provided by the blockchain, the proof of presence provided by the BlokSec application, and the proof of consent provided by the Personal Consent Smart Contract (also executed on the blockchain) – provide three very strong factors of authentication. BlokSec brings all of these factors together with every user authorization event, and the transaction records are recorded on the blockchain providing auditable, irrefutable proof of the integrity and origin of the transactions. The result is the most robust and secure authentication platform available today, and one which is capable of being the foundation of the next generation of authentication services.

BlokSec's Tri-Factor Authentication

proof of possession *– cryptography and consensuses - verification of digital signature handled by the distributed nodes of the blockchain*

proof of presence *– verification of user presence through biometry or (fallback) knowledge of PIN provided by the BlokSec iOS and Android applications*

proof of consent *– recoded request context to prove the user provided their permission to execute the transaction, maintained in the Personal Consent Smart Contract on the blockchain*

In summary, blockchains preserve complete historical information about a record, including verifiable proof of who created or modified the record and cryptographic evidence of the record's integrity. Being auditable and indisputable makes blockchains an ideal tool to keep records of authentication events. From BlokSec's perspective, it also provides one more very important advantage – the decentralized, consensus-based nature of the system removes the need for a trusted 3rd party acting as a centralized authority. This gives the BlokSec platform the credibility required to strongly assert a person's identity, without the need for the reputation and trust of the big identity providers.