Enhancement of Online Identity Authentication Though Blockchain Technology

Reza Ismail
30th October, 2017
reza@syscode.asia

Abstract

Applications of online identity authentication in general could be greatly enhanced via the utilization of Blockchain encryption and smart contract technology in order to increase user and identification security, transparency and verification process.

Current online authentication process rely heavily on user passwords, dual-factor and multi-factor authentication processes. The problem with these methods are that passwords which are used extensively in all authentication processes are stored in a database which are extremely insecure and easily hacked.

Third party authentication providers require the same set of passwords and personal identity information to be stored by a third party system which introduces further security, privacy issues and bottlenecks.

The Blockchain technology is currently being used to power cryptocurrency exchanges worth over 100 Billion USD (as of July 2017). Applying this technology and its cryptographic principles into online identification and authentication process could prove to be a key to greatly enhancing security of this process.

1. Introduction

Online transactions are wrought with security concerns, mainly over authenticating the transaction process between the transaction source, its destination and everything else in between. Online identity authentication has evolved from simple passwords as proof of identification to multi-factor authentication which requires a set of challenges which must be met and completed in order to confirm identity.

The issues with passwords are widely known. Organizations are hacked and passwords and personal information are stolen on an almost daily basis. As of this writing the largest data and identity breach occurred merely weeks ago as 711 Million personal information including email addresses and passwords, were leaked via a misconfigured Spambot. A few months prior to that, a River City Media database leak exposed 1.37 Billion personal records into the public domain.

Current implementation of authentication and digital signature processes 'blindly' rely on a third party to perform authentications. These providers run on authentication servers and digital signature schemes which needs to be trusted by their users. This does not remedy the situation as they too can be exposed to the same risks as other online service providers. A compromise on their services may effect the whole network of users. This problem is generally referenced as the 'Trusted Third Party' problem.

In this paper we will attempt to explore identity authentication via implementation of the Blockchain cryptography and smart contract concepts as proof of identity and ownership.

2. Blockchain Overview

The Blockchain is a decentralized ledger of transactions across a peer-to-peer network. Blockchain technology is built on three main concepts: consensus, trustless and decentralized. It requires consensus by the network for a transaction to be added into the Blockchain via an extensive Proof of Work (POW) algorithm. Because it does not require a central authority (or 'Third Party') to verify or approve transactions, it is trustless in the way that it cannot be controlled or 'owned' by a single entity. The Blockchain is decentralized because it is replicated across millions of computers and devices across the world; there is no single point of failure.

The POW algorithm varies across different Blockchain implementations, however the key concept is that an entity must perform a set of actions to prove that the transaction has performed the required amount of work to be able to commit a transaction into the network; in a cryptocurrency network, entities performing the POW is rewarded with a small transaction fee. This process is termed as 'mining'.

In Bitcoin's implementation, a new block is added to the chain roughly every 10 minutes and the complexity of the POW algorithm is adjusted to ensure this remains true. Mathematically, it is impossible for a single entity to make changes to the Blockchain faster or more cost efficiently as the whole network, thus the Blockchain network cannot be tampered with or at least attempts to destabilize it would prove to be too costly. Currently the calculated cost of POW for one Bitcoin transaction is equal to 215 kWh, equal to powering an average American home for almost a week.

3. The Smart Contract

Aside from cryptocurrency, a new method of utilizing this technology is via Smart Contracts. A Blockchain Smart Contract, is a set of programmed code which uses Blockchain identity encryption and signing technology to self-execute a set of instructions or agreements. These 'contracts' are also able to self-enforce themselves based on pre-set parameters.

The main goal of a Smart Contract is to allow two or more anonymous parties to trade and execute agreements with each other, usually over the internet without the need for a middleman.

In the context of online identity verification, using a banking transaction as an example, the bank would be Party A while its client would be Party B, and the transaction middleman in this scenario is the third party provider which serves as a host for the authentication to take place.

A Smart Contract implementation for identity verification replaces the third party middleman as it performs the process of authentication via verification of the Blockchain identity hash and transaction signing keys.

4. Identities in the Blockchain

Blockchain uses cyptography in the form of a double (Secure Hash Algorithm) SHA-256 to hash and encrypt addresses. An SHA-256 hash performed twice is believed to be equal to the number of atoms in the (ENTIRE) universe. As of January 2015, Bitcoin was computing 300 quadrillion SHA-256 hashes per second. For a well equipped computer to brute force a specific address in this algorithm would take an estimate of 3.6 x 10^13 years. As a point of reference, our universe is believed to be 13.7 x 10^9 years.

Every transaction within the Blockchain begins with an address hash. This address may contain the user's identity and acts as a container for the user's actions and transactions, be it in a cryptocurrency value transfer or a smart contract asset transfer.

Every Blockchain transaction is made up of some value or information, a public key hash and a private key hash of the originator or recipient. This way the recipient of the transaction can use their own set of private and public keys to either verify the transaction or perform any other set of entries to the transaction, or vice-versa.

This is the pillar to the cryptography scheme of the Blockchain. It is designed to never need for a third party to verify or authenticate its transactions.

5. Smart Contract Authentication (SCA) Layer

When applying this technology to authenticate identities, the block of information can be hashed to contain information which is commonly used as a challenge query scenarios as proof of identity, such as date of birth; proof of known origin such as a mother's maiden name; and proof of ownership such as a first pet's name. A Smart Contract generator can be programmed through a Smart Contract Authentication (SCA) layer to activate and execute every time an authentication is required by either party and self govern itself within a predefined scope of actions.

The SCA can be developed on top of multiple Blockchain frameworks, including Ethereum, Hyperledger and even Bitcoin itself. The SCA exists and transacts over existing Blockchain

networks and use the same mining and verification processes as any other cryptocurrency implementation.

The obvious benefits are that we eliminate the need for a third party to authenticate transactions between two related entities. Costs can be reduced while security and privacy is greatly enhanced. Hijacking the authentication process would require the same amount of effort of hijacking a cryptocurrency network and hacking any password database will not necessarily provide access to the system since the private keys of an individual's identity are still required even though a password is present.

The SCA can be generated on the fly by any individual initiating a transaction. Again, in a banking environment as an example, even a bank officer's support call can trigger an SCA process whereby the bank officer only needs to request the client to complete the SCA by tapping a button or keying in the challenge question -answer on his smart phone, nobody needs to know the name of your first pet, not even the bank teller.

With the continuous digitization of our society, the idea of digitizing a person's identity on the Blockchain is definitely not as far fetched as it may seem. The benefits of securing a person's identity with the Blockchain is undeniable. However, as in any new implementation of an existing technology or process, there are issues to consider. In real world implementations, it will require an overhaul or at least a focused effort to integrate this technology with existing implementations of identity authentication and digital signature schemes in order to begin an initial acceptance of this technology in the market.

6. References

1. Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2009
2. "Programming the Blockchain in C#", GitHub, N.p., n.d Web July 2017 <https://www.gitbook.com/book/programmingblockchain/programmingblockchain>
3. World's Biggest Data Breaches, N.p., n.d. Web 10th Sep, 2017 <http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>
4. Michael Crosby, "Blockchain Technology", Sutardja Center for Entrepreneurship & Technology Report, October 16th 2015
5. Albert Levi, M.Ufuk Caglayan, "The Problem of Trusted Party in Authentication and Digital Signature Protocols" Bogazici University
6. "An Illustrated Guide to Cryptographic Hashes", N.p.; n.d. Web May 2005 <http://www.unixwiz.net/techtips/iguide-crypto-hashes.html>
7. "Bitcoin Enegy Consumption Index", N.p.; n.d. Web Oct, 2017 <https://digiconomist.net/bitcoin-energy-consumption>