



## **EverID WHITEPAPER**

V= # 2018February14.GA.1

EverID.net

Bob Reid - Bob@EverID.net

Brad Witteman - Brad@EverID.net

## Table Of Contents

<b>i. Glossary</b>	4
<b>1. Abstract</b>	5
<b>2. Introduction &amp; Problem Statement</b>	6
<b>3. EverID Principles</b>	9
a. Organizational decisions derived from principles	10
b. EverID Organizational Operation:	11
c. Organizational Mandates:	12
d. Technological decisions derived from principals	13
<b>4. Design Approach</b>	16
a. Decentralized ID hub for individuals	16
b. EverID Platform	16
c. Points of Access to Identity	17
<b>5. EverID Decentralized Identity Platform</b>	19
a. EverID Overview and Technology Stack	19
b. EverID Technology Stack Diagram	20
c. EverID Architecture Diagram	21
d. Biometrics	21
e. EverID Datagram	22
f. EverID DApps	23
g. EverID Application Programming Interface (API)	24
h. EverID Core Smart-contracts	25
i. Ethereum Private Blockchain	27
j. EverID Supernodes	27
Portals	28
 EverID Whitepaper	 1

Bridge System	29
Conduit System	29
<b>6. The EverID Logic Flows</b>	<b>30</b>
a. Individual Self-Enrollment	30
b. Agent Enrollment of an EverID	31
c. Validation of the EverID	32
<b>7. The ID + CRDT Economy</b>	<b>33</b>
<b>8. Conclusion</b>	<b>38</b>
<b>9. Acknowledgements</b>	<b>39</b>
<b>Addendum 1 - ID + CRDT = Utility Token &amp; Credit Currency</b>	<b>40</b>
Seed funding	41
Presale and Crowdsale	42
Funding the Identity Network Foundation	42
<b>Addendum 2 - Organizational Identities</b>	<b>45</b>
<b>Addendum 3 - EverID Datagram</b>	<b>47</b>
<b>Addendum 4 - EverID API</b>	<b>48</b>
<b>Addendum 5 - EverID Use Cases</b>	<b>52</b>
Individual:	52
Individual Enrollment (Agent)	52
Identity Verification, Healthcare & Food Assistance	53
Energy Subsidy Grant and Renewal	54
Organizational:	55
Subsidized Vaccination Distribution Program	55
Refugee Enrollment and Service Delivery	55
Refugee Employment Services	56
EverID Whitepaper	2



## i. Glossary

Biometrics	The measurement and analysis of unique physical or behavioral characteristics of individuals (such as fingerprint, voice patterns)
Blockchain	A merkle signature schema invented to record the Bitcoin cryptocurrency's transactions. It is an unalterable transaction ledger that acts as the source of trust in that system. Other innovations on top of the blockchain include Smart Companies, Smart Contracts and DApps.
DApp	Decentralized application delivered from a distributed (peer-to-peer) or decentralized network, rather than a centralized server infrastructure.
Distributed Computer	A computing infrastructure that is dynamically created from a series of peer-to-peer nodes running the same software.
Ethereum	The base blockchain technology underlying the EverID stack. It is a proven, trusted open-source system which is built by a highly-engaged distributed organization and which has a vibrant developer community.
IPFS	Interplanetary File System <a href="https://ipfs.io">https://ipfs.io</a>
Public/Private key pair	The cryptographic set of keys used to identify users and to secure transactions on the blockchain.
Smart Contract	Program on the blockchain which enables for the automated completion of transactions based upon conditions, prerequisites, or user actions.
Solidity	The smart contract framework within Ethereum, containing code which runs within the Ethereum Virtual Machine contained in the Ethereum wallet.
Token	Token - currency in distributed application ecosystem stored in wallets
Wallet	A decentralized software application that can address a cryptocurrency blockchain to transfer cryptocurrency. Includes a user's Public/Private key pair.

# 1. Abstract

All value exchange and economic activity, at its root, is based on trust. Historically, humans required banks, governments, contracts, centralizing agents to aid the trust process, to verify the person is who they say they are, that they have certain attributes, like a wallet or account, a document, etc. Trust & identity, and therefore all value exchange, have been hampered for half the world, the 3-4 billion people in emerging & frontier markets, for far too long. Given the aforementioned, EverID is building The Identity Network (IN): a non-profit stewarded identity network for the common good of the planet which is self-funding, transparent, and independent. IN supplies the protocol & infrastructure for every human being to own & control their own database of identity data, including their biometrics. Not just on a device, but in the network too, enabling 7+ billion humans to scale the economic stack. Only with recent advances in cryptography and permissioned, distributed databases could a distributed, user-owned database be feasible.

The IN protocol + network solves the problems of building an economy for 3-4 billion people, which make up 20-30% of the world economy (USD \$15-25 trillion). Put simply, a robust economy requires (a) a protocol + network to be able to handle 10s of billions of transactions per month (scaling to trillions), in near real-time, with the highest security, for under \$0.01/transaction, (b) biometric identity verification, and (c) a smart contract transaction engine that allows users & orgs to exchange value (i.e. send USD \$1 billion to 200M users with 100% transparency and 100% verification). EverID's proof-of-authority network, plus protocol with identity datagram (packaging of biometrics + govt. IDs + 3<sup>rd</sup> party attestation) AND smart contract platform is the only blockchain solution that solves the scale, price, security & timing required for a "real" economy in emerging markets. The only other platforms putting biometrics "in-network" with associated "smart contracts" are nations, like India and Indonesia, where centralization is simply not working to deliver economic development & value to 50% of the planet.

Knowing the constraints of time (needs to be near real-time), cost (needs to be less than a USD penny per verification), transaction volume (needs to handle 1-10 billion transactions per month – and scaling to trillions) & security (needs to be more secure than existing centralized

databases & public blockchains), a special consensus mechanism is required to economically scale real-time verifications, while enhancing security. By establishing IN as a stand-alone, non-profit foundation, we can be assured that the network won't be captured by either EverID, the IN Foundation or outside actors. Only non-profit and economic development organizations are allowed to participate in the governance of IN. Also, the IN Foundation & EverID will both have signatory rights on any software release, thus eliminating that vector of attack. Further, a smart-contract will be established to automatically allocate funds to IN to pay for an ever-increasing amount of users & transactions. As such, IN will be an autonomous, non-capturable, decentralized network, owned by no one, functioning into perpetuity and embodying the principles of identity for Sustainable Development Goals (SDGs)<sup>1</sup> into code.

EverID is dedicated to liberating humanity from subservience to centralized, non-user friendly identity management & capital allocation organizations by creating a secure, decentralized identity management and value transfer system. We respect the privacy and wishes of the individual, while extending trust more broadly, and enabling all to interact and participate in the modern digital world. We are no longer able to rely on the social community constructs or existing processes & institutions to validate an individual's identity, transfer value or allocate capital in the digital world we live in.

EverID is a user-centric, self-sovereign identity and value transfer solution based on blockchain technology and the cryptographic underpinnings of that system, and reflects the principles of identity espoused in the sustainable development goals (SDGs). Upon those foundations, EverID is architected with a focus on resilience, availability, security, and control. The system operations are controlled and participation incentivized through an ERC-20 token, the ID.

## 2. Introduction & Problem Statement

Verifiable and persistent identity is the foundation of all economic systems. The lack of that identity is a major impediment to service access by the poor and those unable to directly participate in the digital world. Of the 7+ billion people on earth, over 1 billion lack legal identity,


---


<sup>1</sup> <https://sustainabledevelopment.un.org/sdgs>


close to 1.5 billion lack a bank account, 4+ billion do not have smartphones (thus unable to access a digital or crypto wallet). EverID wants to bring those communities into the digital world by providing them with digital identities, digital wallets, and document management that are stored on the blockchain, accessible and controllable by that individual. To be specific, by incorporating biometrics, existing government IDs and 3rd party attestations that are housed in a distributed, user-owned database, EverID is able to extend digital identity, digital wallets and document storage to humans who do not have a device; although enrollment requires a smartphone, usage & ownership of this user-centric identity + wallet + documents only requires biometrics (face & fingers). With the proverbial shirt on one's back, one is able to be verified, access one's wallet, manage one's docs and engage in value exchange in the 21st century economy. Those individuals who have their own mobile phone will be able to expand their EverID with additional pieces of data, and use it in more flexible ways. A user-centric, self-sovereign, biometrically verifiable identity solves the problems that have plagued the 3+ billion people living in poverty. Specifically, since industrialized societies have access to lower cost capital (due to lower perceived risk), that is where capital concentrates, creating a self-fulfilling system of the poor staying relatively poorer. The industrialized societies have been, until now, unable to accept risk at the same rates in emerging societies. EverID changes that paradigm. By giving biometrically verifiable identity to individuals, and collectively in organizations, with the ability for institutions anywhere in the world to create smart contracts with those orgs & individuals, EverID simultaneously offers industrialized societies a lower risk profile into which it can invest or loan capital, AND gives individuals and organizations in emerging economies access to lower cost capital.

EverID empowers individuals with the tools to protect and manage their own identity data, and importantly allows them to profit from institutions that wish to access data or verify their identity. For example, banks, governments, hospitals, telcos and other large institutions need to verify identities to open a bank account, get a SIM card, give & track a vaccine, etc., and pay organizations like EverID to verify an identity, transfer documents or money securely; in such cases, EverID will give a percentage of the revenue collected to the individual who is getting verified. Also, by giving digital identity to those who lack it, they get direct tangible benefits, as does the general society via an increase in economic development.



 Scale of Network

 Platform Management

 Identity Sources

 User & Currency

Network + Protocol: scalable & neutral	Self- soverei gn	Govts, Banks, NGOs, Orgs Send money to users	Smart Contract platform: orgs + users, any value exchange	Biometr ics form core of identity	Valida ted or Govt. ID integr ated	3rd party Attest ation (non- govt. accoun ts)	Stable Curren cy	Does NOT require user to have a phone	Sele ctive Shar ing	Wall et	Doc. storage & mgmt.
---	------------------------	---	---	--	---	--	------------------------	--	------------------------------	------------	----------------------------

### 3. EverID Principles

The principles guiding the technical and governance design of EverID reflect the Principles for Identity for Sustainable Development<sup>2</sup>. We assert that privacy is a human right, and the individual should have control over and effectively own their own database of identity elements, including their biometrics; and a user should have choice over what & with whom he/she shares info. The platform is available to all human beings available from birth until death, encrypted by design to protect users' privacy and is interoperable with other systems. There should be recourse if a user's rights are violated. Users should be informed and compensated for access to their identity information, and enabled to selectively share data with another party or deny access. We propose to fund a network of identity verification nodes which will be governed as a stand-alone foundation to ensure longevity, security & transparency of the network.

EverID is an organization of people that have the following unanimous, unchanging beliefs and principles about a person's identity information:

- All individuals should be included
- If an individual does not have access to technology, they should still be able to participate
- The system should be available forever
- All individuals should be specifically identifiable
- All information about an individual should be stored in the most secure manner possible
- The individual should possess and control their identity, if they are able
- The individual should be able to selectively share their identity information per interaction
- The individual's information should not be owned or controlled by any party other than the individual
- The system should be resilient against attack
- The system should be able to bridge to other systems

---

<sup>2</sup><http://documents.worldbank.org/curated/en/213581486378184357/pdf/112614-REVISED-English-ID4D-IdentificationPrinciples.pdf>

## a. Organizational decisions derived from principles

- Inclusion - EverID is built to address the needs of a world of 10+ billion people and to continue to grow indefinitely. We are working with various Non-governmental organizations to address the needs of the poorest and most vulnerable. Our goal is to enroll all of humanity. Our principle of inclusion is also reflected in our policies and governance.
- Device independence - if an individual does not possess technology, an agent system will enable them to be enrolled and public access devices used for EverID validation, use and updating. Public Access Devices (PADs) will use the EverID SDK to add identity validation to devices for banking, government services, healthcare, and more. The Bridge Service allows an EverID user to securely access and use their data on another device that they don't own. Further, since there are only 2.1 billion smartphones in the world, EverID architected a platform in which any individual can possess digital identity and a wallet with just their biometrics, thus reaching all 7+ billion human beings.
- Longevity - The EverID foundation is intended to be endowed and continually funded to exist indefinitely and continue to provide this service to users long after the departure of the founding team. The internal governance of the foundation will be constructed to provide a clear standard operating procedure and a mechanism to perpetuate, operate and evolve EverID to continue to be relevant and secure.
- Specificity - the key to identity is knowing you are dealing with a specific individual. To accomplish this, EverID records multiple types of biometric information for each individual identity and continues to sample those biometric sources during transactions for user validation. Further, EverID records and stores legacy identity documents, like national ID cards, drivers licenses, passports, voter ID cards, and also captures 3rd party attestations by cryptographically signing those affirmations of claims.
- Security - all information is stored on the individual's devices and the blockchain. The system stores the individual's information in a proprietary encrypted datagram. That

datagram is then stored on the blockchain behind a series of challenge-response locks.

- **Control** - the individual's data is recorded in a manner that allows granular control of how it is shared, with whom, and for how long. That sharing mechanism is enforced by smart contracts per transaction, with automatic resolution.
- **Ownership** - to fulfill the principles of SDG, users must own their own databases, both on-device and on-network or on-chain. It is no longer prudent to entrust ownership of one's biometrics & other identity metadata to centralizing forces.

## b. EverID Organizational Operation:

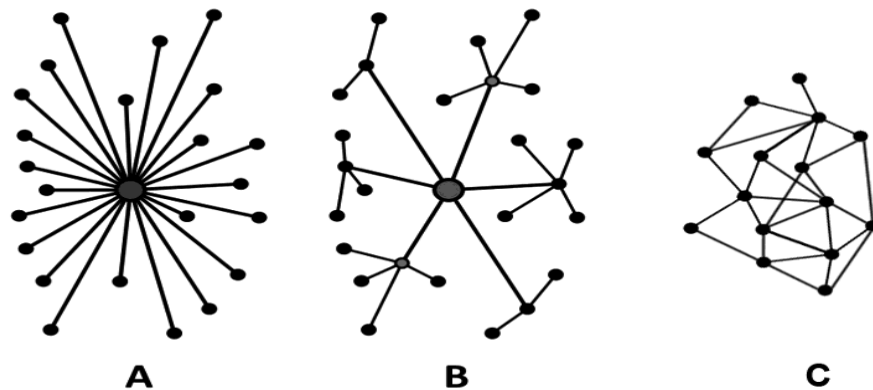
- **Organizational Structure** - EverID is a for-profit organization that is funding a foundation. The foundation, is designed to ensure transparency, neutrality, security & longevity of supernodes that house the EverID infrastructure. The economic model of EverID is intended to enable this long-lived organization by charging CRDTs for specific transactions within the system, and allocating a percentage of earnings to the IN foundation on an on-going basis. The IN foundation will have a board of directors, drawn from NGOs, IGOs and organizations with the same principles as EverID.
- **Management Team Structure** - the management of the foundation and the EverID operating company are mostly different, as their primary focus is different. The foundation is governed by a council of Caretakers whose mission it is to ensure the transparency, neutrality, security & longevity of the network; the criteria for selection of a Caretaker is that the organization must be a not-for-profit organization or an economic development focused organization and show at least 10 years in serving the public good. The EverID operating company is managed by a CEO, CTO, and management team. The core focus of the EverID operating company is to create economic and social value.

### c. Organizational Mandates:

- Ensure that the information is able to be controlled by the user, that they are able to retrieve their data, that they are able to use that data on-demand, and they are able to update that data on demand.
- Enable the information to be used wherever an individual needs to prove their identity - in the EverID app, or through Public Access Devices which have been EverID enabled through the SDK and API.
- Ensure that the biometric components of the system are in lockstep with the capabilities of the devices on the market. For example, if heartbeat biometrics become common and portable, include that type of biometry as an option for the biometric components of the system.
- Enhance the system with additional types of identity data and personal / private information over time, making it more capable of dealing with the entire spectrum of identity proof use cases.
- Enable the “build up” of an individual’s EverID over time, to ensure that those individuals who lack their own technology and are enrolled into the EverID system are able to update their EverID with more and more information, and eventually transfer their larger data set to an EverID DApp for storage and use when they obtain their own technology.

## Architectural Comparison:

A	Centralized Architecture - a central hub coordinates activity within the system.
B	Decentralized Architecture - not centralized, not distributed - some centralized resources, some distributed resources. Centralized resources are for coordinating the connections between the distributed resources.
C	C - a peer-to-peer, mesh network without a centralized resource.



### d. Technological decisions derived from principals

- Decentralized architecture - in order to ensure that the user's data is under their control, EverID is based on a decentralized architecture wherein the network-resident resources and the mobile applications are all part of the same decentralized system, making a distributed computer.
- Decentralized App - or DApp - a software application designed to work inside of a decentralized architecture.

- Blockchain - the is built on top of the Ethereum Enterprise blockchain, a private blockchain instance hosted on EverID operated infrastructure.
- The individual's information should not be owned or exploited in any manner without their direct consent. For example, if a user is interested in engaging in an arrangement wherein they wish to provide certain demographic information pseudo-anonymously about themselves for a discount on a Streaming Video service, they have the ability to enter into that transaction without compromising the security of the rest of their information. The user's identity data is atomically sharable.
- The IN system should be resilient against attack at each network node.
  - The EverID infrastructure is operated on a series of supernodes in the network - these supernodes are the host of the blockchains, the per-user IPFS storage locations, the Conduit System to integrate other systems and data, the Bridge Service to allow individuals to transfer their data from blockchain to EverID app instance, and the API Server to enable transactions from SDK-enabled devices . The data on the supernodes are secured with the user's Public/Private keypair, biometry, as well as a password/PIN. There is no ability to DDOS the EverID infrastructure as it is decentralized, has a financial disincentive in fees charged for transactions, and API requests are funneled through a queueing regulator to ensure that there is equal access to the services, and to mitigate potentially negatively impacting usage or load.
  - The EverID DApp and EverID Agent DApp are both based upon a cryptocurrency wallet for the Ethereum blockchain. The DApps in the EverID system are also secured with the user's biometrics and a password/PIN. The Bridge Service is also secured with the user's biometrics and password/PIN.
  - The EverID API and SDK are secured by a per-partner API key and per-partner SDK implementation key. These two keys are enrolled into the EverID system. The SDK requires that the SDK implementation key is embedded in the software

of the Public Access Device (PAD), however, the API key can be refreshed, enabling the prevention of key hijack compromising the system. In the case of a key hijack, a new API key is issued to the partner organization, and through the SDK, updated on uncompromised devices., and their SDK implementations when trying to access the supernodes are then challenged to provide the correct API key, and if the API key hasn't been updated, the host device has been compromised and can be blacklisted.

- The EverID Datagram is the proprietary storage array of the user's identity information. It consists of a nested series of information locked behind Biometric locks and knowledge locks (password, PIN) designed to bootstrap the unlocking of the next section of the datagram. Each individual has an EverID Datagram stored in IPFS on the supernodes, referenced to by the smart contract which recorded their identity to the EverID ID Blockchain.
- The platform should be able to bridge to other systems
  - Through the EverID API and SDK, the EverID System is able to be integrated into other applications and other devices not directly addressed by EverID's product offering.
  - Through the Conduit System, disparate sources of information can be integrated into the user space allowing the individuals to incorporate data from existing systems into their EverID.



## 4. Design Approach

A discussion of the design approach to various elements of the EverID system follows.

### a. Decentralized ID hub for individuals

EverID has been designed as a decentralized application, with a focus on availability, flexibility and extensibility. EverID is a mobile-first company that is interested in propagating the underpinnings of the EverID technology to other mobile phone software, PC software, proprietary, and embedded systems. The EverID infrastructure is designed to integrate with other data sources external to the system through the Conduit System and API.

### b. EverID Platform

The EverID Platform is based on a decentralized architecture where network-resident resources and the mobile applications are all part of the same decentralized system, making a distributed computer. Decentralized architectures suffer from a problem of concurrency — if one network node wants to address another network node, both nodes have to be online at the same time, which is not always possible. To ensure that the EverID system is always available, EverID will operate hardware clusters to host various software components of the EverID platform.

- EverID Datagram - the file structure for the EverID dataset which resides in the EverID DApp on the user's mobile phone and in the EverID Supernode. The EverID Datagram, like a .torrent file, is able to contain other data types and has no restriction on size.
- EverID Decentralized App - or DApp - a software application designed to work inside of the EverID decentralized architecture. Similar in function to a crypto-currency wallet, it creates the user's identity set (ECDSA 25519 public/private key pair) and records the user's information into the EverID Datagram.

- EverID API - a RESTful service hosted on a server in the EverID Supernode that enables interactions between identities and outside parties.
- EverID Core Smart-contracts - a series of Solidity smart contracts for various functions within the EverID system.
- Ethereum Blockchain - EverID is built on top of the private Ethereum blockchain, a blockchain instance hosted on EverID operated infrastructure and distinct from the public Ethereum blockchain.<sup>3</sup>
- EverID Supernode - a hosted service environment for the EverID platform infrastructure
  - IPFS storage array - a hosted instance of an IPFS storage system allowing distributed storage of the user's EverID Datagram.
  - EverID Filer - enables the recording of new EverIDs into the system
  - EverID Validator - enables the validation or verification of various components of an individual's EverID

### c. Points of Access to Identity

The user's information needs to be held in a secure manner, however, identity is not an island, and needs to have bridges to other services and the ability for the user to use their identity both online and offline.

The EverID Platform provides methods for the user to share and control identity information from their EverID DApp, using an Agent's device and the EverID Agent DApp, or using an EverID-enabled device (integrated with the EverID Platform through the EverID API).

---

<sup>3</sup> Please note, the private blockchain uses a proof-of-authority system. The EverID Foundation will hold 50% of the authority and the EverID operating company holding the remaining 50%, in this way there is no possibility for a 51% attack on the integrity of the blockchain.

Information is able to flow into the EverID platform from integrated data sources through the Conduit System, a secure integration system able retrieve and add user-specific information to an individual's EverID.

## 5. EverID Decentralized Identity Platform

EverID is a decentralized platform comprised of a combination of network nodes running EverID Software on user devices, agent devices, EverID Supernode hosted infrastructure and by extension, other systems through the EverID API and Conduit System.

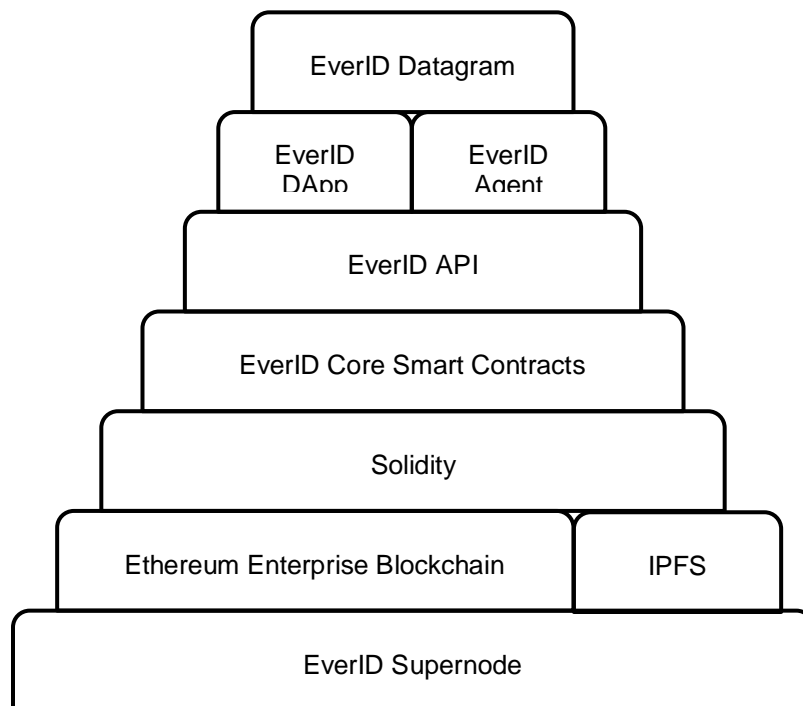
### a. EverID Overview and Technology Stack

EverID is a technology stack which includes:

- EverID datagram of an individual's identity
- EverID DApp is mobile telephone Decentralized Application (DApp) which gives the user the ability to self-enroll into the EverID System, and to record, update, store, transfer and share their identity information
- EverID Agent DApp is a mobile telephone Decentralized Application (DApp) for Agents, which gives certified agents the ability to enroll individuals into the EverID System and enables users to have access to their EverIDs when they don't have their own technology
- The EverID Application Programming Interface (API) memorialized in the EverID Software Development Kit (SDK) is made for other organizations to embed EverID functionality into their services or applications
- EverID core Solidity smart contract set which powers the EverID system and consists of: EverID Creation & Management, EverID Validation, EverID Transaction, and EverID Remote Management.
- EverID Identity Blockchain hosts the EverID Datagrams for the universe of individuals who have been enrolled into the system

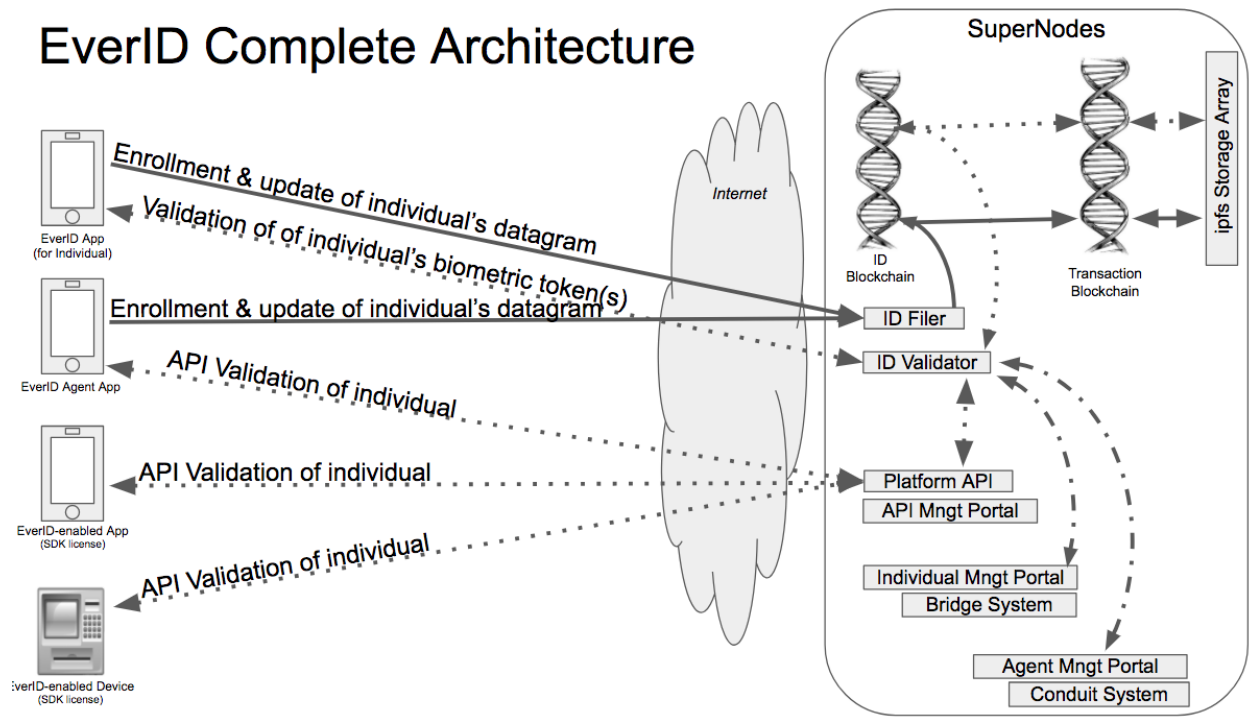
- EverID Transaction Blockchain hosts the transactions of individuals who have EverIDs
- ID Token (ERC-20 token) helps to track transactions in the system, creates a strong disincentive to spamming or DDOSing the system, and enables the enrolling of individuals into the EverID System
- EverID Supernodes host the various software services and servers required to create and operate the EverID Decentralized Platform.

## b. EverID Technology Stack Diagram



## c. EverID Architecture Diagram

### EverID Complete Architecture



## d. Biometrics

EverID uses biometry, or the specific unique physical or behavioral characteristics of individuals, to specifically identify an individual. By recording an individual's physical characteristics into EverID the system is able to specifically identify an individual, and ensure that each individual has one and only one EverID, preventing Sybil attacks.

Biometric capture capabilities have been added to mobile phones, and those capabilities have evolved over time. EverID will continue to include sources of biometry as they become commercially available in new devices. The user's biometric samples will be refreshed over time as frequency rules, biometric sample types, and system requirements change. Currently, EverID leverages both facial and fingerprint scanning, both of which achieve very high accuracy and are sourced from industry leaders that regularly supply such services to banks, nations and large organizations; by including two sources of biometry, EverID achieves a higher level of security than most in the market. As biometric advances are made, EverID will incorporate

additional sources of biometry, including iris, pulse, voice, DNA and others. Each biometric lock is accompanied by a user knowledge proof to ensure user consent to the transaction.

## e. EverID Datagram

The EverID Datagram is the proprietary storage array of the user's identity information. It consists of a nested series of information locked behind Biometric locks and knowledge locks (password, PIN) designed to bootstrap the unlocking of the next section of the datagram.

Each individual has an EverID Datagram stored in IPFS on the supernodes, referenced to by the smart contract which recorded their identity onto the EverID ID Blockchain.

The EverID Datagram is resident on the user's mobile device and in the EverID Supernode. Any updates to the Datagram are mirrored / synchronized with the other copies of that individual's Datagram on their devices or in the EverID Supernode as soon as the devices come online.

An EverID DApp, Agent DApp, or EverID Enabled device can create an EverID Datagram, however, external access to the EverID Datagram is possible through the EverID API.

The EverID Datagram, and its storage, is in the control of the user at all times, allowing them to control not only who has access to what information, but how that information is stored in the long-term. The user's data is protected by encryption using the EverID Public/Private key pair, user biometrics, PIN and Password, and the user is the only holder of those decryption keys. If the user wishes to delete their EverID, the anonymous biometric identifier used during enrollment persists, preventing the user from attempting to create a different identity in the system. The smart contract which records the user's EverID will be closed in a special manner which marks the EverID as inactive preventing future use, removes the pointers associated with the storage of the user's EverID Datagram, and encrypts and seals the storage with a special user key created by a mnemonic. For the user to recover their EverID in the future they would need the mnemonic for the special user key, their biometrics, their PIN and Password. This

conforms with the privacy requirements to allow the user to control, modify, or disable their identity information from being used. The special “delete EverID” logic conforms with the “right to be forgotten” and “right to erasure” requirements of the Data Protection Directive (Directive 95/46/EC) and General Data Protection Regulation (GDPR EU 2016/679) respectively, as the information is neither indexed by an external entity, nor available on the public Internet.

## f. EverID DApps

The EverID DApp and EverID Agent DApp are both based upon code commonly used to create a cryptocurrency wallet for the Ethereum blockchain. The DApps in the EverID system are secured with the user’s or agent’s biometrics and a PIN. The Bridge Service is secured with the user’s biometrics, PIN, and password.

The user with their own technology will use the EverID DApp to self-enroll, store and control their EverID directly. The EverID Datagram will be stored locally with a backup copy in the EverID Supernode IPFS storage array.

For those individuals who do not own their own technology, they can become enrolled into EverID by an Agent who has a device running the EverID Agent DApp. The user inputs all of the same information as if they were self-enrolling on the EverID DApp, however, they have the assistance of the Agent to help them with the scanning and data entry that the individual may be unfamiliar with and to teach them how to use their EverID. EverID Agents are compensated per-transaction for both validated new enrollments, and the ongoing validations against those individuals enrolled.

The system automatically polices rogue EverID Agents by analyzing patterns of behavior and alerting on behaviors that it finds unusual. Once alerted, the system will introduce additional checks on that transactions and subsequent transactions. Examples include multiple agents (who don’t know each other) verifying a suspect transaction, introducing a secondary verification by another agent on a suspect agent’s transactions, and finally removing a suspect agent from the system.



## g. EverID Application Programming Interface (API)

Through the EverID API and SDK, the EverID System is able to be integrated into other applications and other devices not directly addressed by EverID's product offering.

Hosted in the EverID Supernode is a server instance hosting a RESTful api to the EverID distributed computer. The RESTful API details can be found in Addendum 2 - EverID API.

The EverID API and SDK are secured by a per-implementation API key and per-partner SDK key. These two types of keys have a hierarchy, SDK keys have API keys. The SDK requires that the SDK implementation key is embedded in the software of the Public Access Device (PAD) or software application, however, the API key can be refreshed, enabling the prevention of a key hijack from compromising the system. In the case of a key hijack, a new API key is issued to the partner organization, and through the API Management Portal, updated on uncompromised devices. SDK implementations, when trying to access the supernodes, are always challenged to provide the correct key pair (SDK and API), and if the API key isn't correct, or hasn't been updated, the node device has been compromised and is automatically blacklisted from the platform. Blacklisted devices will need to be reinitialized with the appropriate SDK key and API key to again gain access to the EverID Platform.

The EverID API is secured through a HMAC<sup>4</sup> (hash-based message authentication code) system. Instead of sending over the SDK Implementation Key and API Key, we actually send a hashed version of the keys, together with more session information. In this manner we are able to secure the API, validate the message body has not been tampered with and control the access of disparate devices to the EverID Platform.

Through the API an EverID user is able to interact with their EverID on devices that they don't own, like, fingerprint-sensor enabled ATMs, or facial-recognition enabled medical tablet. They are also able to use their EverID in apps not provided by EverID for services like, biometric unlocking, simple user onboarding (automated KYC / AML checks), and medical form auto-fill.

---

<sup>4</sup> [https://en.wikipedia.org/wiki/Hash-based\\_message\\_authentication\\_code](https://en.wikipedia.org/wiki/Hash-based_message_authentication_code)

## h. EverID Core Smart-contracts

Using the Solidity smart contract framework for Ethereum blockchains, EverID is built on top of four main core smart-contracts:

- EverID Creation & Management
- EverID Validation
- EverID Transaction
- and EverID Remote Management

EverID Creation and Management - the smart contract used to create and evolve an EverID on the platform. This smart contract requires the user's public key, user's EverID datagram, the user's UserName, the user's Password, and the user's PIN. This smart contract is written to the EverID ID Blockchain and includes a pointer to the IPFS Storage Array URIs where the user's EverID Datagram has been stored, a hash of the EverID Datagram for integrity checks, and the creation time as a shared secret.

EverID Validation - the smart contract used to validate EverIDs. Validation requests can come from the EverID DApp, EverID Agent DApp, or EverID API enabled app or device. Validation requests are written to the EverID Transaction Blockchain and requires the user's public key, a biometric sample, the user's UserName, and the user's PIN.

EverID Transaction - the smart contract used to track identity information sharing and ongoing transactions against a user's EverID. Transaction requests for sharing medical information from a user's EverID, for example, would record the user's grant of specific information to another public key address of an individual associated with the user's medical clinic. Transaction requests are written to the EverID Transaction Blockchain and require the user's public key, a biometric sample, the user's PIN and user's UserName. The information shared, the recipient of the information (through their public key), the length of availability, and the enforcement of that availability are all recorded.

EverID Remote Management - the smart contract used by individuals who do not own their own technology, and are using Agent terminals to manage and update their EverID Datagram. Remote Management requests are written to the EverID ID Blockchain and require the user's public key, two different biometric samples, the user's PIN, the user's UserName, and user's Password.

Additional smart contracts will be added to the system as the need for additional capabilities arise. Note: Organization EverID identity smart contract is covered in Addendum 2.

EverID Core Smart-Contract Utilization Matrix

	Creation & Management	Validation	Transaction	Remote Management
EverID created from DApp	X	X	X	
EverID created from Agent DApp	X	X	X	X
EverID API Validation		X	X	
EverID API Remote Management	X	X	X	X

## i. Ethereum Private Blockchain

The EverID decentralized identity platform and associated transaction record are captured and stored in a set of private Ethereum<sup>5</sup> blockchains<sup>6</sup>, private instances of the Ethereum blockchain running on EverID operated hardware.

The Ethereum blockchain is an evolution of the shared ledger system underneath the Bitcoin cryptocurrency.

## j. EverID Supernodes

The EverID Platform is decentralized, meaning that it is a distributed system that relies on certain centralized services for coordination and bootstrapping.

The EverID infrastructure is operated on a series of Supernodes in the Internet network. These supernodes are the host of the centralized services used for coordination of the EverID platform. These centralized services include: private Ethereum blockchains, the IPFS storage array for

---

<sup>5</sup> <https://ethereum.org/>

<sup>6</sup> <http://www.goldmansachs.com/our-thinking/pages/blockchain/>

per-user storage, the Bridge Service to allow individuals to transfer their data from blockchain to EverID DApp instance, the conduit system to integrate other systems and data, and the API Server to enable transactions from SDK-enabled devices.

As the private Ethereum blockchain runs on a Proof-of-Authority mechanism the EverID foundation and the EverID operating company will each receive 50% of the authority in the system, making the theoretical 51% attack an impossibility. Consensus of transactions rely on pre-approved “sealer” authority nodes to seal new blocks in the blockchain. More information about the Ethereum Proof-of-Authority protocol, “Clique” can be found here <https://github.com/ethereum/EIPs/issues/225>.

There is no ability to DDOS the EverID infrastructure as it is decentralized, hosted on private infrastructure, and all requests are funneled through queueing regulators to ensure that there is equal access to services, and to mitigate potentially negatively impacting usage or load. Additionally, the ID Token required for most transactions on the platform, discussed in depth later, creates an additional financial disincentive to attempts to flood the network with spurious traffic.

The ID Filer service takes care of creating EverIDs in the system and creates a mapping between the individual’s UserName, Public Key and PIN. The Filer’s mapping is relied upon for Agents to locate an individual’s EverID Datagram and download it for use. The ID Validator service takes care of validation requests to the system and is the first step in nearly all transactions on the EverID Platform.

- Portals

To enable the control of the EverID platform and allow for access to specific services, three portals will be operated in the EverID Supernode: API Management Portal, Individual Management Portal, and Agent Management Portal.

The API Management Portal enables EverID to issue SDK License Keys and API License Keys to participating organizations, and to share development resources to implement EverID into software applications or embedded devices.

The Individual Management Portal enables EverID users to access the Bridge System to recover their EverID in the case of disaster or accident.

The Agent Management Portal enables EverID to issue Agent Keys (similar to an API License Key) which belongs to a hierarchy under an organization's Master Agent Key.

- **Bridge System**

The Bridge System is a special authentication system which through a series of challenges and biometric checks ensures that an individual is the owner of their EverID and should be allowed access to save their EverID to a new EverID DApp instance. This is similar in concept to a "restore from backup" service.

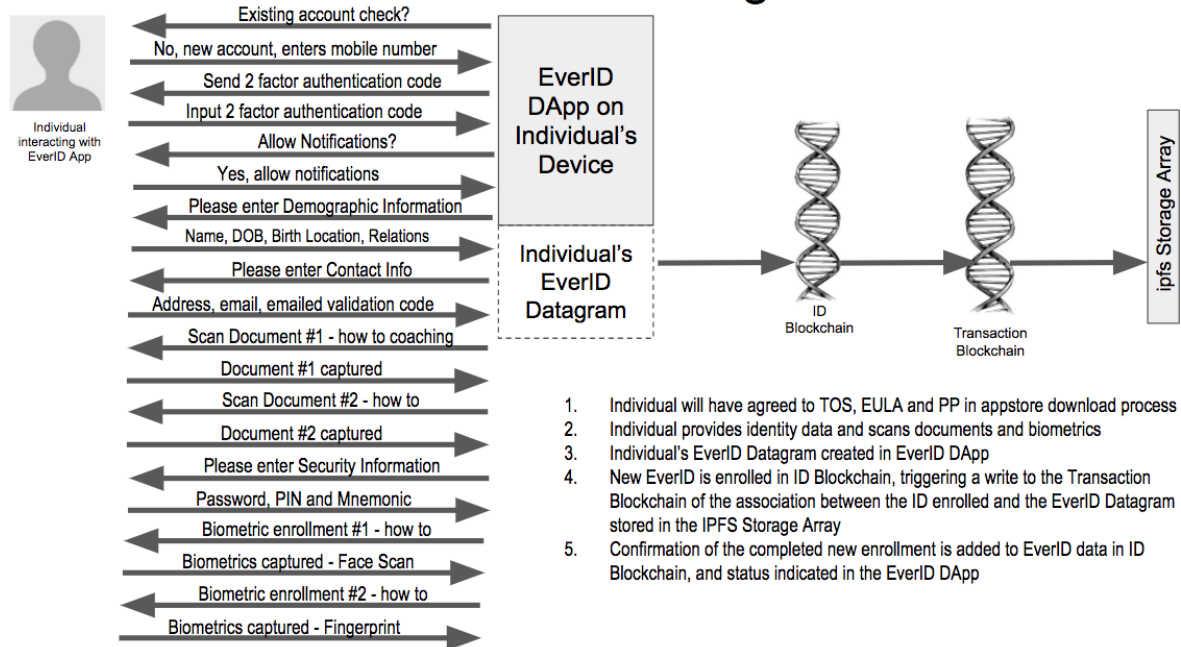
- **Conduit System**

Through the Conduit System, disparate sources of information can be integrated into the EverID Platform's user space allowing individuals to incorporate data from existing systems into their personal EverID. Examples of this inbound information would be national identity registers, healthcare systems, online services, refugee databases, etc.

## 6. The EverID Logic Flows

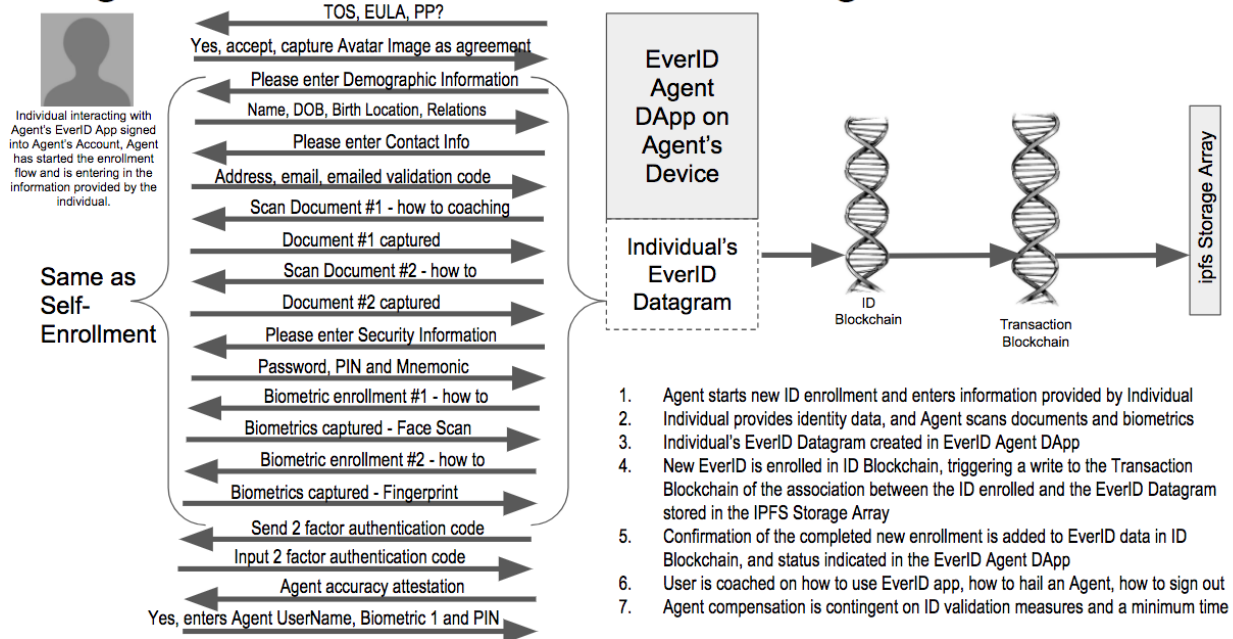
### a. Individual Self-Enrollment

#### Self-Enrollment of an EverID Datagram



## b. Agent Enrollment of an EverID

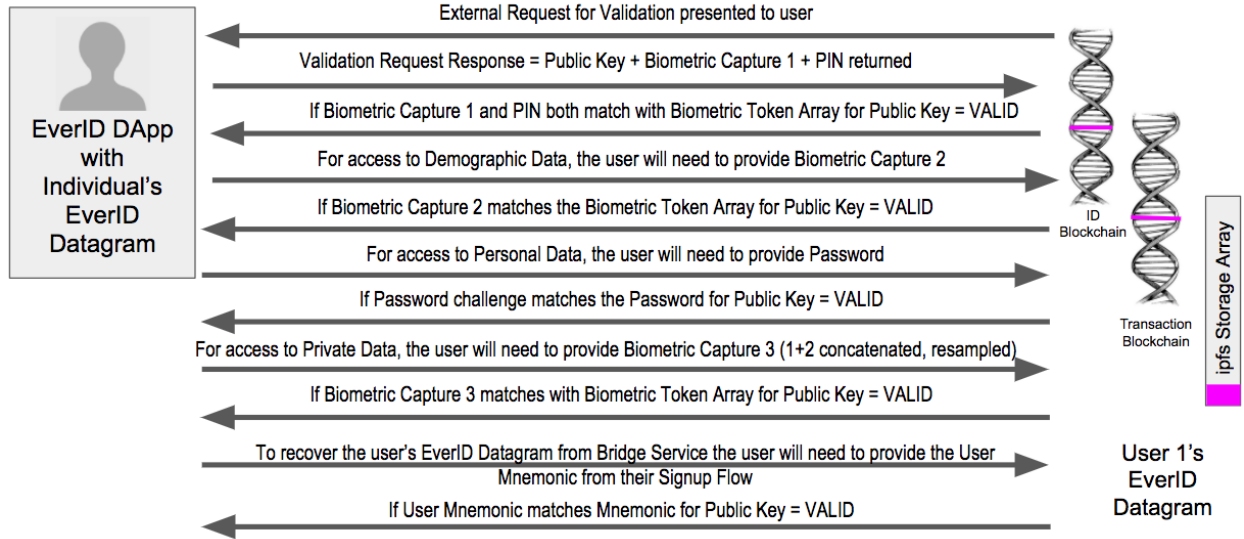
### Agent Enrollment of an EverID Datagram





## c. Validation of the EverID

### Validating using EverID



## 7. The ID + CRDT Economy

EverID supplies end-users with a digital identity (biometrics + existing government IDs + 3rd party attestations), a digital wallet and document management (housed on-device and on-network). Thus, creating a platform for end-users to engage in existing economies with full sovereignty, anywhere in the “economic stack.” EverID is the creator and enabler of an identity ecosystem leveraging the power, transparency and security of the blockchain. With identity validation, users are able to open bank accounts, receive aid, selectively share data with hospitals, e-commerce and other organizations. For institutions like NGOs, IGOs, governments, banks, hospitals, etc., the value proposition is that they can track service delivery & consumption (all databases are updated in real-time), verify funds are securely delivered to the “right person” (reducing fraud & leakage, increasing transparency); by putting biometrics “on-chain”, institutions will be able to validate individual identities with simply the user’s biometrics (users don’t need to have smart phones).

EverID, intends to utilize (1) its own token (“ID”) and (2) a credit (“CRDT”) strategy as follows:

- 1) IDs are a utility token controlling access to the network regulating the applications and services. Varying levels of access to network resources are distributed to the holders of the ID tokens. For example, an end-user may need to hold 1 ID in their wallet if they want to use the Remittance functionality of the platform, however, an institution may need to hold 50,000 tokens in their wallet to gain access to the EverID SDK and API. Such a construct will allow partners access to the following applications (such applications will require purchasing of CRDT credits):
  - a) Identity recording (new individuals get EverIDs)
  - b) ID Verification. Biometric, government ID and 3rd party attestation, including zero-knowledge proofs
  - c) Tracking of funds, goods and services to ensure that they are received by the intended recipient.
  - d) Access to aggregated data and research
  - e) Payment for API access (organizations that use the EverID platform using the API will pay for that access)

The ID token will initially be sold in 3 “Token Sale Rounds”: 1) the current seed round via a SAFT agreement, 2) the Crowdsale pre-sale targeted to open in April, and 3) the Crowdsale targeted in May, 2018. The first 2 pre-sale Token Sale Rounds are intended to be used to raise proceeds for EverID to set up its infrastructure, build its network, contract with vendors, service providers and strategic partners, and issue its tokens in the Crowdsale. The Crowdsale proceeds will be used to expand the network and network applications.

- 2) The CRDT will be sold as a digital credit that allows institutions and end-users who have access to the platform to purchase services and applications on the EverID network including:
  - a) International remittances
  - b) Incentivization of the system (compensating agents in the system)
  - c) Payment for identity verification (confirmation that an individual is who they represent themselves to be)
  - d) Compensation to individuals (when an individual chooses to share certain information with certain organizations, they are entitled to compensation for that access, or when an individual transacts in the economy there may be costs for the transactions).
  - e) Storing and managing documents
  - f) Sending of conditional and unconditional vouchers, cash and digital monies
  - g) Management of end-users

The ID will be used to manage and scale identity, tracking and matching applications across the digital identity landscape, or “identiverse.”

#### **Incentivized Viable Economic Model:**

CRDTs will be distributed to contributors of value in the network (like Agents, Users, etc.), incentivizing engagement, development, promotion and adoption. EverID agents will be compensated based on valid registrations of individuals, and a subsequent portion of those individuals’ validation earnings. Users will be compensated for verifications made upon their

identity, and other services (e.g. cash transfer); furthermore, EverID is partnering with organizations to deliver additional income opportunities. The CRDT can also be traded into local currency or cell phone minutes to provide support for universal basic income.

EverID will earn revenue in US dollars (or other liquid currencies) in the process of institutions paying for identity verification, sending of money and management of documents. For example, the market for identity verification in India at massive scale currently yields \$0.015 per /verification; as of February 2017, there were 16 million verifications per day, and currently averaging 139 million per month<sup>7</sup> of the roughly 1 billion identities.<sup>8</sup> Over \$3.3 billion dollars has been sent over such a platform, reducing leakage & fraud and increasing payouts by 12-20%.<sup>9</sup> EverID will offer similar services and share in the savings. For example, if an NGO or bank transfers \$1 billion to 100 million users, the EverID platform will save the NGO or bank \$120-\$150 million (based on the 12-15% increased payouts being seen in India), and earn a good percentage (i.e. 30% or \$45 million) of the transfer. Similarly, managing documents for institutions, like governments, banks & hospitals requires storage, conditional access & permissions, all of which institutions pay for (i.e. a health agency in a given country will pay USD \$100s of millions for such a platform).

---

<sup>7</sup> <http://stateofaadhaar.in/wp-content/uploads/State-of-Aadhaar-Full-Report-2016-17-IDinsight.pdf>

<sup>8</sup> <http://www.kpcb.com/internet-trends> pg. 258-259

<sup>9</sup> <http://www.kpcb.com/internet-trends> pg. 260

In addition to identity management, EverID earns revenue from the following:

- Remittances. When users transfer money to each other over the platform; typically, these transfers can be categorized as remittances, a \$596 billion dollar a year market. A representative remittance company earned roughly \$50 million in revenue with 2 million users and 5.5 million transactions in 2017. Additionally, EverID will earn revenue on connecting users to low-cost loans (i.e. earn \$5-\$100 per user qualified for a bank account) and direct lending itself.
- Transaction fees over and above identity verification
- Loan broker
- Referral fees to institutions of verified customers
- Sale of aggregated data
- Calls to action and conversions
- Service of advertorial content
- Eventually becoming a lender
- Marketing/Transaction fees for NGOs
- Monetize wallet, profile and can sell financial services

## **The CRDT credit**

EverID, has a credit or voucher token, the CRDT, which is used to manage and scale identity applications across the digital landscape, or identiverse. Basic operations on the EverID platform will require the spending of CRDTs and in most cases the holding of ID Tokens, thus contributing to its value. CRDTs will be held in EverID DApps, in EverID Agent DApps, or in the EverID account. ID Tokens will be held in EverID DApps, in EverID Agent DApps, in the EverID account or in a compliant Ethereum wallet.

The CRDT distribution and usage cycle creates a circular economy within the EverID platform helping to propel additional use. Each EverID enrollment, verification, update, or transaction will require the spending or holding of CRDTs. When validations are conducted against an individual's EverID by institutions like telecommunications companies, banks, governments and NGOs, a percentage of the transaction will be remitted to the individual in the form of CRDTs.

In this way, the individual is directly benefiting from participation in the ecosystem. Further, a percentage of the earnings will be given back to CRDT Users depending on activity in the network. For example, if EverID earns \$10 million in a month, 10% or \$1 million worth of CRDTs will be given to Users who were verified, sent money, managed docs, etc. (commensurate on the amount they participated in those network activities).

At the outset, EverID will produce applications for refugees, protection of women & children and micro-financing. For refugees, EverID is enabling civil registration and conditional cash transfer with demand being pulled from EverID's partner organizations. For protection of women & children, EverID will leverage the biometric registration of family members to facilitate the screening of girls & women to prevent human trafficking. For microfinancing, EverID plans to integrate as an Identity provider in the Gates Foundation's Mojaloop framework to promote financial services for the unbanked.

CRDTs will be spent to interact with individual's identity, analogously to the way Ethers (ETH) are spent to acquire collective computing on the Ethereum blockchain.

EverID expects to expand the economy to provide money exchange, currency remittance, and other financial services to EverID users. These services are controlled by varying regulations per jurisdiction or country, and those regulations and the associated requirements for licensure or registration will be satisfied by EverID prior to engaging in the regulated activity.

## 8. Conclusion

EverID is a user-centric, self-sovereign identity system that is designed to bridge the digital and physical worlds by digitally recording each individual's biometric identity. Each individual identity and each transaction are recorded into a durable, permanent, auditable storage system powered by private Ethereum blockchain and IPFS Storage Array. EverID will continue to add biometric identification methods to the EverID Platform over time as the capabilities of mobile terminals changes.

The EverID Platform is designed so that an individual is in control of their identity information and how that identity information is used and by whom. EverID Supernodes host the centralized resources needed to operate the EverID Platform, which ensure that the individual's information is always available and backed up, and that the platform is able to interact meaningfully with external resources.

The time is ripe for this style of platform as the concept of decentralization, biometrics and the mobile device technology lifecycle are both mature enough to support widespread adoption. Decentralized computing has risen to prominence in the last 7 years with the creation of Bitcoin and Ethereum, and is now considered to be mature enough technology to be incorporated into other solutions. Mobile telephony devices have increased in capability to the point that local biometric systems are able to be used, and cryptography will run sufficiently quickly to handle the associated tasks on demand.

## 9. Acknowledgements

These people do not endorse and are not involved with the EverID Project.

“If I have seen further it is only by standing on the shoulders of giants.”

– Sir Isaac Newton (and Steve Jobs)

EverID would like to thank:

Charles Babbage

RADM Grace Hopper USN Ret.

Vint Cerf & Bob Kahn

Ralph Merkle

Tim Berners-Lee

Bram Cohen

Satoshi Nakamoto

Vitalik Buterin



# Addendum 1 - ID + CRDT = Utility Token & Credit Currency

EverID has both a utility token, the ID, and a credit, the CRDT. The ID, represents the value of the economy, and will be offered for sale in a Presale and Crowdsale. The CRDT is the native credit that Users & Institutions use to manage and scale identity applications across the digital identity landscape, or “identiverse.” ID is the only token currently being offered. CRDTs are a credit or voucher.

Each CRDT will effectively carry a smart contract to share profit to users and the foundation. As such, the network will be self-funding, users have incentive to participate, growing as the number of users & transaction value increases.

EverID will initially peg the CRDT to the US dollar (\$). Each CRDT is equal to USD \$0.01. In the future, the CRDT may be pegged to a basket of stable fiat currencies or commodities, or simply evolve into a stable token itself. The goal of pegging to a known and accepted fiat currency is to achieve stability, liquidity and transparency. It follows, EverID will collect revenue in US dollars, and convert them into CRDTs; that is, transaction fees are in CRDTs, but at a guaranteed fixed amount of equivalent USD due to the peg. Revenue comes in the form of institutions that pay for identity verification, sending of money, management of documents and subscriptions to a hosted eGovernment platform. Institutions and end-users will purchase ID tokens, which grants access to EverID’s suite of applications (i.e. ID verification, sending money, storing & managing documents, enrolling a new identity, tracking consumption, aggregating data, integrating payments, etc.) inside the EverID network. Once they have access to the network, institutions and end-users purchase applications as they normally would, which require payment in CRDTs. Institutions and end-users will pay EverID in USD or other fiat currencies, and EverID will convert those monies into CRDTs, which are spent on the various applications.

By selling ID tokens, EverID will raise capital to establish a CRDT-based economy. In the future, EverID may engage in micro-financing by loaning CRDTs, which is a more stable value of exchange than many others. The combination of financial services with smart contracts, biometrically verifiable & traceable, establishes EverID as the standard in user-centric identity that is able to bridge to existing institutions. In offering a stable credit of exchange & payment, EverID will alleviate the concerns and hassles that many users face in emerging economies, avoid the volatility of non-pegged cryptocurrencies, and become a form of stored value in many parts of the world. End-users' CRDTs may be redeemable by EverID into mobile data or other utilities in the future.

EverID's token model Crowdsale is designed to minimize investor risk, and deliver stability for both institutions that partner with EverID, as well as users.

EverID will initially issue a total of 800,000,000 IDs.

**Co-founding:** 25% of IDs are allocated for EverID co-founding members.

- **Allocation:** 200,000,000 IDs will be allocated to co-founding members of EverID
- **Timing:** IDs will be issued and distributed before the launch of the public Crowdsale

**Seed, Presale & Crowdsale rounds:** 50% of IDs are allocated for financing rounds.

- **Allocation:** 400,000,000 IDs will be allocated in three rounds of financing. USD \$2m will be raised in a seed round to scale the product, add partnerships, launch initial partners & users and prepare for a Crowdsale at a 50% discount.
- **Timing:** Roughly USD \$30M will be offered in a Presale round at a 25% discount. And an estimated USD \$40M will be offered for sale in the Crowdsale.

## Seed funding

EverID is raising up to \$2m in Seed funding to support its first months of operation (including reaching its Crowdsale, beta version of the EverID stack, and growing strategic partnerships) by selling 14,000,000 IDs at a 50% discount to the targeted Crowdsale price. The funds are being raised via a Simple Agreement for Future Tokens (SAFT), referring to the Crowdsale expected

in 2018, with the following special conditions: the seed round will convert to ID tokens with a 50% discount to the target price of ID at the time of Crowdsale. Part of the Seed fund will be used in the project for product development, intellectual property protection, product integration and customization for trials, personnel, travel and general business expenses. The anticipated budget is as follows: Partnerships, Legal & Finance will account for 37% of expenditures. Marketing & promotion will account for 15% of expenditures. Engineering development will account for 37% of expenditures. And Regional Partnerships & Logistics will account for 10% of expenditures.

## **Presale and Crowdsale**

EverID will offer IDs prior to (Presale) and during the Crowdsale.

- During the Presale EverID will offer 186,000,000 at a 25% discount. Any ID not sold during the Presale will carry forward and be included in the Reserve account.
- During the Crowdsale 200,000,000 IDs will be offered in 5 tranches released every 2 days.

## **Funding the Identity Network Foundation**

EverID will fund the Identity Network foundation to set up, oversee elements of the shared systems in the EverID Supernodes. If \$10M USD is raised, then 5% will be allocated to establish the Identity Network foundation; for every USD\$ 1.00 above \$10M, 2% will be allocated to the Identity Network foundation. If IN becomes obsolete due to technical advances, or public chains offer greater transparency, speed, cost or other benefits, IN will be donated to an appropriate charity.

### **The governance of the Identity Network foundation will be as follows:**

- **Mission:** safeguard the independence, transparency, security and longevity of the network so that it exists for humanity forever.
- **Funding:** EverID will donate a percentage of capital raise per the above, plus a percentage of identity verification earnings on an on-going basis, thus creating a self-funding network.

- **Board of Directors:**

- Must be from an NGO or IGO whose efforts are for economic & social development and has been in existence for 10 years or more
- Must adhere to the principles espoused in the Sustainable Development Goals

- **Rights and Responsibilities:**

- Ensure network cannot be taken over & transactions are transparent
- Hold 50% authority. In a “proof of authority” network, this prevents any organization, including EverID, from ever changing the base code
- Establish independent observer nodes
- 2 board members are signatories on code release

## **Holding ID Tokens**

Those institutions which wish to operate Observer Nodes will require the holding of 1,000 to 50,000 IDs, (depending on the size of the institution, user base, access to higher service levels, intended use, etc.), in their EverID Wallet in order for the Observer Node to participate in the EverID Distributed Computer.

IDs provide differentiated level access based upon the number of IDs maintained in the holder’s wallet. ID holders are provided with CRDTs based upon the volume of their transaction, meeting eco-social KPIs and creating value for the network.

Basic Access to EverID network requires EverID wallet with a minimum of 5 IDs. Full access requires 500 IDs. Observer nodes/rights requires between 1,000 and 50,000 IDs.

<b>Differentiated Access Levels</b>	
<i>Amount of ID Tokens held in wallet</i>	<i>Access Levels provided</i>
0 ID	Consumer-level access to platform (recipient)
1-5 ID	Participant in economic exchange - for example remittances
500 ID	API access
1,000 to 50,000 ID	SDK or Observer Node access

End-users do not need to own IDs to transact as a consumer on the network. Transactions can only be done in CRDT credits. Incentive rewards are based in CRDTs. For example, when a consumer registers and opens an EverID wallet, we deposit 10 CRDTs in their wallet. When they validate their ID, they get another 10 CRDTs, when they invite a friend who signs up, they get another 10 CRDTs, when they consume content, generate value data, take education and certification classes online, get a health checkup, apply for credit, etc., they earn CRDTs. CRDTs are pegged to the USD and can be used to transact on the Network or can be cashed in for fiat with a significant transaction fee.

## Addendum 2 - Organizational Identities

The nature of society is that individuals belong to various organizational entities. They are citizens of a nation-state, they are residents of a city, they are members of a soccer team. All of these organizations may play a role in the EverID system.

To provide the ability for these entities to exist in the EverID system, there is a special kind of EverID called an Organization EverID. Organization EverIDs are created with an Organization EverID smart contract template entered into by at least two EverIDs. This Organization EverID smart contract has the ability to create an Organization EverID, which is able to participate in the EverID system as any other EverID.

The EverID platform will issue a public/private key pair to an Organization EverID smart contract. Organization EverIDs can only be created and become “valid” on the system when two individual’s EverIDs become associated with the Organization EverID by initiating the creation of the Organization EverID smart contract. The creation of an Organization EverID requires the spending of EVER Tokens.

All Organization EverID transactions are multi-signature transactions, conforming to the governance structure of the organization as defined by the Organization EverID smart contract. The Organization EverID requirement for each transaction to require a multi-signature transaction is satisfied by any authorized Administrator associated with the Organization EverID. Organization EverIDs require two authorized Administrators to enter into any transactions within the EverID system, in the case where an Organization only has one authorized Administrator all rights to create new transactions are halted. Existing transactions in motion will continue as defined in their respective smart contracts, unless an authorization is required, which will not be able to be satisfied, preventing the smart contract to continue.

The initial EverIDs associated with the Organization EverID automatically become authorized Administrators for the Organization EverID, and may grant other individuals entry into the Organization EverID, or, entry to and Administrator authorization for the Organization EverID. EverIDs in Organization EverIDs become authorized Administrators by requesting to join the

organization, then being granted Administrator rights to the Organization EverID. EverIDs may leave an Organization EverID by request, if there are no remaining organizational requirements to be satisfied - for example an individual who owes dues to his Organization may be prevented from leaving the organization until they have paid their dues. An Organization EverID exists until all Administrator EverIDs associated have been removed from the Organization EverID smart contract. This is a similar process to the enrollment of individuals as administrators into an ICANN listing.

An Organization EverID is preserved even after there are no Administrators remaining associated with the Organization EverID. Organization EverIDs may participate in transactions in the EverID system in the same methods as individuals, however, their transactions are marked with an Organization flag for use to display in the user interface.

Organization EverID structures will be defined and operated by smart contracts on the EverID blockchain, and will conform to the Organization EverID template used to create it. Complex governance structures may require expansion of the Organization EverID smart contract structure over time, however, it will begin as a templated framework.

Organization EverIDs can earn enrollment incentives within the EverID system. An example of such organization would be the Girl Scouts of Springfield who's EverID information was used for the Enrollment Applications used by the Girl Scouts to enroll themselves, enroll their friends, and enroll the public during their weekly visits to the homeless community center. All validated enrollments could be rewarded with CRDTs paid to the Organization's EverID.

# Addendum 3 - EverID Datagram

## EverID Datagram Explained

### EverID Datagram:

- Layers of the onion nested dataset requiring individual locks to access individual components
- The individual components are only queried when the transaction requires it - getting reward points for a movie ticket does not require anything other than the user's public key to validate enrollment in program, however, a user may need to scan their biometrics to check into a medical office
- For SDK transactions, the majority of the time the Individual's Biometric Token Array and Demographic Data will be the only pieces of the EverID Datagram queried
- Enables the individual who owns technology to have and control their data on their devices and on SDK-enabled device, as well as archived on the EverID blockchain
- Enables the individual who does **NOT** own technology to use their EverID Datagram through Agents devices, SDK-enabled devices, from the archived version on the EverID blockchain

### Example Datagram Unlocks:

- Validate user ID - 1 Biometric Capture + PIN = user identity is valid
- Unlock User ID - 2 Biometric Captures + PIN = user identity is valid and access to user demographic data is given
- Medical - 2 Biometric Captures + PIN + Password = user identity is valid and access to user Personal data is given
- Change National ID - 2 Biometric Captures concatenated = user identity is valid and access to user Private data is given



## Addendum 4 - EverID API

The EverID Client REST API is a REST-based API for integrating EverID into applications or embedded environments. Use the web services provided by the API to create, read, update, delete, and search content in the EverID Platform. For more information about the API, see The EverID API Developer's Guide.

NOTE: To use any of these interfaces, you must have a EverID SDK License Key and an EverID API License Key. To create your credential set to be able to address the EverID API, please contact [PartnerSupport@everid.net](mailto:PartnerSupport@everid.net).

The EverID Client API is a RESTful interface for building client applications. The capabilities of the API include the following:

- Search for EverID.
- Validate, and retrieve EverID.
- Create, retrieve, update, and close transactions.

You can use the EverID Client API to work with XML, JSON, text, and binary objects. In most cases, your application can use either XML or JSON to exchange data such as queries and search results with the EverID API Server.

The examples in this section use the command line tool curl for sending HTTPS requests. Though the examples rely on curl, you may use any tool capable of sending HTTPS requests. If you do not have curl, you can download a copy from <http://curl.haxx.se/download.html>.

The following HTTP response codes apply to all requests to the API services. Additional response codes are covered in the usage information for each operation.

<b>Code</b>	<b>Description</b>	<b>Cause</b>
200	OK	Success
400	Bad Request	Unsupported, invalid, or missing required parameters.
401	Unauthorized	User is not authorized.
403	Forbidden	User does not have access to this resource.
404	Not Found	No matching pattern for incoming URI.
405	Method Not Allowed	Service does not support HTTP method used by the client.
406	Unacceptable Type	Unable to provide content matching client's Accept header.
412	Precondition Failed	A non-syntactic part of the request was rejected. For example, an empty POST or PUT body.
415	Unsupported Media Type	A PUT or POST payload that cannot be accepted.

### **Service Descriptions:**

Use the /search service to search for an EverID using the User Name/PIN value pair.

Use the /everid service to validate and retrieve EverID.

Use the /transaction service to create, retrieve, update, and close transactions. You can also query the status of transactions.

Use the /config service to manage properties of your REST API instance, such as setting the MIME type for error reports, location to send error reports, and enabling debugging output.

## **Resource Descriptions:**

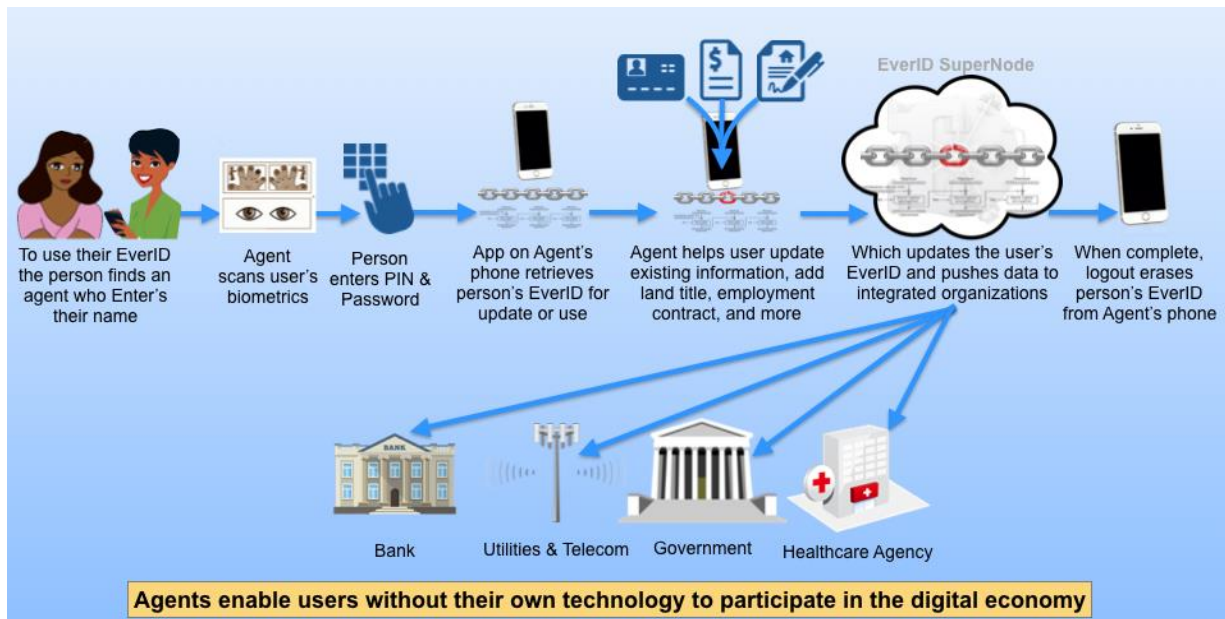
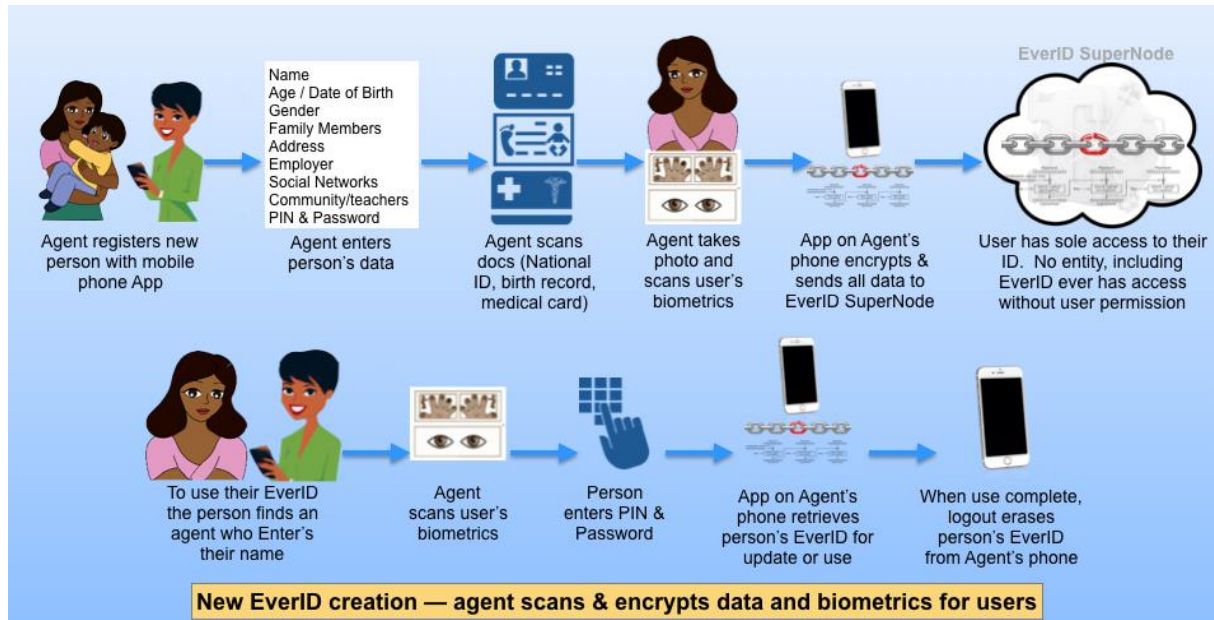
<b><i>Resource URI</i></b>	<b><i>Description</i></b>
<b>/search</b>	
/v1/search/{name}?pin={pin} (GET)	Search the database using a string query for {name} (user name) and PIN, which returns a public key for biometric challenge.
<b>/everid</b>	
/v1/everid/validate/publickey?bt={token},pin={pin} (POST)	Perform a validation of the biometric token {token} and {pin} for an individual's public key.
/v1/everid/retrieve/publickey?uri={datagramuri},part={part} (POST)	Retrieve a {part} of an EverID from its IPFS storage array location {datagramuri} for an individual's public key.
<b>/transaction</b>	
/v1/transactions/create/publickey?txid={txid} (POST)	Creates a transaction {txid} for the individual who's public key is given in the request URI.
/v1/transactions/retrieve/publickey?txid={txid} (POST)	Retrieves the status of a transaction {txid} for the individual who's public key is given in the request URI.
/v1/transactions/update/publickey?txid={txid} (POST)	Updates a transaction {txid} for the individual who's public key is given in the request URI.
/v1/transactions/close/publickey?txid={txid} (POST)	Closes a transaction {txid} for the individual who's public key is given in the request URI. Most transactions will close based upon the smart-contract enforcing the parameters of the transaction, however, in certain cases

	a manual "close" to stalled transactions may be necessary.
/v1/transactions/status/publickey?txid={txid} (GET)	Retrieves the status information for the transaction whose id matches the {txid} transaction id for the individual who's public key is given in the request URI.
<b>/config</b>	
/v1/config/reportencoding (POST)	Set the error report MIME type.
/v1/config/reportlocation (POST)	URI to send error reports.
/v1/config/debug (POST)	Enable or disable debugging output, which is sent using the report encoding and report location parameters for delivery format and location.

# Addendum 5 - EverID Use Cases

## a. Individual:

### i. Individual Enrollment (Agent)



## ii. Identity Verification, Healthcare & Food Assistance



Bastian wants a tuberculosis (TB) vaccination for his daughter, Dayu, and authorization for food assistance. He scans himself at a PC with Internet access and enters his PIN, which is validated against the blockchain, and displays a photo of Bastian and link to his records to clerk.

- User identity validation
- Secondary confirmation with photo
- Retrieval of status & records

2

After review, Bastian is granted the vaccination for his daughter and the food assistance for his family.

→ **Healthcare and food assistance grants are recorded in agency's systems AND updated on Bastian & Dayu's identity**

3



When the medical service is completed, the clinic staff rescan Dayu verifying that she was given the approved TB vaccine and recording that into her EverID.

- Proof an individual received vaccination
- Budget for vaccinations pay for services
- Added to child's electronic medical record

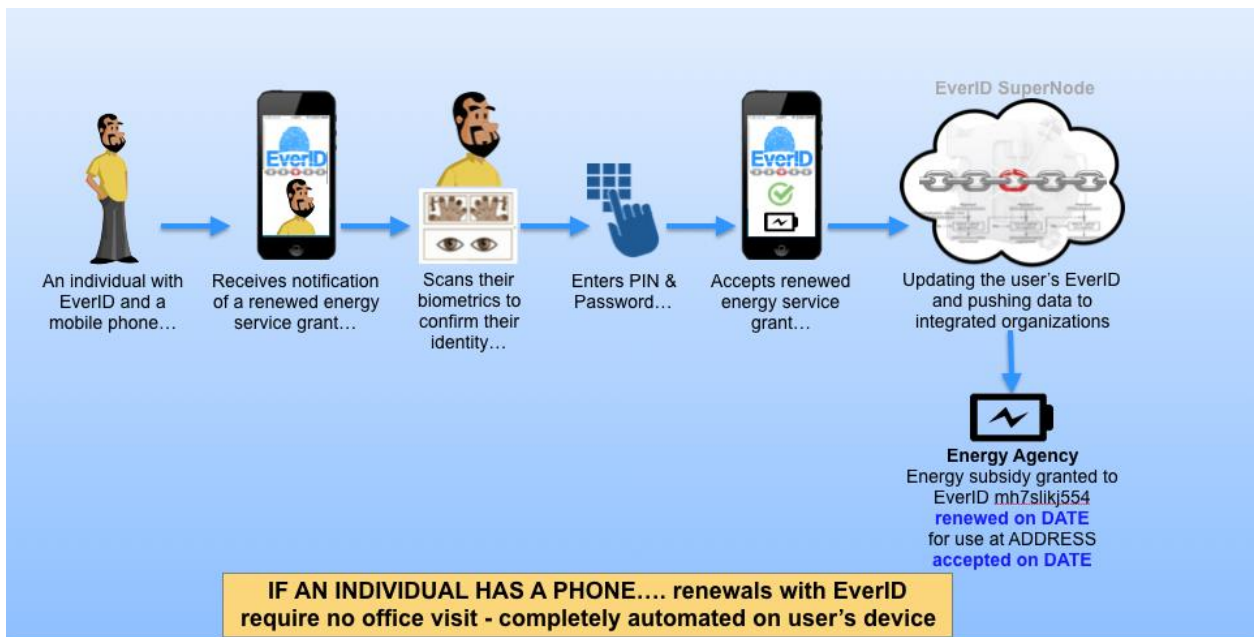
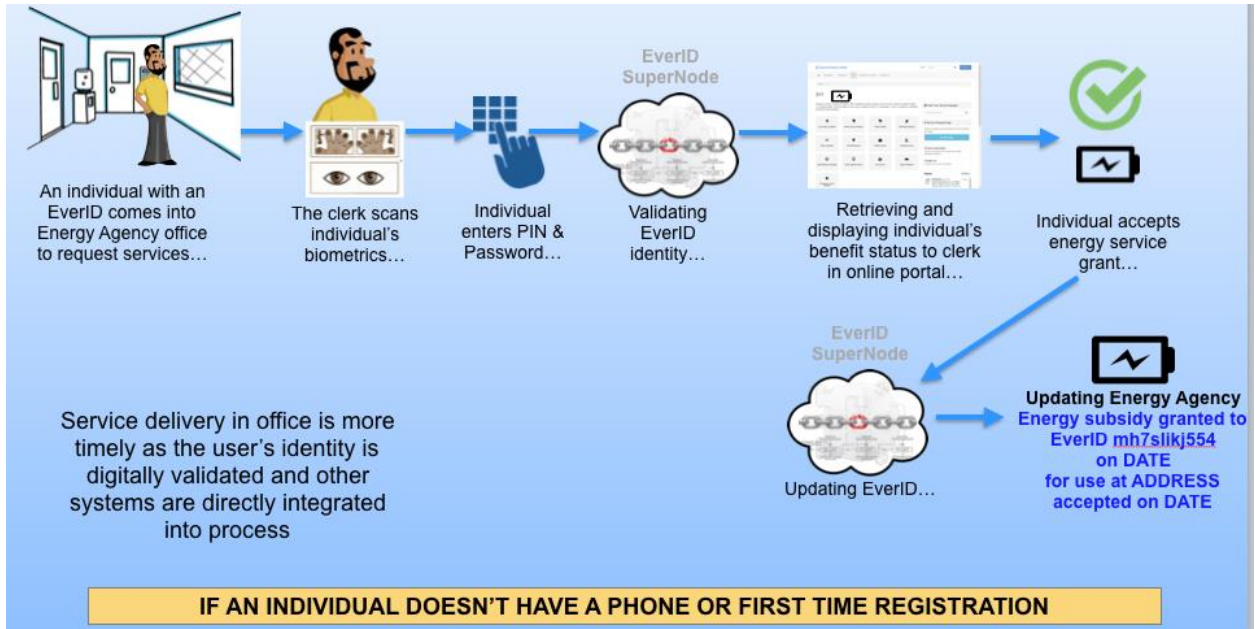
4



At the Raskin Rice Allocation Point, Bastian scans in and enters his PIN, retrieving and displaying his photo and the food assistance grant to the Allocation clerk. The clerk records the amount given, allocating the monthly aid provided to Bastian's family.

- Verification of food aid grant
- Record of amount of food aid dispensed
- Tracking of total food aid provided

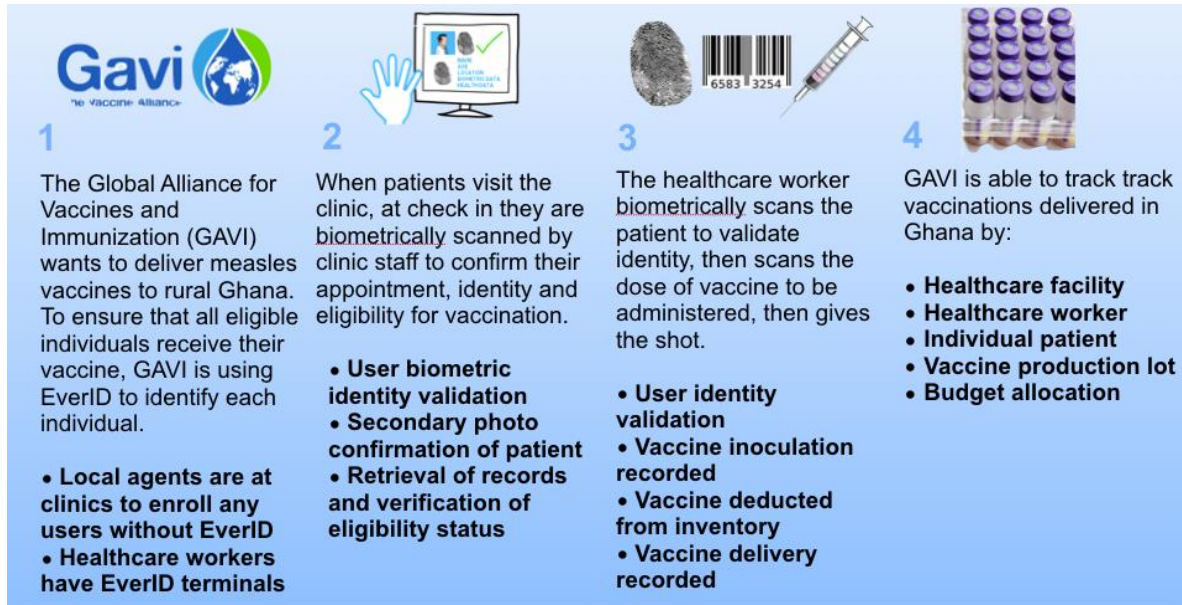
### iii. Energy Subsidy Grant and Renewal



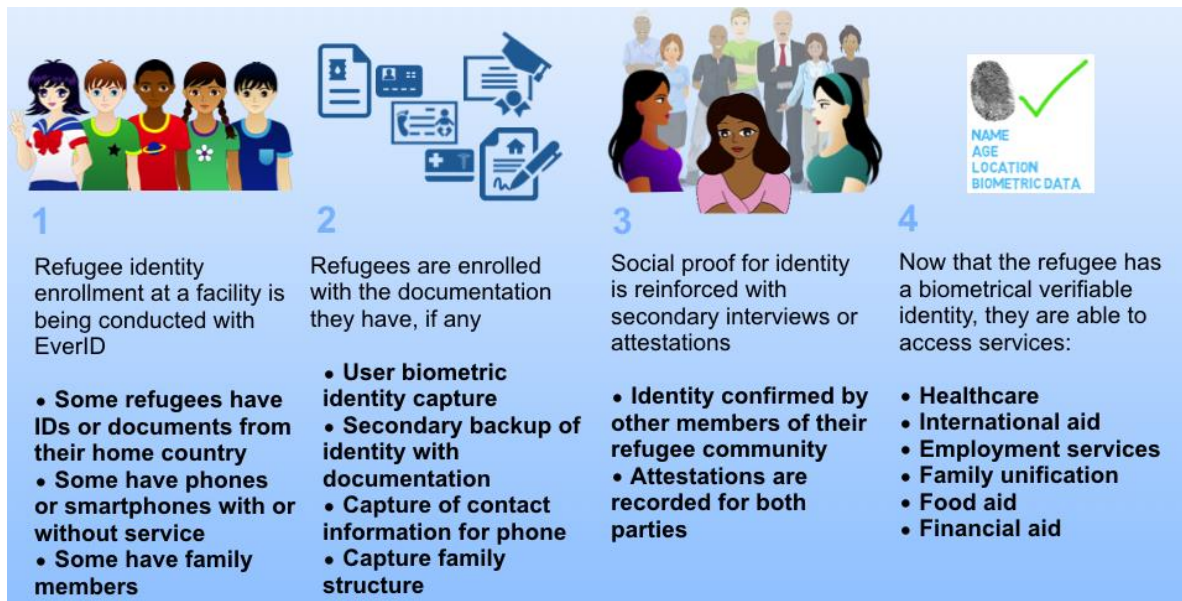


## b. Organizational:

### i. Subsidized Vaccination Distribution Program

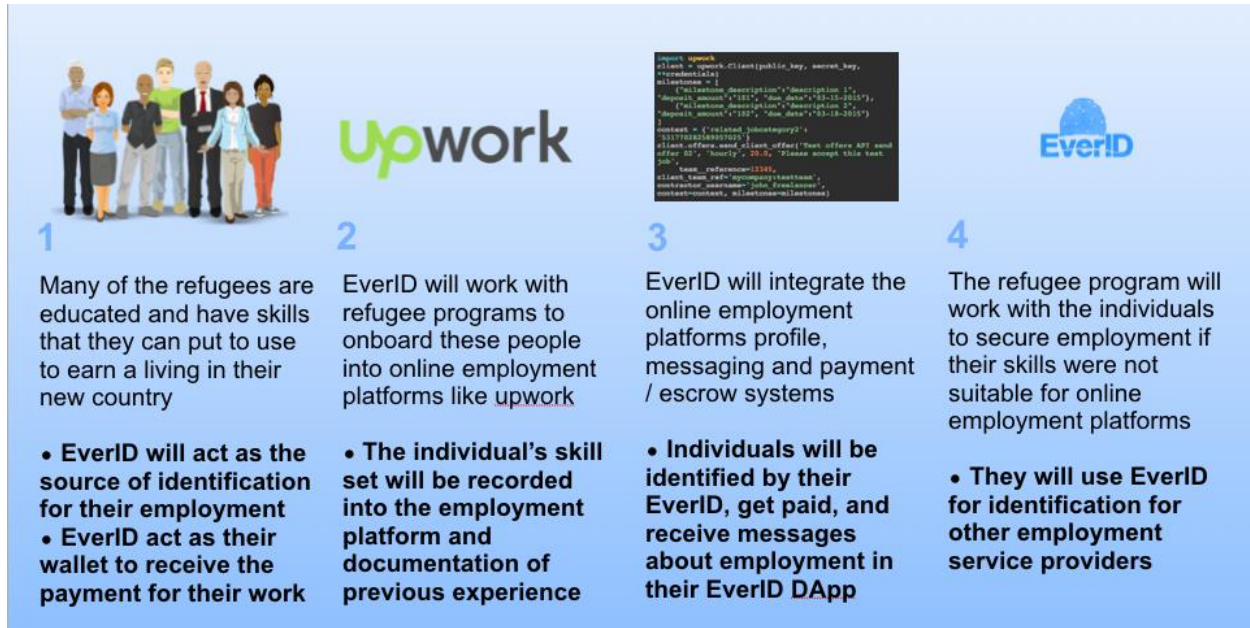


### ii. Refugee Enrollment and Service Delivery

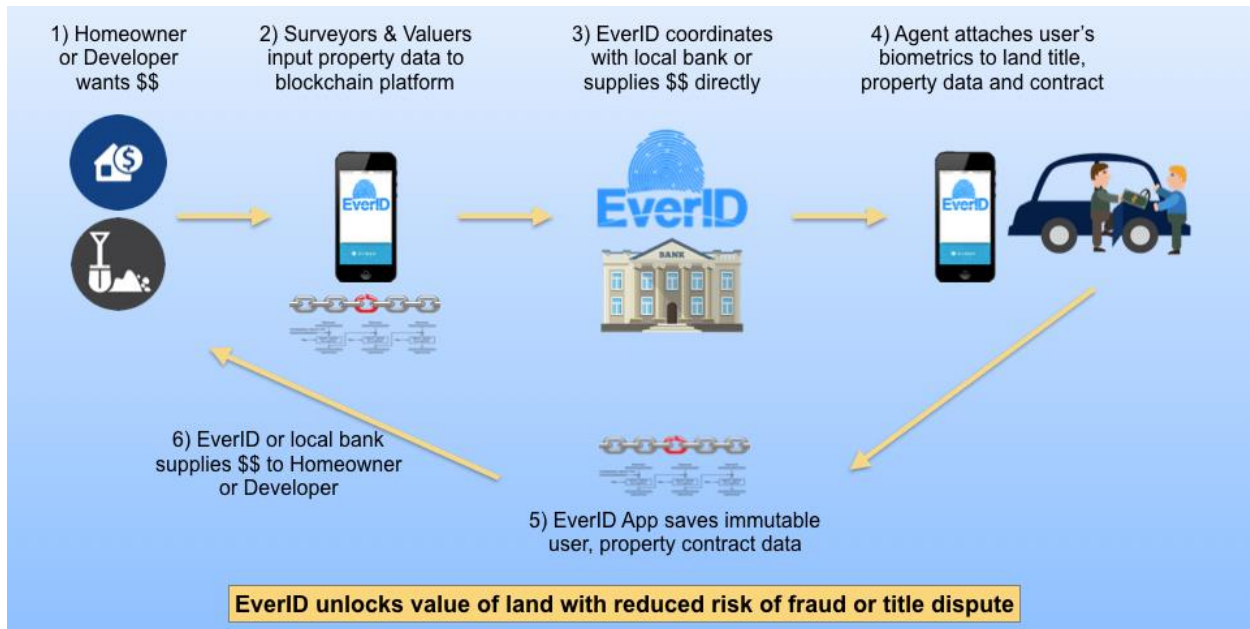




### iii. Refugee Employment Services



### iv. Land Enrollment Platform



# Addendum 6 - Bibliography

## **Cryptocurrencies:**

Nakamoto, Satoshi; "Bitcoin: A Peer-to-peer Electronic Cash System", 2008, <https://bitcoin.org/bitcoin.pdf>

Buterin, Vitalik; "A Next-Generation Smart Contract and Decentralized Application Platform" 2014, <https://github.com/ethereum/wiki/wiki/White-Paper>

Bank for International Settlements, "Committee on Payments and Market Infrastructures, Digital Currencies", 2015, BIS Publishing, ISBN 978-92-9197-384-2

Chiu, Jonathan; Koppel, Thorsten; "The Economics of Cryptocurrencies - Bitcoin and Beyond", 2017, [https://www.chapman.edu/research/institutes-and-centers/economic-science-institute/\\_files/ifree-papers-and-photos/koeppel-april2017.pdf](https://www.chapman.edu/research/institutes-and-centers/economic-science-institute/_files/ifree-papers-and-photos/koeppel-april2017.pdf)

Farell, Ryan; "An Analysis of the Cryptocurrency Industry", 2015, Wharton Scholarly Commons [https://repository.upenn.edu/wharton\\_research\\_scholars/130/](https://repository.upenn.edu/wharton_research_scholars/130/)

Poon, Joseph; Dryja, Thaddeus; "The Bitcoin Lightning Network, Scalable OffChain Instant Payments", 2016, <https://lightning.network/lightning-network-paper.pdf>

<https://themerple.com/what-is-a-pegged-cryptocurrency/>

## **Biometrics:**

Jain, Anil K.; Boelle, Ruud; Pankanti, Sharath; "Personal Identification in Networked Society", 1996, Springer, Boston - ISBN: 978-0-28539-9

Vo, Thi Thuy Linh; Dang, Tran Khanh; Küng, Josef; "A Hash-Based Index Method for Securing Biometric Fuzzy Vaults", 2014, Springer International - ISBN: 978-3-319-09769-5

Mjaaland, Bendik; Gligoroski, Danilo; Knapskog, Svein; "Biocryptics: Towards Robust Biometric Public/Private Key Generation", 2009, NISK-2009

Staff; "National Biometric Security Project - Biometric Technology Application Manual", 2008, National Biometric Security Project [http://www.planetbiometrics.com/creo\\_files/upload/article-files/btamvol1update.pdf](http://www.planetbiometrics.com/creo_files/upload/article-files/btamvol1update.pdf)

Lovisotto, Giulio et al.; "Mobile Biometrics in Financial Services: A Five Factor Framework", 2017, <https://www.cs.ox.ac.uk/files/9113/Mobile%20Biometrics%20in%20Financial%20Services.pdf>

### **Digital Identity in Markets:**

Gelb, Alan; and Clark, Julia, "Identification for Development: The Biometrics Revolution." CGD Working Paper 315. Washington, DC: Center for Global Development. <http://www.cgdev.org/content/publications/detail/1426862>

Zindros, Dionysis S; "Trust in decentralized anonymous marketplaces", 2015, National Tech University of Athens <http://dspace.lib.ntua.gr/bitstream/handle/123456789/43147/pseudonymous-trust-2.pdf>

Soska, Kyle; Christin, Nicolas; "Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem", 2015, ISBN 978-1-931971-232 <https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-soska-updated.pdf>

Lyons, Tom; "The Book Of Fermat Edition 1", 2017, Fermat <https://www.fermat.org/downloads/book-of-fermat.pdf>

Pon, Bryan; Locke, Chris; Steinberg, Tom; "Private Sector Digital Identity in Emerging Markets", 2016, Caribou Digital Publishing, ISBN 978-0-9935152-7-9 <http://cariboudigital.net/new/wp-content/uploads/2016/08/Caribou-Digital-Omidyar-Network-Private-Sector-Digital-Identity-In-Emerging-Markets.pdf>

Makaay, Esther; Smedinghoff, Tom; Thibeau, Don; "Trust Frameworks for Identity Systems", 2017, [www.openidentityexchange.org](http://www.openidentityexchange.org)

Cutler, Joseph; Hansen, J. Dax; Ho, Charlyn; "Self-Sovereign Identity and Distributed Ledger Technology: Framing the Legal Issues", 2017, <http://PerkinsCoie.com/Blockchain>