HashCash – A revolutionary step towards creating a secure digital identity cum authentication platform in the highly vulnerable web world

A White Paper from HashCash Educational

Version 1.0

August 2019

Secure Digital Identity for all

INTRODUCTION:

The concept of a digital identity is one of the oldest challenges in the world of internet. Unlike our offline platforms, digital platforms lacked a formal digital identification system. This was a potential gateway to malicious activities and the possibility of identity theft. The concept if finally changing with the introduction of standardized digitally signed credentials. Blockchain can play a major role with decentralized registration and distribution of public network keys required for digital signature verification. The two primary steps lay the foundation stones for a global public system for independent identification. It would be a simple digital identity system which is not dependent on a centralized authority which does not face the risk of a breakdown. The HashCash network has been designed for the purpose which also encompasses aspects like Governance, Scalability and Accessibility.

HashCash Network also employs a Design by Privacy instrument globally. It also employs first grade authentications like pair wise same name identifiers; inter peer private agents, and selective revelation of personal information using no knowledge crypto. The technology has the capacity to play a major transformative role in four major markets namely

- Identity and access management
- Data integration
- Reg Tech
- Cyber Security

The HashCash Network will provide economic benefits for the parties like Credential Issuers, Verifiers, and Owners

CONTENTS

THE PROBLEM: DIGITAL IDENTITY IS THE BIGGEST CHALLENGE ON THE INTERNET

The problem is actually increasing gradually and even in the year 2019, the scenario is the same

In the world of internet, there is absolutely no full proof technique to determine whether you are an artificial bot, a terrorist, hacker or an underage teen trying to access adult stuff. These challenges are not prevalent in the offline world in case the conman is smart enough to takeover, duplicate and use someone else's identity. Online world is full of possibilities and the dark possibilities of the web world pose serious risks for both customers and businesses. Both parties have a lot at stake in the web world. It can range anything between a bank account to vital personal information. Impersonations have led to the loss of millions of dollars across the globe.

In the physical world, identity protection and proving one's identity is easy

One just needs to take out his/her wallet and prove his credentials in a place like a library or an airport or a hospital. The digital world has fewer alternatives when it comes to identity proofs like the passport, driving license or an ATM card.

The verification of digital assets over a network is highly challenging simply owing to the absence of human intervention in scrutinizing the claims. A computer or a data processing machine is incapable of doing a human level filtering of authentication claims.

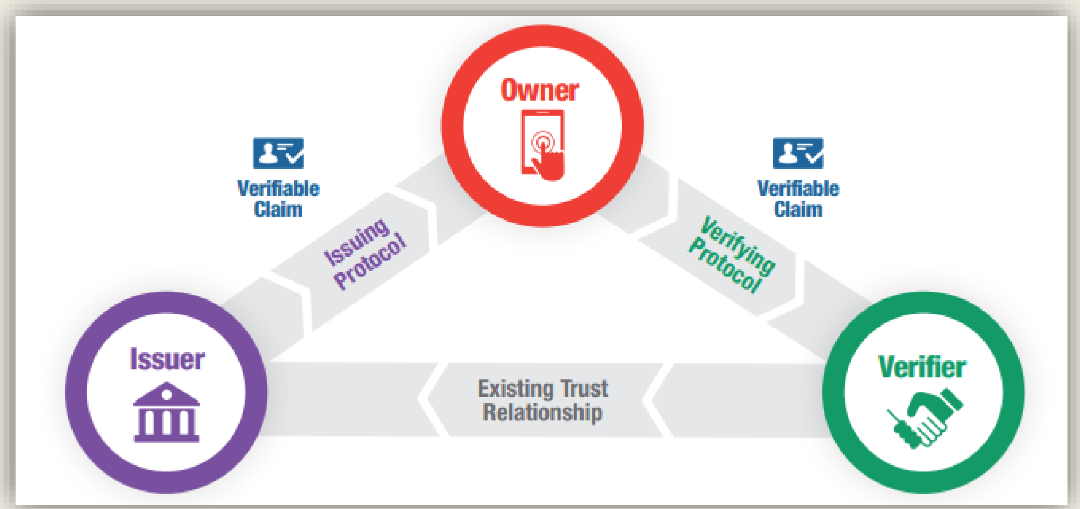
Standardization of digital credentials is very important especially when it comes to verification by digital signatures. This system has been globally regulated and has two basic keys. These keys are used to validate the digital signature. The first key known as the signing key is used for the sole purpose of signing the document. This key is kept secret by the issuer while the other key called the public key is a verification key which is used for signature verification and tamper protection. For a globally acceptable digital adoption system, one must have a standard public key verification protocol in place.

World Wide Web Consortium or the W3C was established in the year 2017 in the month of April

In order to understand the objective of the W3C group, one must read the below clause carefully

'It is currently difficult to express banking account information, education qualifications, healthcare data, and other sorts of machine-readable personal information that has been verified by a 3rd party on the Web. These sorts of data are often referred to as verifiable claims. The mission of the Verifiable Claims Working Group is to make expressing, exchanging, and verifying claims easier and more secure on the Web.'

The new standards of digital verification are an effective way to validate the authenticity of the users of digital assets. The degree of verification always depends on the number of parameters which can be verified



The Verifiable Claims Ecosystem

The standardized verifiable claims or digital signature verification

The digital signature verifications are conducted by PKI or Public Key Infrastructures. However, the generic architecture of PKI or Public Key Infrastructures is cumbersome, centralized and costly. The PKIs need to be certified and verified by Certificate Authorities which is an expensive process. The entire processes of verification using PKIs are cumbersome and not pocket friendly at all. The only feasible solution to avoid these problems is through a blockchain network which would have a completely decentralized model which would minimize the risk of single point failures.

THE SOLUTION

With modern Blockchain Technology, one can easily go ahead and provide a solution to this existing problem. A blockchain is a vast decentralized root of reliability which is not owned by anybody but can be used by everybody. Blockchain is a technological platform which would turn the centralized root of trust model which uses Certification Authorities and consortia; it uses a consensus platform which would authorize transactions over the internet.

Blockchain in Spirit Replaces trust in humans with high reliability in basic mathematical models for accuracy and minimizing errors in handling digital identity authentication!

Irrespective of the design of a given blockchain, the primary design of a blockchain is completely tripe cryptographic. To understand the concept in detail, one must go ahead and read the descriptions given below:

- Each transaction over the blockchain network is digitally signed and verified

- Each transaction irrespective of the type of transaction would be inked to the previous one through a hash making blockchain ledgers continuous and full proof
- The validated transactions are duplicated across all the machines connected over the blockchain

The results are startling, especially when it comes to the large cryptographic ledger which is absolutely immutable in terms of its capacity to offer full scale protection to the data set against any kind of external malfunctions or changes.

The whole objective of using the blockchain is to use shift from the centralized private key identity to the publicized or decentralized private key identity. The quantum shift from the centralized PKI to the decentralized PKI model has several advantages.

USING PUBLIC BLOCKCHAINS FOR DIDs – ISSUE DIGITALLY SIGNED CREDENTIALS AND CAN BE VERIFIED EASILY BY ANYONE

A point has finally been reached where offline identity verifications can be used online too! Blockchain ensures a Self Sovereign Identity for all! The same platform can also act globally offering the best in class services to identity owners, issuers and verifiers acting just like the world of internet. The internet or a DNS acts on open protocols and open standards which are not owned privately. Thus every participant has the potential to work on it, improve and enrich it at the same time. An identity system working on a public blockchain would function along the same lines with open protocols and open standards, making the blockchain accessible to the public who in turn can work and enrich the same. At the end of the day, this platform would offer **Identity for Everyone.**

The platform will not be under single ownership since it would lead to a conflict with the clause of self sovereignty. Identity will always be under the ownership of the individual and cannot be taken away by anyone. If identity systems are controlled by a blockchain consortium those personal identities are being compromised automatically.

Conclusion

Blockchain is a platform which in all its abilities is the best match to handle the challenges and requisites of the digital industry which wishes to secure personal ids against siphoning and other challenges like digital identity thefts. Blockchain in itself creates an unbreakable chain of ledgers which are connected securely and does not allow any modifications in the storage blocks. Hence, to prove one's identity over the blockchain network one has to go forward and reach a consensus of identification proceeded with authentication and access fulfillment.