Blockchain Biometric Signature

TRUSTO

ICO 3.0

Blockchain Biometric Signature

Today the vast majority of modern authentication implementations strive to maximize both security and convenience; that is the way to make it as difficult as possible for a fraudster to steal or spoof the rightful user's authentication factors (e.g. device, password, token, biometric). TRUSTO interference for the TRUSTO ecosystem with access to the protected asset or service for the rightful user using Trusto Hybrid Biometrical Blockchain. TRUSTO biometrical document blockchain is the beneficiary of this new technology of the Trusto Hybrid Biometrical Blockchain.

But while Trusto Hybrid Biometrical Blockchain. transaction signing is leaps and bounds better than using passwords or tokens, even that isn't a foolproof method: without anti-tampering mechanisms, the log can still be corrupted. The digital signature prevents tampering with individual entries, but entries could be falsified by deleting existing entries or adding counterfeit summaries. That means some of the scenarios I outlined previously that could be headed off by using biometric authentication -- a trader denying responsibility for a bad transaction; redirecting funds through a falsified account -- could nevertheless be covered up if the Trusto Hybrid Biometrical Blockchain for the criminal accessed and rewrote the transaction on the log.

TRUSTO Platform Blockchain and are fond of converting complex transactions and sequence from code in to real world to be used with any knowledge or expertise or experience in computer science or coding. Our are of expertise is in Blockchain-based applications include any business transaction that can include:

- Business order tracking
- Supply chain
- Banking and Finance
- E-learning
- Healthcare
- Online shopping portals
- Insurance,
- Travel
- Music
- Renewable energy
- Contract validation

Discourage the user from circumventing the intended security mechanisms. TRUSTO Multifactor authentication (MFA) aims to meet these objectives by making it harder for fraudsters to defeat security mechanisms without adding inconvenience for the user.
Today technology for Mobile authentication methods often use two authentication factors to boost security:
Possession: something you have, such as the smartphone itself.
Knowledge: something you know, such as a password.
They can also be used in an "out of band" fashion, where authentication on (an authenticated) device is used to gain access through another channel, such as through a website via a browser on a laptop.

Passwords in the TRUSTO ecosystem MFA's Armor Multi-factor authentication aims to maximize both security and easy convenience for users. Password protection is a 70-year-old technology that was conceived for a far simpler digital world. They are the shining suits of armor of the cyber-defense world – antiquated, solid, and ineffective against modern hacking arsenals. First, passwords are vulnerable to phishing, interception, guessing, brute force attacks, and large-scale data breaches. Fraudulent email requests for password resets, fake web pages meant to steal credentials, and key-logger malware (which records physical keystrokes) are just a few examples of the phishing and spying techniques that are used to steal passwords or PINs. Second, passwords are often stored in a central location.

In September 2017, Deloitte Digital experienced a data breach that resulted in emails and passwords being exposed belonging to as many as 350 corporate and government clients. Earlier in 2017, hackers also exposed HBO administrator passwords in a 1.5 terabyte data theft. Most of the world top companies including Paypal, Master, Visa Card, Google have lost users Identity. users have an increasing number of web-based accounts and are relying on more digital services than ever. TRUSTO ecosystem best practice is to have different passwords for all of them. However, the only way to feasibly remember them all is with a password manager (most of which cost money). But even password managers have vulnerabilities, such as "clipboard sniffing" (reading the copy-and-paste engine), Use of passwords on smartphones is even more inconvenient and insecure than with other devices that provide some reasonably secure means to store passwords. TRUSTO ecosystem consider other knowledge-based factors such as security questions and onetime-passwords are also inadequate.

A security question can be guessed through research on social media or even stolen through other means of social engineering (pretending to be someone else to request knowledge).
One-time passwords succumb to a different flaw: They can be intercepted.
Considering the radical evolution of our networks and computing devices that has taken place since passwords were invented, it is plainly obvious that they are woefully insecure and inconvenient. Authentication needs to be rethought, yet we remain heavily reliant on them today, according to a recent study after 18 months made by Trusto team are an attractive alternative to passwords as a second authentication factor because where are inherently convenient and unique technology for generating of public and private key's .. They are easy to use but difficult to steal reproduce and to spoof and is quantum proof technology in case is using our hardware biometric dynamic key.

TRUSTO biometric modality has unique characteristics that bring advantages in terms of both security and convenience.

TRUSTO Multimodal Biometrics for Authentication Multimodal biometrics have been seen as a way to improve biometric performance in terms of false match and false non-match scores; the more data that can be used for biometric matching, the better the performance.

TRUSTO Hybrid multiple Blockchain modes can also be used to improve their resistance to fraud. By using multiple biometric modalities in concert, the advantages of each biometric can be exploited, while neutralizing their respective disadvantages. This combination of multiple modalities will be crucial as spoofing methods become more sophisticated. To better illustrate this point, consider some of the following multimodal methods and how they help with spoof detection as well as biometric performance: Voice Biometrics Enhanced with Facial Recognition is the second step in biometric technology evolutions.

A facial analysis is conducted while the user is speaking to determine the liveness of the speaker. Real-time analysis of how the mouth moves when the user speaks a random passphrase helps ensure that the voice and facial recognition scan match and that the sample is not an audio/video recording of the targeted victim played from a device.
These Biometric Blockchain multimodal authentication methods not only improve the biometric performance but also make it more difficult for fraudsters to spoof biometric scans. They also avoid negatively impacting the user experience by operating simultaneously.

Blockchain solutions also provide the transparency necessary to prevent wholesale falsification of the entire chain. While the nonce proof-of-work helps prevent overnight falsification of a chain, a publically accessible chain guarantees that a chain is not counterfeit since it is not under the sovereign control of a single authority. Public blockchains are stored in a decentralized fashion, across thousands of nodes globally, operated by independent entities. At any time, past or present, a block on the chain can be validated for a given date and time.

TRUSTO PLATFORM will initially focus on several key applications. A decentralized token exchange will facilitate fundraising, secure, save, or exchange and file or document, and transfer of financial instruments on the blockchain. Asset-to-asset (P2P) transfer will be enabled from the start, meaning that any currencies and assets can be used to pay network fees, thereby placing minimal burdens on end users.

TRUSTO is designed to take the any legal token or document concept to its fullest expression, the platforms who is a new product in the cryptocurrency world thanks facilitating instant exchange and other existing projects. 'One of the use cases we want to realize from the start is a kind of decentralized Trusto Ecosystem where anyone can develop for their project or security system in such a way to be unique for private and public sectors, TRUSTO PLATFORM' built-in blockchain-based reputation system where developer , investors , public organizations and private companies can have a way to develop multiple applications for :

- TRUSTO applications on Cloud technology of Blockchain for Private
- TRUSTO applications on Cloud technology of Blockchain for Institutions
- TRUSTO IOT
- TRUSTO IOMT
- TRUSTO Biometrics ID
- TRUSTO Security
- TRUSTO Data Storage
- TRUSTO Data Management
- TRUSTO Data on Biometrics Blockchain
- TRUSTO Biometrical infrastructure security
- TRUSTO Medical Blockchain Biometrical infrastructure
- TRUSTO API development
- TRUSTO API Development Reward program for companies and institutions

TRUSTO PLATFORM Ecosystem give the way to Enterprises to rethink the traditional role of transaction logs, their associated storage, and analysis. Typically, logs have been kept on the server in files and compressed archive formats. They have been kept in ORACLE, SQL databases or NoSQL document stores. Theses storage schemes, however, are insufficient for non-repudiation, vulnerable to tampering and lack transparency. For complete, end-to-end certainty, and legal non-repudiation, tamper-evident and auditable transparency -- you simply can't beat the blockchain and biometrics pairing.