IDHub Whitepaper v0.6

Blockchain Based Digital Identity

Don Hsieh
Email: don@idhub.network

April 22, 2019

Abstract

Identity is the missing layer of Internet. The IP addresses are linked to machines, not humans. People can not tell the real identity of their counterpart of a transaction. There is a huge need for an effective method to prevent duplicated or fake accounts. A method to uniquely bind a human to an identifier to facilitate the process of identity verification (IDV) is desirable. The identity of a user is fractured and scattered among service providers. The tedious process of remembering different passwords for login to websites is unnecessary. We can help users to reclaim their sovereignty of identity back. Identity is broken. Let's fix it.

IDHub is a digital identity platform based on blockchain. Benefited from decentralized architecture of blockchain and privacy protection via smart contracts, IDHub empowers users with identity sovereignty: "I own my identity and I have full control over my identity." The design principles of IDHub are sovereignty, security, and privacy. Security is achieved by the immutability of blockchain architecture and encryption library such as NaCl. Privacy is provided by distributed storage such as Kademlia. We also follow the guidances stated in the paper "Engineering Privacy." An identity of IDHub is represented by a tree and a graph. Merkle tree realizes the least disclosure of identity attributes. Identity graph illustrates interactions among users. A key attribute of an identity is reputation. Accurate evaluation of borrower's reputation is crucial for credit loans.

Comparing with the competitors, their business models have the problem of token consumption. Their token flow from inspector to holder and then to attestants. The attestants collect significant amount of tokens but they do not answer the question: "how the attestants will use the token?" This results in reluctant attestants. We shall offer an incentive for attestants to join the ecosystem and a monetization mechanism for the token. IDHub solves the problem through advertisements. The advertisers will buy token from the attestants.

IDHub helps migrant workers, refugees, or economically disadvantaged by providing ubiquitous accesses to their digital identities. Combine with attestations of authorities and third parties, IDHub facilitates the process of microcredit, digital payment, and financial inclusion. By building a transparent and reliable ID as a Service (IDaaS) ecosystem, IDHub achieves our ambition: "One identity, one world."

Contents

1 Value Proposition

We propose the IDHUB as a token of exchange in a blockchain based identity system which focuses on sovereignty, security, and privacy. The IDHub system provides:

- Users: strong privacy and security when storing or authorizing identity attributes, and a share of tokens.
- Attestants: improved revenue and a mechanism of monetization.
- Inspectors: less expensive verification process, less fraud, and instant response.

2 Introduction

2.1 Digital Identity

A digital identity is a set of attributes that correlates to an identifier. People without identity are excluded from financial access and social welfare. According to World Bank, 1.7 billion worldwide have no bank accounts [1]. The severity of people without identities is recognized at a global level. The content of United Nations Sustainable Development Goal 16.9 [2] states that by 2030, provide legal identity for all, including birth registration. IDHub aims to help economically disadvantaged, migrant workers, refugees, and unbanked by providing them a digital identity.

People without a legal identity can not apply for a bank account. People without a bank account can not apply for a credit loan. It adds up a vicious cycle of poverty. The bank account holding rate of 60 countries is illustrated in Figure 1. The diameter of each country is proportional to its population. The countries whose bank account holding rate below 20% are Turkmenistan, Guinea, Afghanistan, Iraq, Cameroon, Pakistan, Egypt, Malawi, Haiti, and Nicaragua. Turkmenistan has the lowest rate, which is only 1.8%. They are mainly located in Central Asia, Western Africa, and Central America. People in these regions can hardly participate in financial systems. We may improve their lives by providing them an identity so that they are qualified for opening a bank account. "Banking the unbanked," as the slogan goes.

Identity systems could be categorized into two schemes [3]. The foundational identity schemes are developed as universal multi-purpose systems capable of supporting the entire range of needs for legal identity across all applications. The functional identity schemes are developed in response to a specific application such as safety nets, finance, healthcare, transport, immigration, and elections. In safety nets domain, the identity systems remove fraud using uniqueness and electronic cash transfers. Regarding finance, they accelerate financial inclusion using digital banking and digital payments. They track immunization of children in healthcare domain and issue driver's licenses in transport domain. They help immigration domain by tracking border crossings and issuing passports. They also issue voter credentials to combat vote rigging in elections. Classified in functional identity scheme, IDHub is an identity system which devotes to safety nets and finance domains as highlighted in Figure 2.

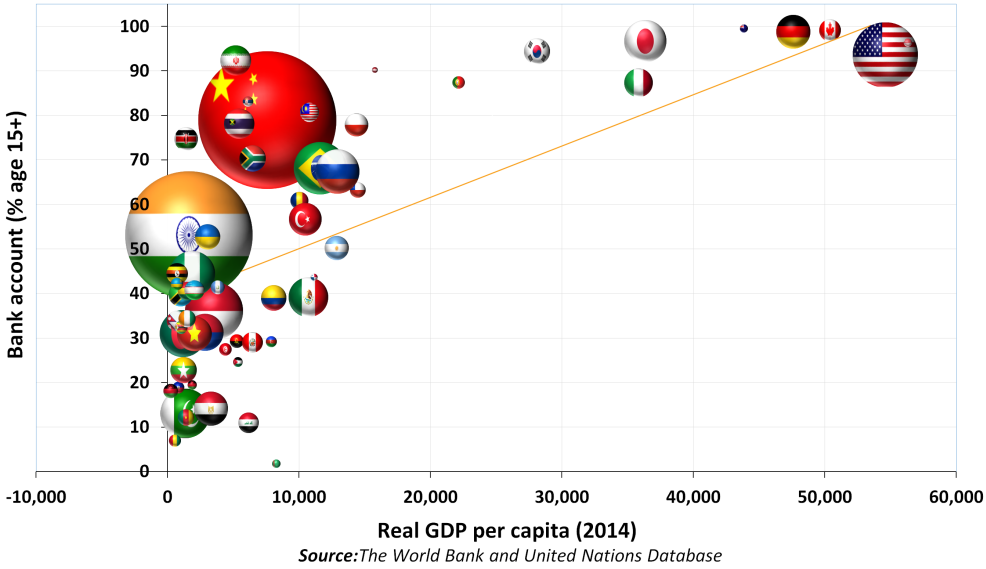

Figure 1: GDP per capita vs. the percentage of having a bank account

2.2 Related Countries

2.2.1 China

The local government of Chancheng district, Foshan city, Guangdong province, China announced Intelligent Multifunctional Identity (IMI) [4] system in June 2017. Based on blockchain and real name authentication, IMI deals with the problem of residents identification online. The three characteristics that IMI claimed are validated information, credible source, and the least disclosure. All identity attributes on IMI are validated because they are endorsed by authorities or other credible sources. Attestations from different sources constitute an identity. A user may have an ID card attestation from the government, an income attestation from a company, and a medical record attestation from a hospital. The least disclosure principle states that the data to be disclosed should be within the smallest scope and returned in coarse-grained value, instead of raw value. For instance, when a user applies for a loan, the value to be disclosed is the range of income, not the exact income value. The residents in Chancheng who are verified by the IMI will be granted access to government services. Using paired public and private keys, the system is also said to be able to verify users' identity automatically without requiring them to be physically present at a service center.

2.2.2 Estonia

Estonia launched its e-Residency program on 1 December 2014. People around the world may apply for e-Residency to obtain entry of the European Union business environment and access to public services. E-Residency facilitates company registration,

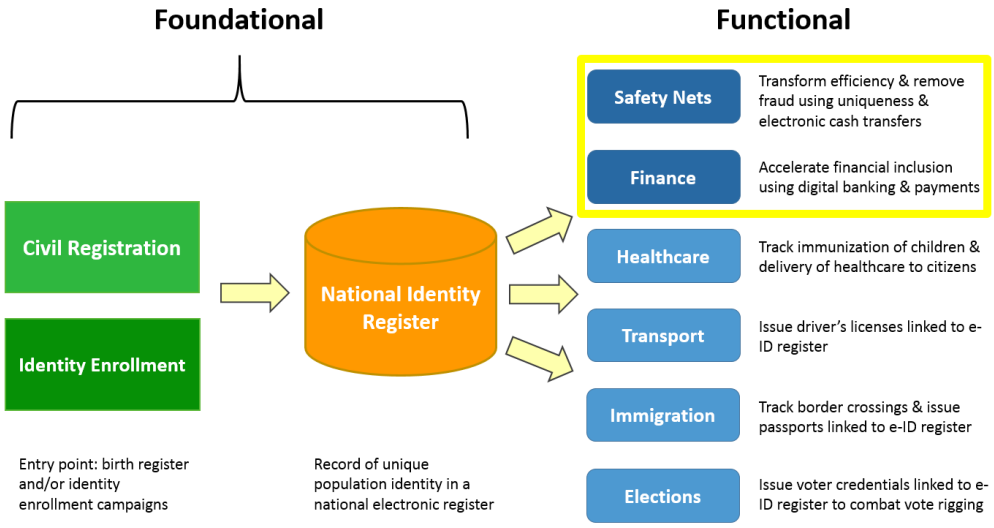

Figure 2: Foundational and functional identity schemes.

document signing, exchange of encrypted documents, online banking, tax declaration, and fulfillment of medical prescriptions. E-Residents pay tax in their native countries, which provide them with the public services, not Estonia. Furthermore, e-Residents will have their financial footprint monitored digitally, in a manner stated to be transparent. E-Residency does not grant the right to reside in Estonia. Besides offering e-Residency program, Estonia is evaluating a way of providing currency to e-Residents.

2.2.3 Malawi

Located in southern east of Africa, Malawi is one of a few African countries not bothered by civil war. Recognized as one of the most underdeveloped countries by United Nations, 55% of Malawi people live under poverty line. Malawi relies on agricultural products export heavily so that Economy of Malawi is sensitive to the price volatility of international agricultural products. The fact that Malawi had no national identity system until 2016 make it suitable to adopt digital identity.

2.2.4 New Zealand

Launched in 2013, RealMe [5] is an identity verification service backed by New Zealand Post. RealMe enables New Zealand citizens to access identity and other online services with one account. The first of two major RealMe functions is a single login to multiple participating online services. If a RealMe account has been verified, it also works as an online ID. The other is a control in privacy of personal information and protection from identity theft. RealMe acts as a gatekeeper and does not store the information shared by users. With the least of disclosed information, third parties can identify the

user and get on with providing a service. [6]

2.2.5 Switzerland

Known as Crypto Valley, Zug is a city of Switzerland that supports cryptocurrency entrepreneurship. Zug launches an Ethereum-based digital identity service which allows residents to exercise digital signature. Zug has a plan to realize e-Voting in the Spring of 2018.

2.3 Related Organizations

2.3.1 ID2020

ID2020 [7] is an alliance committed to improving lives through digital identity. The four criteria they propose are personal, persistent, portable, and private. "Personal" means unique to you and only you. "Persistent" means lives with you from life to death. "Portable" means accessible anywhere you happen to be. "Private" means only you can give permission to use or view data.

2.3.2 Decentralized Identity Foundation

On May 22 at Consensus 2017, panelists from Microsoft, uPort, Gem, Evernym, Blockstack, and Tierion announced the formation of the Decentralized Identity Foundation (DIF). The mission of DIF [8] is to build an open source decentralized identity ecosystem for people, organizations, apps, and devices. DIF believes that the pillars of the new ecosystem are decentralized identities anchored by blockchain IDs linked to zero-trust data stores that are universally discoverable.

IDHub is planning to participate in ID2020 and DIF and to work with them together to fix the identity problem. Among the four working groups of DIF, we are most interested in "Storage & Compute" and "Attestations & Reputation."

2.4 Identity System

The design principles of an identity system are sovereignty, security, and privacy. Current service providers are silos and each of them holds a part of identity attributes. The identities of users are fragmented. The processes of signing to websites which requires different usernames and passwords are tedious and totally unnecessary. The users lose control and ownership of their identities and their privacy are sold for profit. This comes to the first design principle of an identity system: sovereignty. Service providers should return the control back to the users so that they can edit, update, and aggregate their identities seamlessly. The users may delete their accounts as they wish, that is, they have the right to be forgotten. Security is another important principle. Centralized identity systems, such as Aadhaar, had been reported user data leaks. Centralized identity systems are honey pots to hackers since the data they store are highly valuable and the count of their servers are limited. The centralized architecture is also vulnerable

to ransomware attack. The decentralization of blockchain based identity system raises the cost of attack and thus provides security and robustness. Lastly, privacy is a crucial concern of users. The blockchain technology is still in its infant stage of development and is known for some shortages such as privacy. The blockchain is the ground for security but other modules are needed to protect privacy. The basic idea of IDHub design is to utilize blockchain, encryption library and distributed storage to realize the three design principles of an identity system.

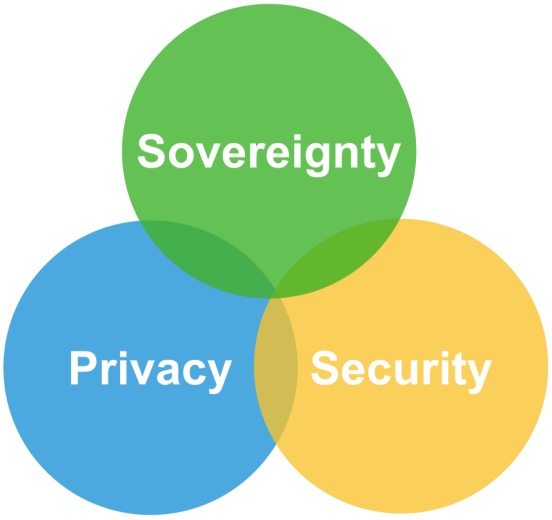

Figure 3: Design principles of an identity system

3 Architecture

Based on the decentralization of blockchain, IDHub is a digital identity applications platform which aims at providing ID as a Service (IDaaS). The amount of accounts per person increases but personal data are controlled and held by service providers, not users themselves. The separation of identity from application is a definite trend in digital society. IDHub realizes the separation by establishing a portable identity management mechanism which reduces barriers and switching costs among service providers. IDHub views identity as a digital asset. To enhance the credibility of claims, IDHub incorporates external attestations as endorsements and builds a verifiable and reliable digital asset ecosystem. IDHub plays a pivot role in data synchronization or migration among service providers, especially when mutual trust does not exist. Besides, IDHub helps local government and residents to build a sustainable and expandable identity system.

The attributes associated with an IDHub identity are called claims. This term originated with claims-based identity, a way of asserting digital identity that is independent of any particular system that needed to rely on it. Since a primary purpose of IDHub identity management is to enable identity owners to easily assert and prove attributes of their identities — personal data, credentials, awards, and degrees. Claims management is at the heart of IDHub architecture. An architecture for verifiable claims must distinguish the essential roles of core actors and the relationships between them; how do they interact? A role is an abstraction that might be implemented in many different ways. The separation of roles suggests likely interfaces or protocols for standardization. The following roles exist in the architecture. Holder acquires attestations from an attestant and selectively provides them to inspectors. An attestant issues attestations to holders. Inspector requests attestations from holders in order to authenticate them. Identifier registry mediates creation and verification of globally unique identifiers. The registry must manage identifiers in a self-sovereign way. Repository stores and curates attestations on behalf of holders. Verifier verifies attestations on behalf of inspectors. For example, inspectors may provide deeper verification by applying certain industry-specific business rules on attestations.

Main identity related actions are registration, attesting, and authorization. An identity is registered through smart contracts and bind the identity with a public key. Delegation is set in case of identity recovery is needed. The value and correctness of users data are guaranteed by attestations from credible attestation issuers. Credible individuals or organizations sign claims with their private key and inspectors verify the claims with public key of the signers. Authorization module notifies users when third party requests their data. Upon with acknowledgment of users, data in permission scope are returned to third party.

The infrastructure of IDHub is a peer-to-peer network powered by blockchain nodes. Utility layer is constituted by common functional components such as identifier registry, claim definition, and proof verification. Four modules built on the infrastructure are identity management, identity verification, dApp interface, and digital asset. The users manage their identities through registration, attributes editing, links to other users, and

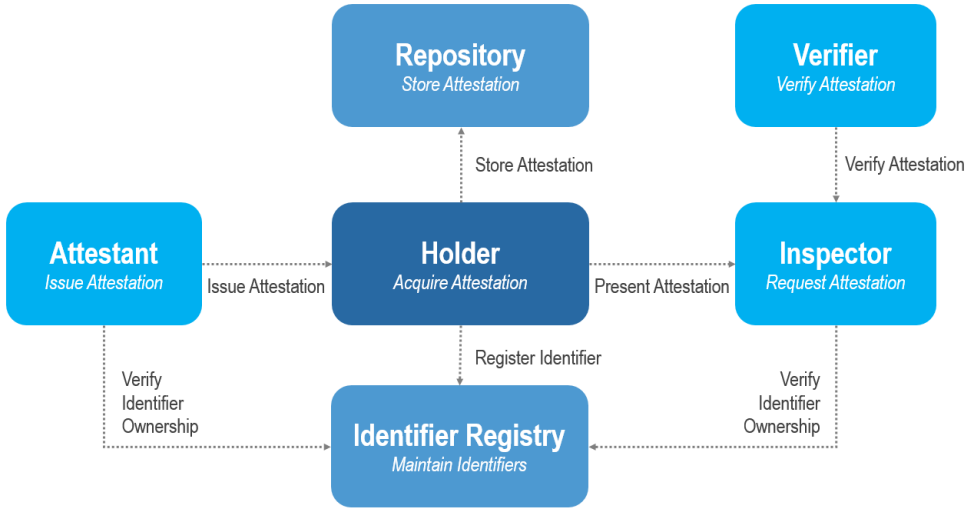

Figure 4: Roles: Holder, Attestant, Inspector, and Verifier

recovery. Identity verification service includes OAuth and digital signature. Contract server retrieves public data and action logs on blockchain. DApp interface service facilitates the interaction between dApp and blockchain. Digital asset service evaluates the current value of user's identity and provides transaction capability. The services are used to develop solutions in finance, education, healthcare, commerce, and travel domains.

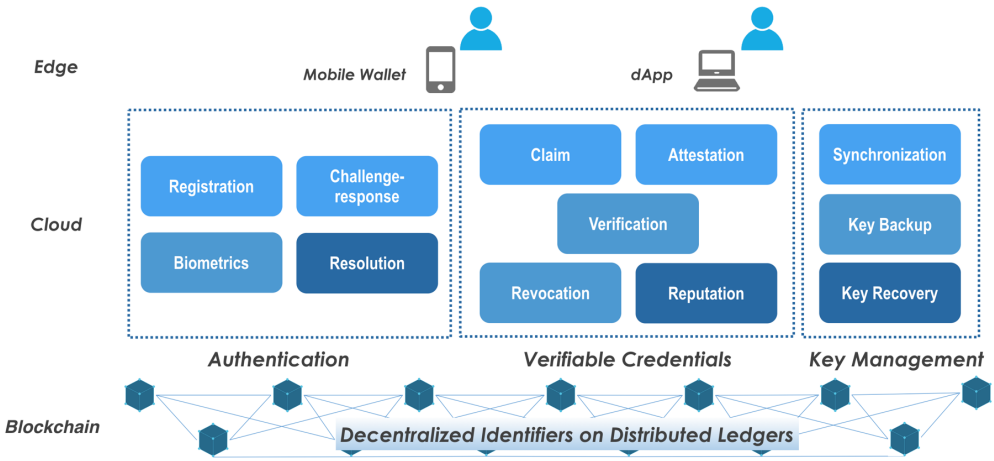

Figure 5: IDHub architecture

3.1 Decentralized Identifier (DID)

Traditional identifiers are assigned by authorities or service providers. Users do not own their traditional identifiers. Decentralized identifiers (DIDs) are created by users themselves with no intermediary and can not be taken away by other individuals or institutions. DIDs are designed to be interoperable among blockchains. DID methods define how DIDs work with a specific blockchain and the generation of the method-specific identifier. The method specific identifier string must be unique in the namespace of that DID method. As globally unique identifiers, DIDs are colon-delimited strings consisting of a scheme name followed by a DID method name followed by a method-specific identifier. Here is an example DID that uses the ERC-725 method:

```
did:erc725:0x20e3B03194756C58B7beD0746DcF570FA2fB7640
```

The method-specific identifier of this DID is an Ethereum address. Each DID is associated with a DID Document. A DID Document is a JSON-LD object that is stored in some cloud storages so that it can be easily looked up. The DID Document must include a DID. It might include things like: a list of cryptographic public keys, a list of ways that the DID can be used to authenticate, a timestamp of when it was created, a cryptographic proof that the DID Document is valid, and a list of services where the DID can be used any number of externally defined extensions. Here is an example DID Document:

```
{
  "@context": "https://w3id.org/did/v1",
  "id": "did:erc725:0x20e3B03194756C58B7beD0746DcF570FA2fB7640",
  "publicKey": [{
    "id": "did:erc725:0x20e3B03194756C58B7beD07...#key-1",
    "type": [
      "Secp256k1SignatureVerificationKey2018",
      "ERC725ManagementKey"
    ],
    "publicKeyHex": "1a0cb8f32c94921649383b14523cb6df04858cf..."
  }, {
    "id": "did:erc725:0x20e3B03194756C58B7beD07...#key-2",
    "type": [
      "Secp256k1SignatureVerificationKey2018",
      "ERC725ActionKey"
    ],
    "publicKeyHex": "00e17b0f13af42bd7c992ef991ebd75f8345b5e..."
  }],
  "authentication": {
    "type": "Secp256k1SignatureAuthentication2018",
    "publicKey": "did:erc725:0x20e3B03194756C58B7beD07...#key-2"
  },
  "service": ["https://api.idhub.network/api/v1/resolve/"]
}
```

Each DID method specification defines the specific distributed ledger against which the DID method operates. The CRUD operations (create, read, update, delete) for DIDs and DID documents on that ledger should be stated as well.

3.2 Claim

A claim is a set of attributes which assigned by users themselves. Identity attributes should follow the format of schema.org whenever possible. Some of the listed attributes are identifier, image, familyName, givenName, email, address, telephone, birthDate, birthPlace, netWorth, jobTitle, height, and weight [9]. The correctness of self-declared claims may be challenged. Claims become valuable when they are endorsed by authorities, that is, an attestation is issued and attached to the claims.

3.3 Attestation

The validity of a claim is guaranteed by its attestation which is in the format of JSON Web Token (JWT) [10]. JWT is an open standard (RFC 7519) that defines a compact and self-contained way for securely transmitting information between parties as a JSON object. This information can be verified and trusted because it is digitally signed. The structure of JWT consists of three parts separated by dots, which are header, payload and signature. The header consists of the type of the token, which is JWT, and the hashing algorithm being used, such as ES256k or RSA. Payload contains the claims. Claims are statements about an entity and additional metadata. Some of reserved claims are issuer, expiration time, subject, audience. Signature is obtained through signing the encoded header and the encoded payload with private key and the specified algorithm in the header. The signature is used to verify the issuer of the JWT and to ensure that the message remains intact along the transmission.

Attestations of identity attributes are valuable and sensitive. A satisfying credential management system fulfills the least disclosure principle which states the identity system should disclose the minimum amount of information about a given entity needed to facilitate the transaction and no more. The reason for following this principle is to both maintain privacy and mitigate the potential side effects of disclosure. The nature of Merkle tree suits least disclosure principle well. A Merkle tree is a tree in which every leaf node is labeled with a data block and every non-leaf node is labeled with the cryptographic hash of the labels of its child nodes. Merkle trees allow efficient and secure verification of the contents of large data structures. Least disclosure is achieved by providing specific hash, therefore only needed data are disclosed.

3.4 Authorization

Authorization is brought into play when a third party requests user data. Data within the scope specified by user are granted if user permits the authorization. OAuth 2.0 is implemented in the authorization process of IDHub. The OAuth 2.0 authorization framework [11] enables a third party to obtain limited access to an HTTP service on behalf of a resource owner by orchestrating an approval interaction between the resource owner and the HTTP service. OAuth 2.0 provides third parties a delegated access to server resources on behalf of resource owners without sharing their passwords.

3.5 Privacy

We put privacy protection at the heart of IDHub design. An identity system should view privacy as top priority to earn trust from users. The eight privacy design strategies are grouped into two classes: data-oriented strategies and process-oriented strategies [12]. Data-oriented strategies includes MINIMISE, HIDE, SEPARATE, and AGGREGATE. The amount of personal data that is processed should be restricted to the minimal amount possible. Any personal data, and their interrelationships, should be hidden from plain view. Personal data should be processed in a distributed fashion, in separate compartments whenever possible. Personal data should be processed at the highest level of aggregation and with the least possible detail in which it is useful. Process-oriented strategies includes INFORM, CONTROL, ENFORCE and DEMONSTRATE. Data subjects should be adequately informed whenever personal data is processed. Data subjects should be provided agency over the processing of their personal data. A privacy policy compatible with legal requirements should be in place and be enforced. Be able to demonstrate compliance with the privacy policy and any applicable legal requirements. The eight privacy design strategies are diagrammed in Figure 6.

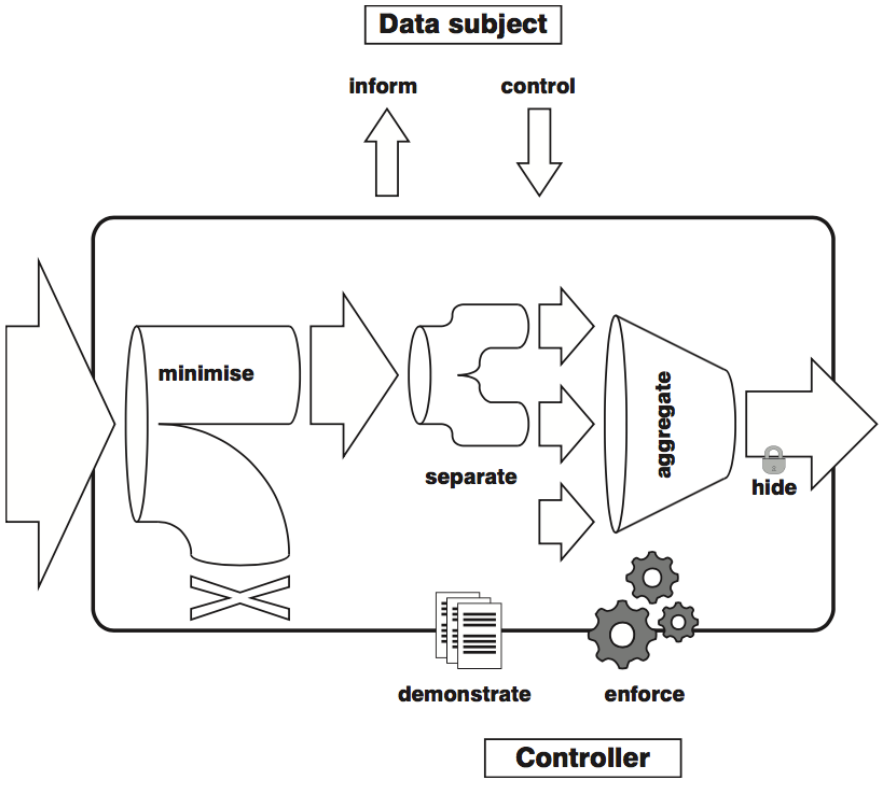

Figure 6: Eight privacy design strategies.

To enforce these strategies, data collection is minimized. Each data request must be approved by user. Selective disclosure is considered in the process of user data

granting. The returned data are coarse grained, not the raw data. This is achieved by zero-knowledge proof cryptography. It is suggested not to store their private data on blockchain, even in encrypted form. Because encryption will eventually be broken by quantum computing.

If an identifier is used repeatedly, the user will be at the risk of data correlation. Instead of having just one public identifier, users should have hundreds of pairwise-unique identifiers issued on a per-relationship basis. The significant amount of identifiers raise the need for an effective system to manage their private keys. That system is called a Decentralized Key Management System (DKMS).

3.6 Identity Graph

An identity graph is a representation of actions among identities. In the graph, nodes are identities and edges are actions. The actions includes adding a friend, an endorsement, and a comment. By converting actions to transactions on blockchain, the reputation of identity can be calculated according to transactions logs. Flow-based programming [13] is suitable for handling data flow in the identity graph since it views an application as a network of asynchronous processes communicating by streams of data chunks. The focus is on the application data and the transformations applied to it to produce the desired outputs. The network is defined externally to the processes.

An identity of IDHub system is represented by a tree and a graph. Claims and attestations of the identity are stored in a Merkle tree while the interactions with other identities are stored as an identity graph.

3.7 Security

IDHub stores index of data on blockchain and value of data in distributed storage system, such as Kademlia [14]. Blockchain is famous for its transparency and immutability. Data on blockchain are immutable unless attackers dominate the majority of computing power of the blockchain, which is infeasible. Kademlia is a peer-to-peer distributed hash table which defines the distance between hash keys as their bitwise exclusive or (XOR). With its novel XOR-based metric topology, Kademlia has desirable features such as provable consistency and performance, latency minimizing routing, delay-free fault recovery, and a symmetric, unidirectional topology. Kademlia uses parallel, asynchronous queries to avoid timeout delays from failed nodes. The algorithm with which nodes record each other's existence resists certain basic denial of service attacks. Using a distributed storage system, IDHub is more secure and robust than a centralized identity system, such as Aadhaar. Security can be further enhanced by encryption before storage. An ideal example of encryption tool is NaCl [15] [16]. NaCl (pronounced "salt") is a high-speed library for network communication, encryption, decryption, and signatures.

3.8 Uniqueness

The uniqueness plays a crucial role in the identification process of social welfare payment and the elimination of fictitious workers. A unique identity ensures that no citizens receive duplicate social welfare payments. Nigeria implemented an digital identity system for civil servants and removed fictitious workers to save $76.6 million annually [17]. Biometric identification refers to identifying an individual based on physiological or behavioral characteristics. Biometrics such as face, facial thermogram, fingerprints, hand geometry, iris, retinal pattern, signature, and speech are evaluated and compared [18]. The most desirable biometrics are fingerprints and iris. They are adopted by Aadhaar to distinguish users. Besides them, facial thermogram looks promising. The underlying vascular system in the human face produces a unique facial signature when heat passes through the facial tissue and is emitted from the skin [19]. A facial thermogram is an image of facial signatures captured by an infrared camera. It is unique to each individual and is not vulnerable to disguises. Even plastic surgery, which does not reroute the flow of blood through the veins, have no effect on the formation of the facial thermogram. The steps of converting a fingerprint to a QR code involves [20]: extracting the core point of fingerprint, extracting features of fingerprint, converting features to numerical values, and generating a QR code by numerical values. The most common method used to find the core point is the Poincaré index method. In fingerprints, minutiae, the discontinuities in the ridge pattern, are major features which are used to compare one print with another. Two types of minutia, the ridge ending and the bifurcation are selected for feature extraction.

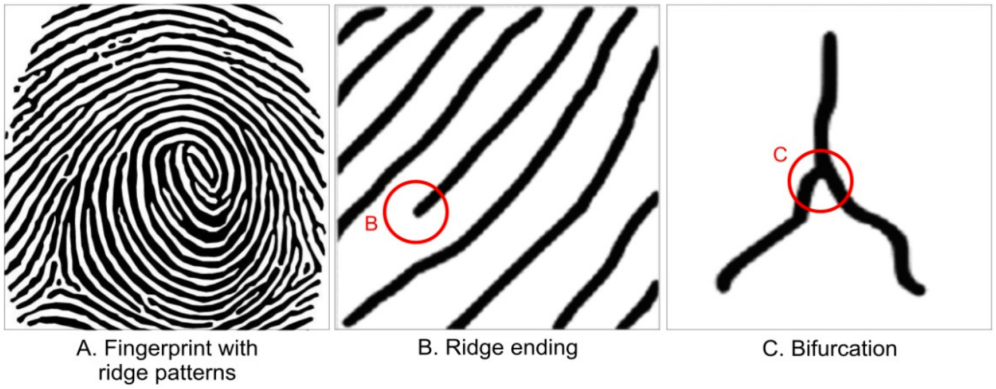

Figure 7: Fingerprint ridge patterns and minutiae.

IDHub realizes the uniqueness of identity by two types of biometrics: fingerprints and iris. Facial thermogram will be considered when its cost is evaluated as affordable.

3.9 Portability

The fact that identities of user are scattered among websites is cumbersome. Repeated login to different websites everyday is inconvenient and unnecessary. Worse yet, the

formats of identity attributes on websites are incompatible, making them silos. Identity sovereignty refers to users have full control over their identities. One indicator of sovereignty is that user can switch among websites seamlessly. IDHub makes identity portable by exporting attributes from social networks and then synchronizing to diaspora [21]. Diaspora is a privacy-aware, user-owned, distributed, open source social network. Social networks profit by analyzing user interactions and using this to advertisement. Diaspora does not use user data for any purpose other than allowing user to connect and share with others.

4 Competitive Landscape

4.1 Aadhaar

The amount of social welfare subsidy that government of India transfers to citizens living below poverty line is reduced by corrupted officers. To tackle this problem, each recipient should be identifiable so that transferring subsidy to them directly is possible. Aadhaar [22] number is a 12 digit unique-identity number issued to Indian residents. The Aadhaar number, due to its uniqueness property, serves as a natural financial address for sending payments to accounts of beneficiaries. Using Aadhaar as financial address gives end to end traceability of an individual's entitlement. Government puts in subsidy to an Aadhaar number and the beneficiary with the Aadhaar number takes out subsidy at a microATM. Aadhaar enables the economically disadvantaged and marginalized to access public services and welfare entitlements by disintermediation. 1.171 billion Aadhaar numbers had been issued. Deduplication is one of the main goals that Aadhaar devoted to. Aadhaar distinguish residents by collecting their biometric information such as photograph, ten fingerprints and two iris scans. Aadhaar stores residents data in MySQL databases.

4.2 Civic

Civic [23] proposes a method to reduce the costs of identity verification industry. Organizations that have investigated in identity verification services may monetize their processes. Building on the distributed data model, the attestation model, and the token, Civic will provide a platform for attestations to be shared between identity verification service providers in order to compensate participants, and keep users in full control of their data. Civic stores a user's data on the user's phone using encryption and biometric locks. The verification process for user data is conducted by Civic. Once fully verified, the attestations to data are written by Civic to the blockchain. Civic's identity partners can request a user's data through custom QR codes to be scanned by the user. The user scans these codes, reviews data requested, and decides whether to approve or deny the request.

4.3 GSMA Mobile Connect

Mobile Connect [24] is a secure universal login solution proposed by GSMA, an association of mobile operators. Mobile Connect matches users to their mobile phone numbers and allows them to log in to websites. Its login mechanism is based on OpenID Connect. Mobile Connect is mainly a third party login module, instead of a full-fledged identity system.

4.4 Sovrin

Sovrin [25] is a decentralized identity network. It allows people and organizations to create portable, self-sovereign digital identities controlled by the owners. The Sovrin

Identity Network (SIDN) consists of multiple, distributed nodes located around the world. With each node has a copy of the ledger, the nodes are hosted and administered by stewards. Once identity attributes are requested and granted, relying party can verify its correctness by the digital signature of its attestant. With distributed management, Sovrin may guarantee the integrity and security of identity attributes and avoid tampered identity. Sovrin makes itself a reliable source which is robust to system failure, resilient to hacking, and immune to subversion by hostile entities. A disadvantage of Sovrin is that it relies on people being responsible for determining whether or not to trust something. As an open source public identity network, the identity information on it does not have authoritative credibility. How well it works depends on the user experience and whether people understand what is being asked of them. [26] The solution proposed by IDHub is to work with the real world authoritative attestation providers such as governments and banks. These authorities can enhance the credibility of the system significantly.

4.5 uPort

uPort [27] is an Ethereum-based smart contract system. The uPort technology consists of three main components: smart contracts, developer libraries, and a mobile app. The mobile app holds the user's keys. Smart contracts form the core of the identity and contain logic that allows users recover their identity when mobile device is lost. The developer libraries help developers integrate uPort into their apps. A core function of a uPort identity is that it can digitally sign and verify a claim, action, or transaction. Identities are capable of updating this file themselves, such as adding a photo or a friend, or granting others temporary permission to read or write specific files. Since they can interact with blockchains, uPort identities can also control digital bearer assets such as cryptocurrencies or other tokenized assets.

5 Ecosystem

5.1 IDHUB Token

The primary usage of the IDHub token (IDHUB) is to prove the identity of a user, offer an incentive for attestants to make attestations, and allocate storage for identity attributes. The maximal total supply of IDHUB will be 500 million, with 44% being distributed to crowdsale participants and 16% being distributed to pre-sale participants. The founding team will receive a share of 20%, which will be vested for 4 years. 10% of the tokens will be allocated to the IDHub Foundation fund to be used for research and development, administration, community operation, market penetration, and legal consultancy. The early backers will hold a share of 10%.

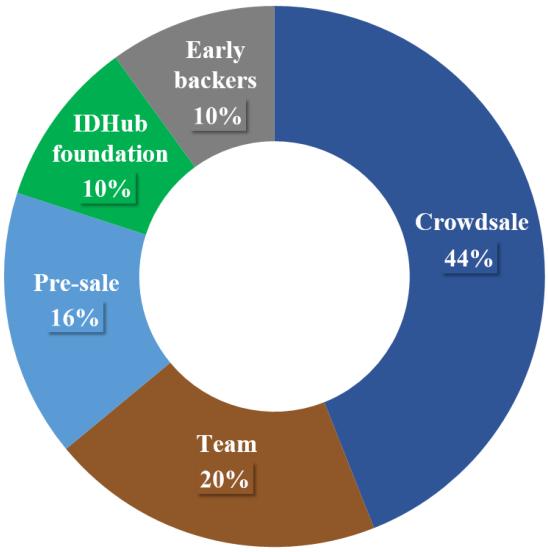

Figure 8: IDHUB Token Distribution

5.2 Attestation

The token IDHUB flows to value providers. Holders are those who claim some attributes that they own. A claim is reliable and valuable if it is endorsed by third parties. Attestants validate the claims and issue attestations to holders while holders rewarding attestants with IDHUB. Inspectors request endorsed claims from holders and pay them IDHUB. Inspectors may verify the attestations themselves or pay verifier to verify the effectiveness of the attestations. The token IDHUB flows from inspectors to holds to attestants. IDHub offer an incentive to the attestants since they make IDHub ecosystem more trustworthy and valuable.

5.3 Security Token Offering

Security Token Offering (STO) is a promising way for crowdfunding that takes investor protection, compliance, fraud prevention, and risk disclosure into considerations. Regulations that exempt a STO are Reg A+, Reg CF, Reg D, and Reg S. To meet the requirements from regulators, only accredited investors are allowed to participate in a STO. Know Your Customer (KYC) and Anti-Money Laundering (AML) are conducted in the process of investor accreditation. IDHub provides KYC/AML and wallet services to serve as infrastructure of STO. The services improves market liquidity for asset trading. Both individual and institutional investors will be benefited from this opportunity.

5.4 Loan

Reputation is a decisive attribute of an identity. The person who owns a good reputation or a high credit score may enjoy a lower interest rate when applying for a loan. Accurate credit score evaluation requires substantial amount of data for training model. A strength of IDHub over competitors is the quantity and quality of user data. Unlike competitors who evaluate credit scores solely on transaction records of users, IDHub has additional data sources from attestations, daily behaviors, and interactions among identities. This yields a holistic view of reputation of an identity. Based on the credit score evaluated, IDHub may suggest a proper range of interest rate when reviewing a loan application of the user. A major concern of lenders is default risk. IDHub supports group lending or the securitization of loans to reduce the risk. A mechanism of loan insurance will be considered if lenders demand further safety in the future. For the convenience of borrowers, IDHub provides automatic exchange of IDHUB and local currencies. Borrowers may repay the loan with local currencies if they wish.

5.5 Advertising

Advertisers suffer losses from frauds and consumers are annoyed by privacy breaches. IDHub can help both of them and reshape the advertising industry. Malicious bots trigger impression or click frauds to harvest from advertising campaigns. Advertisers pay for fake clicks which yield zero results. The privacy data of consumers are sold for profit forcibly. The solution proposed by IDHub is to share advertising revenues with consumers. Consumers decide whether they will read advertisements, and they will be rewarded with IDHUB if they do. If consumers purchase through clicked advertisement, they earn even more IDHUB. For advertisers, the nightmare of ineffective expenditures is over. Each IDHub user is verifiable human, not bot. Advertisers are charged only when authenticated users browse or click their advertisements. Consumers browse advertisements voluntarily and proactively since they have a share of the revenue. An additional advantage that advertisers gain is precise marketing. The identity attributes of IDHub users are attested and the correctness of data forms a solid foundation of user preferences discovery. Both consumers and advertisers are benefited in this win-win situation created by IDHub ecosystem.

5.6 Supply Chain

IDHub will expand identity solution to supply chain. By assigning an identity to each participant of the supply chain, adjusting reputations according to their behaviors, rewarding honest behaviors with IDHUB, the supply chain will be more transparent and effective. Food traceability is a pressing concern to consumers. Take grape wine as an example, it has high economic value and it is easily adulterated. In every stage of the supply chain, chemical profile analysis is conducted to verify the authenticity of the product. The roles of supply chain participants are classified as: Grape Grower, Wine Producer, Bulk Distributor, Transit Cellar, Filler/Packer, Finished Goods Distributor, and Retailer. We build an identity for each participants and their reputations are accumulated as they keep providing authentic products. If a fraud occurs, the reputations of relevant participants are downgraded and the event is broadcasted along the supply chain instantly. In the case of fraud or product recall, IDHub will identify the root of cause within 24 hours. Regarding to interoperability, the system is compliant with international standards such as GS1. The system will build a rewarding mechanism to offer an incentive for honest behaviors. In the IDHub ecosystem driven by participants with good reputation, the end consumers can have confidence in their foods. Start from grape wines, IDHub has the ambition to include other foods to reach food security globally. The design goals are ease of use, low cost, and automation. A prototype is expected to be deployed in Portugal with 200 farmers.

5.7 Business model

The core business of IDHub is identity verification. The extended business scope includes loan (based on credit score) and advertisement (based on authentic identity). Our value proposition is to reduce the cost of identity verification. The inspectors can save their time by buying the attestations they need. The attestants are rewarded with the token IDHUB since they provide credible data and increase the value of system. The users have full control over their identities and their privacy is protected. Our key partners are attestant, community, lender, and advertiser. The community members are the early adopters of IDHub and they contribute to our GitHub repository. Besides identity verification, transaction is another key activity. The transaction records of users serve as a basis for their credit score evaluation. The dominant resource is attestation. The connection with the attestants is also important since the more attestants we have, the more powerful the ecosystem becomes. The targeted customers are attestation holders, inspectors, and advertisers. To maintain customer relationships, we have loyalty program which provides bonus or discount. Gamification is used to enhance user experience and customer engagement. The channels we used to reach potential users are meetup, roadshow, media, and referral program. The main costs are marketing, product development, and administrative costs. Our revenue streams comprise authorization fee, loan fee, and advertising fee.

The business model canvas of IDHub is summarized in Figure 9.

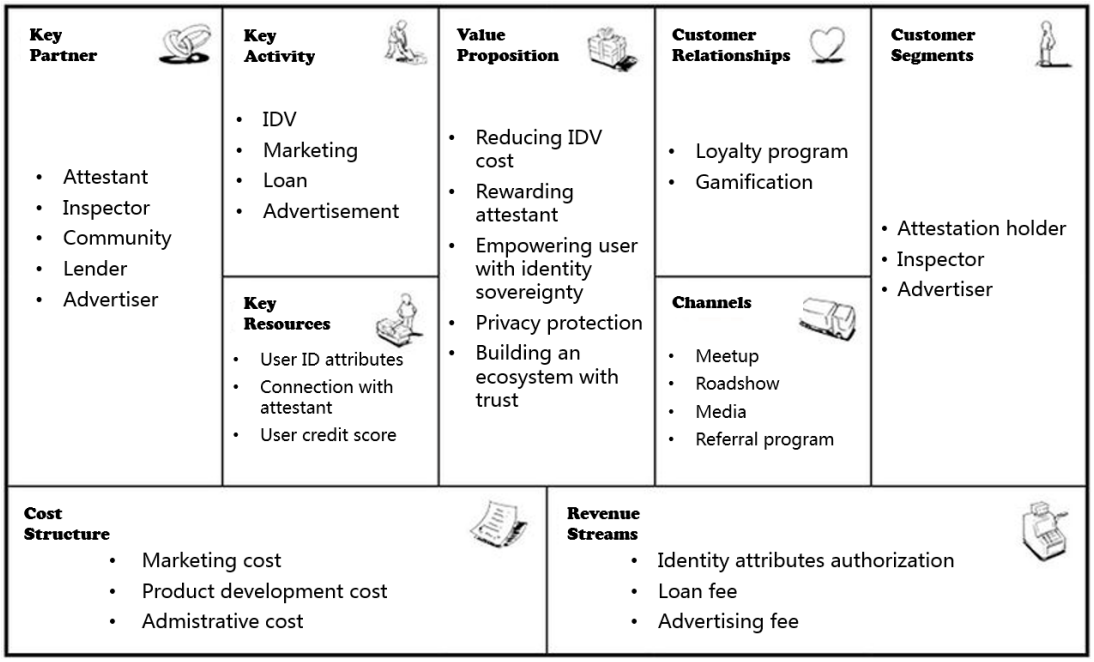

Figure 9: Business model canvas

6 Compliance

6.1 European Union Data Protection Directive of 1995

Known as Directive 95/46/EC, European Union Data Protection Directive is a regulation to protect personal data and privacy of European Union citizens. Directive 95/46/EC is founded on seven principles: 1) Subjects whose data is being collected should be given notice of such collection. 2) Subjects whose personal data is being collected should be informed as to the party or parties collecting such data. 3) Once collected, personal data should be kept safe and secure from potential abuse, theft, or loss. 4) Personal data should not be disclosed or shared with third parties without consent from its subject(s). 5) Subjects should be granted access to their personal data and allowed to correct any inaccuracies. 6) Data collected should be used only for stated purpose(s) and for no other purposes. 7) Subjects should be able to hold personal data collectors accountable for adhering to all seven of these principles.

6.2 Health Insurance Portability and Accountability Act of 1996, HIPAA

HIPAA regulates the healthcare industry in the United States. The main modules of HIPAA are privacy of patients, exchange of electronic medical record (EMR), immutable of EMR, and storage of EMR. IDHub protects the privacy of patients through OpenPDS and supports storage and immutable of EMR through blockchain. Terminology used in the exchange of EMR shall compile with Health Level 7 (HL7) standard. Traditional insurance claim application requires full medical record of insurant. IDHub can satisfy the need of insurance claim application without disclosing medical record. Therefore, IDHub implements a more rigorous approach than what HIPAA regulations demands.

7 Team

Doer Qu
Founder
Council member of Connected City Advisory Board (CCAB)

Kenneth Chen
CTO
Former CTO of APTG
Co-Founder & CTO of Genie Networks Ltd.

Xiaoyu Li
Core Developer

Don Hsieh
Core Developer

Zeqian Yao
Developer

Abbie Lin
Developer

Yupeng Liu
Developer

Arthur Hsiao
Developer

Kevin Lee
Developer

Jiaqi Li
Developer

Michael Wang
Business Development

Cecilia Wu
Marketing Director

Leo Cao
Marketing Manager

Derek Xue
Marketing & PR Manager

8 Roadmap

- 2017
  - Q3: The IDHub project launched.
  - Q4: IDHub was a finalist in blockchain application contest.
- 2018
  - Q1: IDHub Foundation was registered in Singapore.
  - Q2: IDHub acquired the membership of Enterprise Ethereum Alliance (EEA).
  - Q3: IDHUB tokens were listed on exchanges.
  - Q4: Decentralized identifier release.
- 2019
  - Q1: Mobile wallet release.
  - Q2: Cloud storage integration.
  - Q3: Credit score integration.
  - Q4: Biometrics integration.

9 Conclusion

IDHub helps migrant workers, refugees, or economically disadvantaged by providing ubiquitous accesses to their digital identities. Having a digital identity, economically disadvantaged can access to social welfare directly without the deprivation from intermediary. User data are secured by the transparent, immutable, and robust blockchain architecture. Privacy protection is guaranteed via Merkle trees which realizes the least disclosure principle.

References

[1] Asli Demirgüç-Kunt et al. *The Global Findex Database 2017: measuring financial inclusion and the Fintech revolution*. The World Bank, 2018.

[2] Division for Sustainable Development. *Sustainable Development Goal 16*. `https://sustainabledevelopment.un.org/sdg16`. Accessed at 2019-03-14.

[3] Joseph Atick. "Digital identity: the essential guide". In: ID4Africa Identity Forum. 2016.

[4] Coindesk. *Local Government in China Trials Blockchain for Public Services*. `https://www.coindesk.com/local-government-china-trials-blockchain-public-services`. Accessed at 2019-03-14.

[5] New Zealand Post. *RealMe*. `https://www.nzpost.co.nz/personal/realme-id-apply/realme`. Access at 2019-03-14.

[6] New Zealand Government ICT. *RealMe Verified Account Service*. `https://www.ict.govt.nz/services/show/RealMe-Verified-Account-Service`. Access at 2019-03-14.

[7] Inc Identity2020 Systems. *ID2020*. `https://id2020.org`. Accessed at 2019-03-14.

[8] Decentralized Identity Foundation. *DIF*. `http://identity.foundation`. Accessed at 2019-03-14.

[9] Schema.org. *Person*. `https://schema.org/Person`. Accessed at 2019-03-14.

[10] Michael Jones, John Bradley, and Nat Sakimura. *Json web token (jwt)*. Tech. rep. 2015.

[11] Dick Hardt. *The OAuth 2.0 authorization framework*. Tech. rep. 2012.

[12] Jaap-Henk Hoepman. "Privacy design strategies". In: *IFIP International Information Security Conference*. Springer. 2014, pp. 446–459.

[13] J Paul Morrison. *Flow-Based Programming: A new approach to application development*. CreateSpace, 2010.

[14] Petar Maymounkov and David Mazieres. "Kademlia: A peer-to-peer information system based on the xor metric". In: *International Workshop on Peer-to-Peer Systems*. Springer. 2002, pp. 53–65.

[15] Daniel Bernstein, Tanja Lange, and Peter Schwabe. "The security impact of a new cryptographic library". In: *Progress in Cryptology–LATINCRYPT 2012* (2012), pp. 159–176.

[16] Daniel J Bernstein, Tanja Lange, and Peter Schwabe. "NaCl: Networking and cryptography library". In: *http://nacl.cr.yp.to* (2011).

[17] Reuters. *Tanzania orders probe into "ghost workers" on government payroll*. `https://goo.gl/5qFpBB`. Accessed at 2019-03-14.

[18] Anil Jain, Ruud Bolle, and Sharath Pankanti. *Biometrics: personal identification in networked society*. Vol. 479. Springer Science & Business Media, 2006.

[19] Francine J Prokoski. "Disguise detection and identification using infrared imagery". In: *Optics and Images in Law Enforcement II*. Vol. 339. International Society for Optics and Photonics. 1983, pp. 27–32.

[20] Sajan Ambadiyil, KS Soorej, and VP Mahadevan Pillai. "Biometric Based Unique ID Generation and One to One Verification for Security Documents". In: *Procedia Computer Science* 46 (2015), pp. 507–516.

[21] Diaspora Foundation. *The Diaspora Project*. `https://diasporafoundation.org`. Accessed at 2019-03-14.

[22] Unique Identification Authority of India (UIDAI). *Aadhaar*. `https://uidai.gov.in/my-aadhaar/about-your-aadhaar.html`. Accessed at 2019-03-14.

[23] Civic Technologies. *Civic Whitepaper*. `https://goo.gl/xzKvN7`. Accessed at 2019-03-14. 2017.

[24] GSMA. *Introducing Mobile Connect – the new standard in digital authentication*. `https://www.gsma.com/identity/mobile-connect`. Accessed at 2019-03-14.

[25] Sovrin Foundation. *Sovrin*. `https://sovrin.org`. Accessed at 2019-03-14.

[26] Phil Windley. *Sovrin Web of Trust*. `http://www.windley.com/archives/2017/05/sovrin_web_of_trust.shtml`. Accessed at 2019-03-14.

[27] uPort. *uPort Protocol Specs*. `https://github.com/uport-project/specs`. Accessed at 2019-03-14.

D:20190422144245+08'00'