Chino

Decentralized Virtual Identity
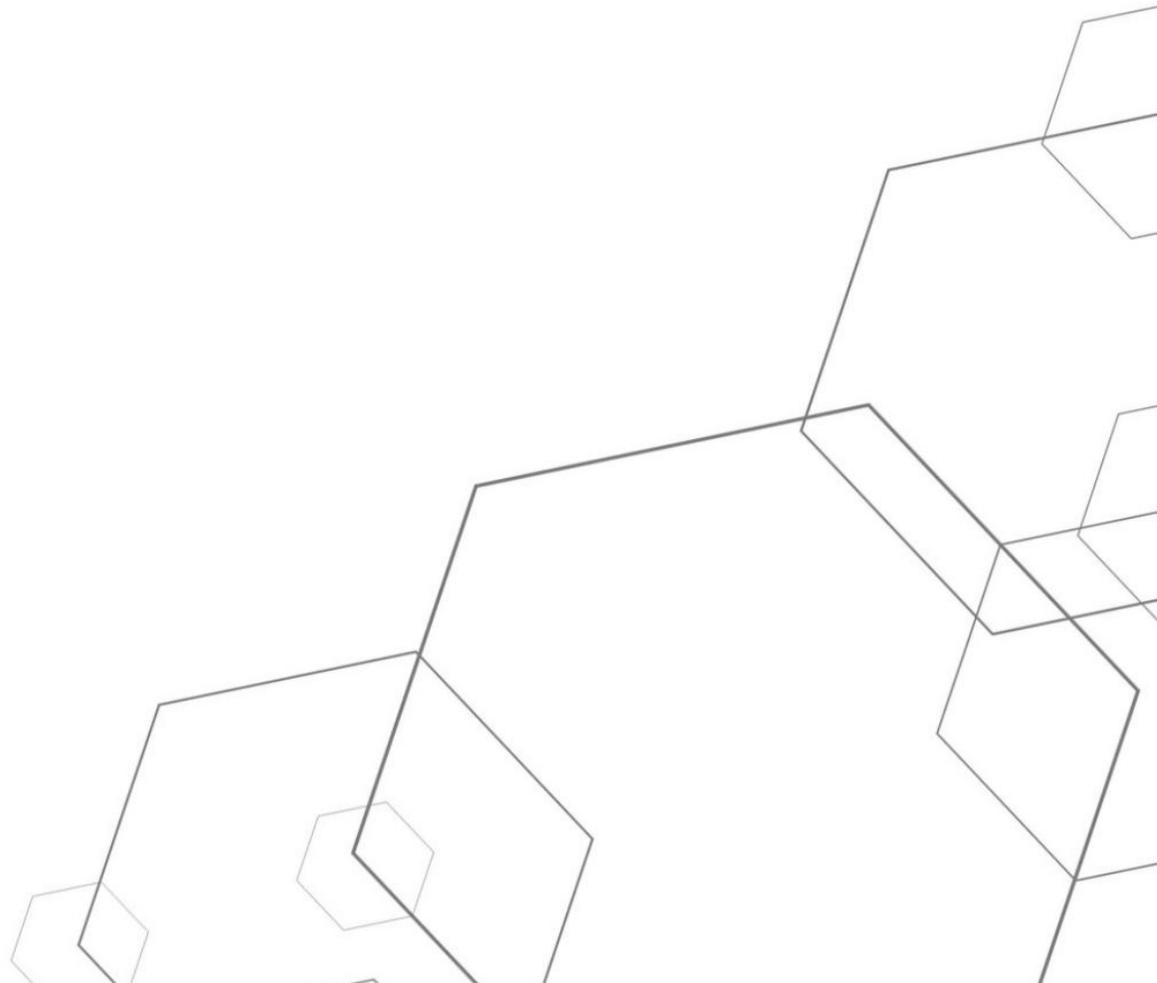
eSatya

eSatya

Introduction

1.1. History

In psychology, identity is the qualities, beliefs, personality, looks and/or expressions that make a person (self-identity) or group (particular social category or social group).[1] The human beings can not exist without an identity and has played vital part in human history. The identity helped our ancestor to verify if the individual was member of the tribe or not. Identity was earlier associated with the people around us; our family, neighborhood, or city. But, once people started traveling and traded with strangers the value of identity became more important for individuals and organization. The identity has helped people not only to travel but to own asset, and access to services, and hence become member of a community.

One of the earliest identity documents inscribed into law was introduced by King Henry V of England with the Safe Conducts Act 1414.[2] The document issued by the king acted as a passport. For the next 500 years and before World War I, most people did not have or need an identity document. After the war, most countries started issuing documents, as national IDs which could be used to prove a person's identity. The document hold information such as the bearer's full name, age, birth date, address, an identification number, gender, and more.

With the advent of the information age, the identity now has become an integral part of human society - Name, Phone No., Email ID, Facebook, Twitter, Instagram, Work Address, Home Address, GPS location, Passport No., Citizenship No., Visa No., Usernames, Passwords, Bank Account No., License No., Employee ID and many more. Clearly, the way we identify ourselves has undergone a revolutionary change.

1.2. Digital Identity

The way we identify ourselves will only continue to evolve, making the management of user identity data and identity verification technologies even more critical. The way we interact with others in digital space has gone a radical

---

[1] James, Paul (2015). "Despite the Terrors of Typologies: The Importance of Understanding Categories of Difference and Identity". Interventions: International Journal of Postcolonial Studies. 17 (2): 174–195.
[2] "A brief history of the passport", The Guardian, 17 November 2006
.,/

eSatya

change. These interactions require us share a lot of information - simple as putting name, gender, and email ID, or putting in more personal information such as photo, date of birth, residential address, phone number, or bank details. Governments globally are increasingly proposing or implementing national digital identity programmes. Many such programmes entail a push to collect, store, and use the biometrics of individuals as the primary means of establishing and authenticating their identity. More than 60 countries have set up a national ID scheme and most of them are issuing electronic national ID cards.[3]

2. Problem

The future of identity management should make sharing and verifying an individual or organization information efficient, and secure. It should free an individual of a burden of maintaining, and verifying separate identities to use services.

Digital identity has become a necessity in almost every sector, whether it's banking, government, healthcare or online retailing. The need for digital identity has risen. However, there are certain problems associated with digital identification system -

1. *Fragmented identification systems*- Due to the lack of interoperability among various identification systems, repeated registration and verification problems arise - which wastes time and resource.
   http://www.nidmc.gov.np/home/pageDetails/15
2. *Document verification and forgery -* Authentication, authorization and attestation of identity and documents is a cumbersome process. The documents even digital need to be verified with the original or notarized. Even then most of the documents are susceptible to forgery.
   https://thehimalayantimes.com/kathmandu/man-arrested-for-passport-fraud/
3. *Authentication -* The traditional digital identity authentication method is password-based, and this information is stored in a place which is easy to hack making the entire information highly vulnerable. The poor cybersecurity systems are vulnerable to attacks.
   https://www.zdnet.com/article/hacking-group-from-nepal-posts-10000-stolen-facebook-accounts-online/
4. *Centralized database and data breach -* The centralized database is prone to attacks and data breach.
   https://www.bankinfosecurity.com/report-attackers-hacked-nepalese-banks-swift-server-a-10437
5. *Data privacy -* Individuals and organizations are often not in control over their own identities. Personal information is regularly shared without awareness and is

---

[3] https://www.gemalto.com/govt/identity/5-reasons-electronic-national-id-card

a centralized source of sensitive data for hackers. The stricter global customer privacy laws are getting enforced.

https://www.recordnepal.com/category-explainers/digital-privacy-national-identity-card-civil-liberty-nepal/

Blockchain technology shows promise in improving aspects identity and access management. Blockchain is a public platform that bypasses middlemen and allows participants to establish trust and verify identity that is cryptographically secure. Blockchain consists of broad class of relatively new security methods and tools, with certain properties of potential value in digital identity management —starting with the financial, travel industries and enterprise identity.

3. Solution

3.1.   What is Blockchain?

Blockchain today is a lot like the internet in the early 90s. Blockchain has been described as one of the most significant technological advances in modern history which has led to it being dubbed "The Internet 3.0". Blockchain is decentralized, practically immutable, and cryptographically verifiable ledger (database), this type of blockchain appears to lend itself to countless applications beyond payments, including identity management, to reduce fraud, and remove bottlenecks.

- *Immutability* - The shared blockchain ledger information is checked for integrity by large network of participants based on shared agreement.
- *Irreversibility* - Once the information is accepted into the ledger it cannot be reversed.
- *Transparency* - The blockchain ledger is visible to all the participants. The records are visible.
- *Low-Cost* - There's no need for middle man to manage the transaction in blockchain reducing the middle-man fees.
- *Decentralized security* - Blockchain uses strong cryptography and large network of participants to create transactions that are fraud-proof.

3.2.   What is Chino?

Chino is a virtual identity card to unify all the identity documents - citizenship, driving license, PAN card, employment ID, college ID, birth certificate, voters ID, blood donor card and many more. The ID would be secure that even banks can rely on it. Chino is an

identity management system built using blockchain technology to provide security using public/private key and hashing to store and exchange information.
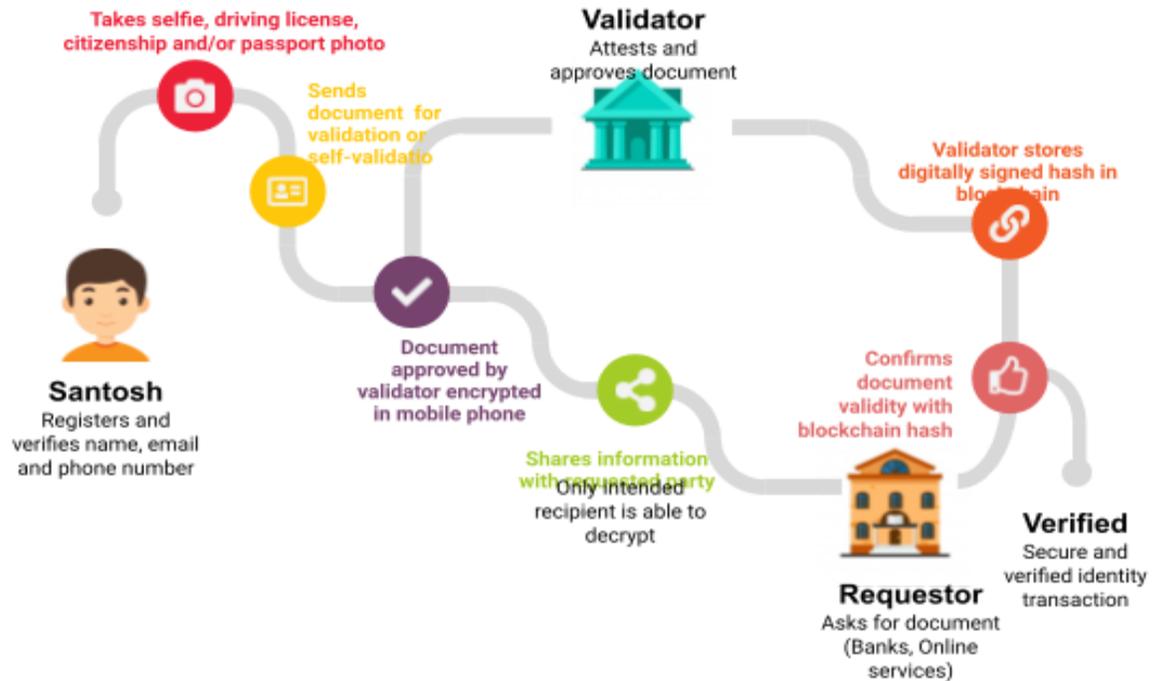
3.2.1. Chino Platform

Digital management currently relies on organization obtaining and keeping records of clients. This presents significant security risks and overheads. Chino presents a blockchain based digital management platform for secure and efficient verification of records without the need to share actual records between the parties. This allows users to have full control of their records.
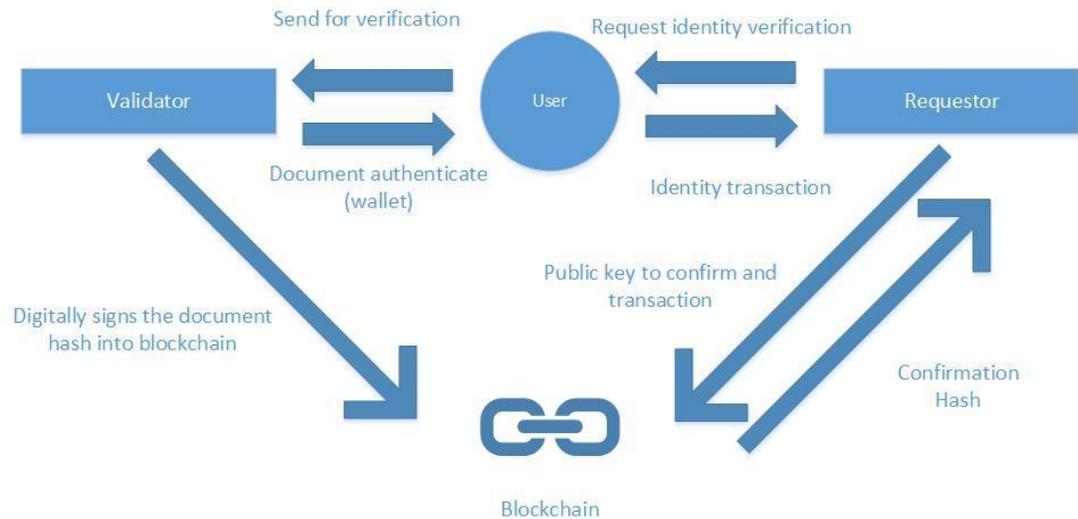
3.2.2. How it works?

Users inputs the information into the Chino system, including scanned copy of their driver's' license, citizenship, passport, and other identification documents. The information is either self-certified or certified by the party. The Chino system hashes these records and digitally signs them using individual's private keys and stores it on the blockchain. The personal data is owned by the individual.

When third parties need to authenticate and verify a user, they request the data, and the user's public key from the Chino system. They then verify it against the digital certificate on the blockchain to prove that the user owns it.

Santosh
Registers and verifies name, email and phone number

Takes selfie, driving license, citizenship and/or passport photo

Sends document for validation or self-validatio

Validator
Attests and approves document

Document approved by validator encrypted in mobile phone

Validator stores digitally signed hash in blockchain

Shares information with requested party
Only intended recipient is able to decrypt

Confirms document validity with blockchain hash

Requestor
Asks for document (Banks, Online services)

Verified
Secure and verified identity transaction

Creating an Identity

1. User fills in the personal information in Chino system
2. User takes a picture and uploads ID documents
3. User confirms the data and self-certifies or third-party (validator)
4. User information and documents are encrypted (private/public key encryption)
5. The system hashes and digitally signs the information into the blockchain

Sharing Information

1. The user decides to share the information with a third-party (recipient)
2. The information is encrypted and only recipient is able to decrypt
3. The identities of both parties are confirmed through validation of sender's public key and signature-hashes on the blockchain
4. The transaction is verified to prove the identity of the user

eSatya

3.2.3. Roadmap

2018
Q3: Chino Planning and Discovery
- Initial research and development of virtual ID
- Chino initiative started by eSatya
- Business plan, design documents and white paper published
- Identify by Use cases for real world problem in Nepali market

Q4: Alpha Release: Emergency App
- Development of prototype Emergency app (without blockchain)
- Alpha release and in-house testing

2019
Q1+Q2: Marketing and Awareness
- Pilot with MyHealth - user sign-ups to the app
- Establish partner enterprise network - validator and requester

Q2+Q3: Beta Release: Transition system into identity management platform
- Expand Emergency App to identity management platform in blockchain
- Proof of concept

Q3: Grow client base and users
- Expand vertical markets to KYC, government and attestation
- Promote and Onboard enterprise into Chino

Disclaimer: All roadmap timelines are subject to change due to business requirements.

4. Market

Chino has identified the following areas where digital identity management can be used -

Emergency
In a case of an emergency, individuals carrying a mobile device would no longer need a physical ID. With the use of Chino, the information on a person's mobile ID can be securely transferred to a first responder's device via scanning of a QR code or transmitted wirelessly on their phone, while at the same time protecting the user's privacy.

Finance

With Chino, banks and financial institutions can carry out Know Your Customer, making onboarding process more secure and faster. Using Chino customers' information is hashed and then digitally signed by the banks private key and placed onto the blockchain. This verified information can be share with any participating banks and they can participate by appending new documents further strengthening her trust factor.

Public

The government agencies issue various documents - citizenship, PAN card, marriage certificate, land registry, vehicle registry, birth certificate and many more. With Chino, government
can certify this information on the blockchain and adjust the ownership or status changes.

Law and Security

With Chino, individuals carrying a mobile device would no longer need a physical ID. The information on a person's mobile ID can be securely transferred to a police officer's device via scanning of a QR code or transmitted wirelessly on their phone, while at the same time protecting the user's privacy. The authenticity of information from issuers is verified via blockchain.