XS: Global Distributed Digital Identity

White Paper

www.getxs.co
contact@hiteshmalviya.com

About Authors

Hitesh Malviya is an acclaimed personality for his pronounced work in the realms of information security, start-up development and Digital Identity. His fields of expertise include Blockchain, Information Security, Agile Product development and Start-ups. He has penned down more than 10 research papers on themed on a wide spectrum of topics such as credit card security, cloud computing security and web application security. His work has been recognized and appreciated by defence ministry of South Africa in past. He has compiled his articles on Blockchain technology and its Use-cases on itsblockchain.com

Rishabh Bahl has been hard core high tech conceptualizer to reality and entrepreneur with experience • Starting out with AMC and remote management. He has Launched and successfully run 2 startups Rish Technologies and TWiss (online healthcare). He has Expertise in deploying disruptive technologies like Blockchain, Neural nets in Data Analytics, A.I, Brain Computer Interface, EaaS. He is the Host on ItsBlockchain video series Blockchain Made Easy on YouTube.

Abstract

Blockchain technologies make tracking and managing digital identities **secure and efficient**, resulting in seamless sign-ons and reduced fraud. Be it banking, healthcare, national security, citizenship documentation, online retailing or walking into a bar, identity authentication and authorization is a process intricately woven into commerce and culture worldwide. Due to the lack of common comprehension and unchecked cyberspace of personal information, identity is facing significant hurdles, specifically in the context of technology. Current methods use problematic password-based systems of shared secrets exchanged and stored on insecure systems. Whereas, blockchain technology, along with biometrics, offers a solution to many digital identity issues, where identity can be uniquely authenticated in an irrefutable, immutable, and secure manner.

Contents

Introduction

Due to the lack of common comprehension and unchecked cyberspace of personal information, identity is facing significant hurdles, specifically in the context of technology. Events such as hacked databases and breached accounts reflect upon growing problems of a technologically advanced society, that lacks outpaced identity-based security innovations.

Current methods use problematic password-based systems of shared secrets exchanged and stored on insecure systems. Whereas, blockchain technology, along with biometrics, offers a solution to many digital identity issues, where identity can be uniquely authenticated in an irrefutable, immutable, and secure manner. Blockchain based authentication uses digital signatures systems, based public key cryptography. In blockchain identity authentication, the only check performed is whether or not the transaction was signed by the correct private key. It is, therefore, inferred that whoever has access to the private key is the owner and the exact identity of the owner is deemed irrelevant.

Problem Statement

One common misconception about identity theft is that it only seriously affects people who are lazy or not careful with their private information. However, that isn't true at all. The number of people having access to our private information, at stores, doctor's offices, or over the phone affects the number of opportunities that strangers have, to steal our private information without us knowing it.

Family identity theft has also become a huge problem, with children unfortunately becoming the victims most of the time. Unlike usual crimes where the culprit breaks into your home or robs you in person, identity theft can be accomplished without us even seeing the perpetrator. Our information can be bought and sold online, as well as in person, and often the perpetrator can't be caught.

Identity theft is not a small problem — it's actually the fastest growing crime in America, with 9.9 million incidents per year. In 2012, 7% of people, sixteen or above were identity theft victims. Credit card, bank account, or other existing accounts' exploitation comprised 85% of the issues. On the other hand, people also experienced new accounts being opened in their name, and these victims were more likely to suffer from serious financial, credit, or emotional distress.

About 14% of victims lost $1 or more, but about half of them lost less than $100. This doesn't sound like a lot of money, but it also didn't consider the amount of time that some victims spend trying to clear all of their accounts up, which can take hours or more (half of identity theft victims were able to resolve issues in a day or less.) However, of those who had personal information used improperly, 29% spent a month or more fixing the issues.

Although it seems strange, family identity theft is a big problem. Child identity theft doubled in 2012 for victims under five (a separate study found that 2.5 percent of households with children under 18 experienced child identity theft.) Different studies concern different age-groups, but what is clear is that child identity theft is real, and a growing problem.

Children are not the only ones suffering from family identity theft either. Family members and friends often have easy access to your personal information because they come to your home. Some information is already known to them because they spend time with you (like your birth date and address), so they have a leg up on other potential thieves. Also, unlike strangers, you already trust them. Although most family members are trustworthy, you should still be careful.

Digital Identity

We often engage in the creation, use and management of digital identities, without fully understanding what and how much we're actually sharing.
We would never leave home without locking the door, yet often save our online banking username and password to our computer – essentially equivalent to leaving the key in the front door, ready for anyone to enter. We don't put a sign on our door that reads "We're away on holiday" yet we happily post such information on social channels for just everyone to see. Consumers express concern about identity theft but at the end of the day are doing little to protect themselves from it from a digital perspective.

Digital identity has become important mainly because of rising online criminal activity – due to the breadth and depth of consumer's online lives; and also convenience.

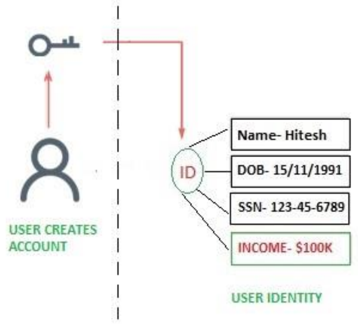
Basically, digital identity is a supplement to the real or core identity of any individual. In other words, digital identity is a set of credentials or attributes that allows a third party to asses and verify the authenticity of the identity in question and the claims being made by it. Such as- whether or not that identity is allowed to enter a certain website or is allowed to make a payment.

Furthermore, digital identities can range from a single attribute or credential, such as age, to the complex, containing details of a consumer's home or bank account. However, the main difference between physical identities and digital identities tends to be volume. Where most people have 3-4 physical identity documents– ID card, passports or – they tend to have a large and growing number of digital identities – multiple email accounts, Facebook, Google and other social media logins.

Core Functions of an Identity System

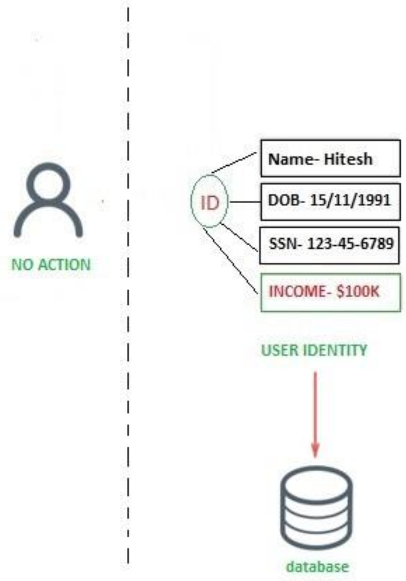
Issue

Whether it's the US government assigning Social Security Numbers or Google letting you select an email address, there is a particular way to create new identities and assign identifiers.



Store

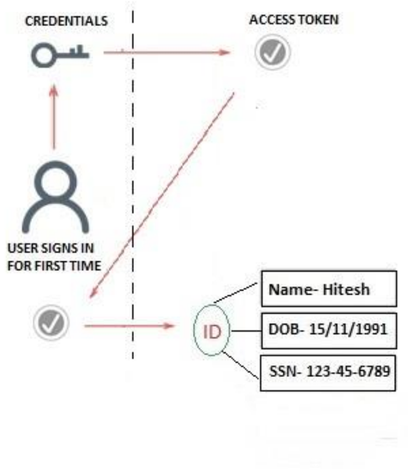
Identity data needs to be stored somewhere. Usually this is a private database with administrator-controlled access, but technologies like IPFS and Blockchain are examples of new models for data storage and retrieval.



Authenticate

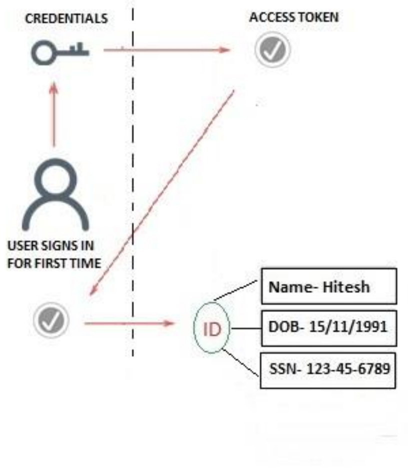
Individuals need to prove they are who they say they are, when attempting to assert their identity. This is done using one or more factors of authentication: something you know (a password), something you have (a mobile phone), or something you are (photo or fingerprint).

For example, think of what happens when you present your drivers' license at a bar or airport. The person inspecting it looks at your photo, then at you, to make sure you're the person represented on the card.



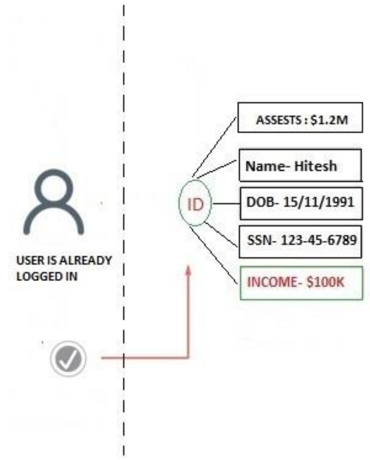
Authorize

Once they've authenticated themselves, individuals are authorized to perform certain tasks. Whether it's being able to access the transaction history for your bank account or being able to enter a bar, identity systems get utility from enabling you to take actions and interact with people or businesses based on certain information about you.



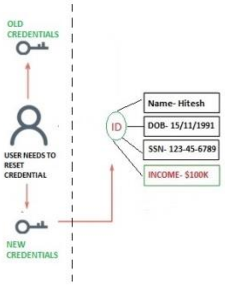
Recover

Stolen wallet or forgotten password? Individuals need a way to regain access to their identity data, should they lose it. (Note: This is often the part of the process where the usability vs security tradeoff is most stark — protecting an account with a random 32-character password and fingerprint isn't much good if "recovery" can be done using your zip code and the last four digits of your social security number. Conversely, asking the average user to print a recovery key when they create their account is absurd.)



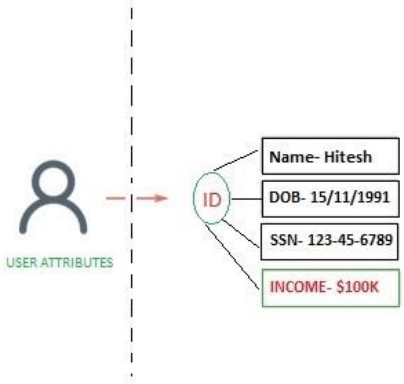
Update

Users or administrators need to be able to add, remove, or edit attributes associated with an identity. Pieces of our identity information change over time: an address gets changed, a new degree is earned, a drivers' license expires, etc. Digital identities need to evolve along with the people they represent.



Audit

How can someone check that your identity data is accurate? In the context of regulated industries, such as financial services or health care, identity data and the process by which it is recorded and accessed, needs to be auditable by relevant government institutions. For user-controlled identity systems like PGP, code is open source and trusted parties host data.



Blockchain

"Blockchain is a distributed database that maintains a continuously growing list of data records, chained together against revision and tampering."

Information held on a blockchain exists as a shared and continually reconciled database. This is a way of using the network that has obvious benefits. The **blockchain database isn't stored in any single location**, meaning the records it keeps are truly public and easily verifiable. **Hosted by millions of computers** simultaneously, its data is accessible to anyone on the internet.

In its purest form, blockchain lets companies instantly make, approve, and verify many types of transactions by leveraging a collaborative digital ledger and a predetermined network of individual contributors or keepers of the blockchain. Once transactions or other data are inside the secure blockchain ledger, cryptography takes over and verification hurdles drastically decrease the chances of data being stolen.

There are two often-referenced categories of blockchain: private, which is permission-based, and public, which is anonymous. Each has its own strengths, but private, permission-based blockchain has an added layer of protection, where participants in a transaction are known and traceable.

Are we willing to let blockchain serve as a clearinghouse or executor for our full digital identities? Think of how that could play out in a few different scenarios.

Private aka "Firm Private": This type is already taking hold. Through blockchain, a specific financial institution can verify and facilitate a stock purchase in real time, but after its completion that transaction can also become a part of a digital identity, protected by blockchain. That way, the information doesn't have to sit in a separate, isolated account behind the bank's walls, but can instead be instantly verified, referenced, and acted upon with other digital identity elements. It also allows the bank to retain some level of authority and management.

Public aka "Classic": As the Internet of Things expands, public blockchain can serve as the ledger in scenarios where only certain elements of a digital identity are necessary and a central authority isn't as integral. For instance, buying a burger at a drive-through. The combination of blockchain and a Bluetooth beacon could verify the car associated with a digital identity, verify the Visa Checkout app running on the car's console, communicate to the restaurant's payment system, and debit a bank account the proper amount. All of that can occur without a holistic digital identity being part of a known or closed network, sharing and accessing only the portions of the digital identity that are relevant to the sale.

Private Shared aka "Industry Private": This is a hybrid type of blockchain that could be the happy medium for financial institutions or stock exchanges, as digital identities and transactions are managed by a "circle of trust." Changes don't require mass approvals nor does the private shared blockchain allows everyone to read and amend, but it keeps power from being consolidated in a sole authority's hands. So in the stock purchase example, a few interconnected industry stakeholders would need to approve the transaction — perhaps a bank, the stock exchange, and the Federal Trade Commission — before it becomes a verified part of the blockchain and of an individual's digital identity.

Our Solution

We intend to build a Global Distributed Digital identity on Blockchain for Consumers, Industries and integration with the Government. We are trying to solve identity theft and validation problem with our solution which is one of the fastest growing problem in the world today. Our solution will establish a channel to verify government issued identity, social media fingerprint, email address and mobile number of a consumer at time of generating digital identity.

Issue of XS ID:

- Through Sign up on our website and mobile app.
- Partnering with Visitor Management Software companies to use our api to create Access Id for visitors when they check-ins first time.
- Create a check-in system and promote it for free to get it rolled out in more premises.
- Use the database of Visitors IDs which we are generating everyday with our VMS Partner. Same way bitcoins need miners for creating BTC, We need such partners to create XS IDs.
- We verify social media account, mobile number, email address, government issues document of consumer at time of ID generation.

Store

We store identity data on our sidechain and use BTC as a monetary token.

Authenticate

We intend to use two multifactor authentication methods:

- XS ID + Private Key
- XS ID + Face Detection

Recovery

Recovery of an identity account can be done by using Face detection and Providing Details of Goverment issued documents.

Possible service to offer under XS for Consumer

- Send and receive Bitcoins, Ether and other Currency (Transaction)
- Login in Partner websites/app with XS ID - Password less login (Authentication)
- Get Partner Discounts/Redeem option (Personalization)
- Share ID with people you want through SMS,Whatsapp, email etc (Identification)
- Search people on XS ID Network and Request for their information, Share information with them on an encrypted network.(Communication)

Services for Business

- Authentication API for website/application
- Identification API for website/application

Market Usecase

AGE VERIFICATION

XS provides an age and identity checking system that allows owners of age gated content to control who is allowed access to their material.

FINANCIAL SERVICES

XS is world’s first user centric identity solution. It allows for large scale deployment while also respecting the privacy needs of your users.

SHARING ECONOMY

By allowing our customer to own their identity data through the XS application. We believe we’ll benefit from a trusting user community, where the risk of fraud is drastically reduced.

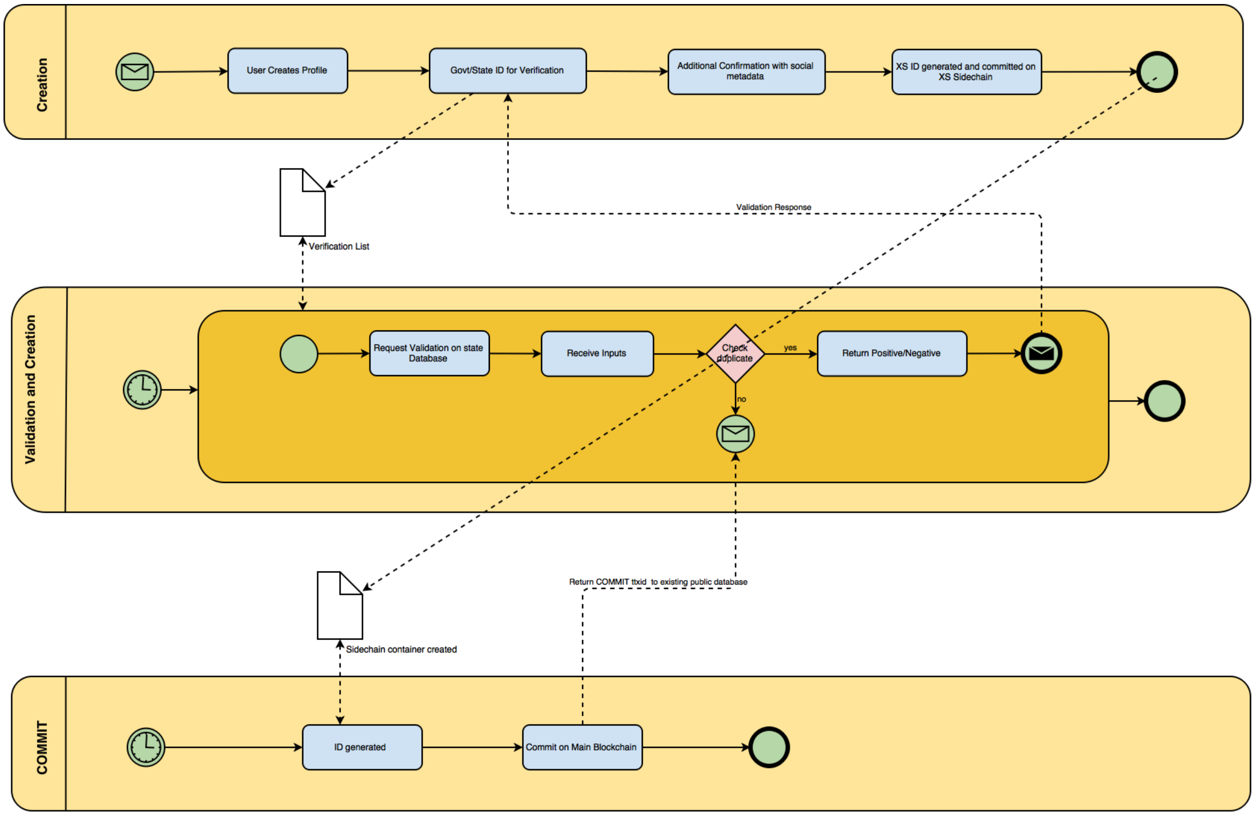
HEALTHCARE

It works on their preferred platform (mobile) and is focused on making their life easier. We could let them use XS to pick up prescriptions or sign-in for appointments.

ONLINE MARKETPLACES

Meeting people in person can create anxiety, while sending goods or money to people online can be risky. XS helps us to reduce some of that risk and anxiety.

Technical Architecture


Creation
User Creates Profile
Govt/State ID for Verification
Additional Confirmation with social metadata
XS ID generated and committed on XS Sidechain
Verification List
Validation Response
Validation and Creation
Request Validation on state Database
Receive Inputs
Check duplicate
yes
no
Return Positive/Negative
Sidechain container created
Return COMMIT txid to existing public database
COMMIT
ID generated
Commit on Main Blockchain

Future Scope

Multiple attributes can be linked with XS digital identity, would be securely stored on Blockchain and It can be used for doing multiple type of online interactions by user. This will create a new way to share information securely over the internet. It will develop a new trust protocol amongst users.

References

1. http://indianexpress.com/article/opinion/columns/shoring-up-our-digital-identities-4447797/
2. http://www.darkreading.com/endpoint/blockchain-and-the-battle-to-secure-digital-identities/a/d-id/1327279
3. http://www.americanbanker.com/news/bank-technology/how-blockchain-fits-into-the-future-of-digital-identity-1080345-1.html
4. https://en.wikipedia.org/wiki/Digital_identity