EverID WHITEPAPER

V= # 2018May4.GA.1.01
   EverID.net

Bob Reid - Bob@EverID.net
Brad Wittean - Brad@EverID.net
### Table Of Contents

1. Abstract  
2. Introduction and Problem Statement  
3. Principles  
   a. Organizational Principles  
   b. Operational:  
   c. Organizational Mandates:  
   d. Technological Principles  
4. Design Approach  
   a. Decentralized ID hub for individuals  
   b. Platform  
   c. Points of Access to Identity  
5. EverID’s Decentralized Identity Platform, the “Identity Network”  
   a. EverID Overview and Technology Stack  
   b. EverID Technology Stack Diagram  
   c. EverID Architecture Diagram  
   d. Biometrics  
   e. EverID Datagram  
   f. EverID DApps  
   g. EverID Application Programming Interface (API)  
   h. EverID Core Smart-contracts  
   i. Ethereum Private Blockchain  

EverID Whitepaper
EverID Whitepaper

6. The EverID Logic Flows
   a. Individual Self-Enrollment
   b. Agent Enrollment of an EverID
   c. Validation of the EverID

7. EverID Economy: ID token + CRDT currency
   a. Holding ID Tokens
   b. CRDT Economy
   c. Incentivized Viable Economic Model:
   d. ID and CRDT Token Example 1:
   e. ID and CRDT Token Example 2:

8. Conclusion

9. Acknowledgements

Addendum 1 - Financing
Addendum 2 - Organizational Identities
Addendum 3 - EverID Datagram
Addendum 4 - EverID API
Addendum 5 - EverID Use Cases

   a. Individual:
      i. Individual Enrollment (Agent)
      ii. Identity Verification, Healthcare & Food Assistance

EverID Whitepaper
iii. Energy Subsidy Grant and Renewal 55

b. Organizational: 56
   i. Subsidized Vaccination Distribution Program 56
   ii. Refugee Enrollment and Service Delivery 56
   iii. Refugee Employment Services 57
   iv. Land Enrollment Platform 57
   i. Micro-insurance Platform 58
   i. Conditional Cash Transfer 58

Addendum 6 - Bibliography 59
## i. Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Biometrics</td>
<td>The measurement and analysis of unique physical or behavioral characteristics of individuals (such as fingerprint, voice patterns)</td>
</tr>
<tr>
<td>Blockchain</td>
<td>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.</td>
</tr>
<tr>
<td>DApp</td>
<td>Decentralized application delivered from a distributed (peer-to-peer) or decentralized network, rather than a centralized server infrastructure.</td>
</tr>
<tr>
<td>Distributed Computer</td>
<td>A computing infrastructure that is dynamically created from a series of peer-to-peer nodes running the same software.</td>
</tr>
<tr>
<td>Ethereum</td>
<td>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.</td>
</tr>
<tr>
<td>IPFS</td>
<td>Interplanetary File System <a href="https://ipfs.io">https://ipfs.io</a></td>
</tr>
<tr>
<td>Public/Private key pair</td>
<td>The cryptographic set of keys used to identify users and to secure transactions on the blockchain.</td>
</tr>
<tr>
<td>Smart Contract</td>
<td>Program on the blockchain which enables for the automated completion of transactions based upon conditions, prerequisites, or user actions.</td>
</tr>
<tr>
<td>Solidity</td>
<td>The smart contract framework within Ethereum, containing code which runs within the Ethereum Virtual Machine contained in the Ethereum wallet.</td>
</tr>
<tr>
<td>Token</td>
<td>Token - currency in distributed application ecosystem stored in wallets</td>
</tr>
<tr>
<td>Wallet</td>
<td>A decentralized software application that can address a cryptocurrency blockchain to transfer cryptocurrency. Includes a user’s Public/Private key pair.</td>
</tr>
</tbody>
</table>
1. Abstract

All value exchange and economic activity, at its root, is based on trust. Historically humans have relied upon their standing in their community or relationship with institutions to confirm their identity in order to facilitate an economic exchange. With recent advances in communication, the world has grown smaller, yet there are still billions of people who lack the ability to prove they are who they say they are, and thus unable to exchange value beyond their small community. Of the 7+ billion people on earth, over 1 billion lack legal identity, close to 1.5 billion lack a bank account, 4+ billion do not have smartphones or digital wallets, and thus are unable to participate in the 21st century digital economy. Existing systems, comprised of centralizing, typically profit-seeking organizations, have failed to empower billions of people with the fundamental rights of a digital identity and value exchange platform. The lack of a user-owned digital identity has hampered value exchange in the emerging and frontier markets for centuries. Given this fact and its disproportionate impact on the developing world, EverID is building the Identity Network (IN): a non-profit stewarded identity and value transfer network for the common good of the planet. Self-funded, transparent, and independent, The IN supplies the protocol & infrastructure for every human being to own & control their own database of identity data, including their biometrics. 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)\(^1\) in software code.
Recent advances in cryptography and permissioned, distributed databases have only now enabled a user-owned identity tool like IN to become feasible. Not tied to ownership of a device, the individual has access to their identity database from the network, enabling 7+ billion humans to scale the economic stack. Recognizing the challenges of delivering ID verification at scale including, time (rapid verification), cost effectiveness (less than a few USD pennies per verification), transaction volume (handle 1-10 billion transactions per month – and scale to trillions) and security (more secure than existing centralized or public distributed databases), led to the specialized network and protocol of IN. Establishing IN as a stand-alone, non-profit foundation, ensures that the network cannot be captured by any actor, including EverID, or the IN Foundation itself. Only non-profit and economic development organizations are allowed to participate in the governance of IN. Further, the IN Foundation & EverID both having signatory rights on any software release, eliminating the concern that a rogue actor could harm the network. Further, a smart-contract will be established to automatically allocate funds to IN to pay for an ever-increasing amount of users & transactions.

EverID is dedicated to liberating humanity from subservience to centralized, non-user friendly identity management and capital allocation organizations by creating a secure, decentralized identity.
management and value transfer system, the Identity Network. 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 and institutions to validate an individual’s identity, transfer value or allocate capital.

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 has architected the Identity Network with a focus on resilience, availability, security, and control, and incentivized participation through an ERC-20 token, the ID.
2. Introduction and Problem Statement

A Verifiable and persistent identity is the foundation of all economic systems. Industrialized societies built robust, functional identity verification platforms, and thus have access to lower cost capital (due to lower perceived risk), which promotes capital concentration, 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. The lack of that identity is a major impediment to service access by the poor and those unable to directly participate in the global digital economy.

With the advent of the IN, that paradigm changes, bringing those communities into the 21st century digital economy by providing them with digital identities, digital wallets, and document management stored on their own database- accessible and controllable by that individual. By incorporating biometrics, existing government IDs and 3rd party attestations that are housed in this distributed, user-owned database, IN extends digital identity, digital wallets and document storage to populations that do not own a personal device; although enrollment requires a smartphone, usage & ownership of this user-centric identity + wallet + documents only requires biometrics (face & fingers) and a PIN. 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 global value exchange in the 21st century economy. Individuals who own mobile phones will be able to expand their digital identity with additional pieces of data, and leverage 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.

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, governments, banks, hospitals, utilities and other large institutions need to verify identities to open a bank account, give & track a vaccine, get a SIM card, etc., and pay ID verification organizations to verify an identity, transfer documents or money securely; in such cases, IN will effectively receive a percentage of the revenue collected, making it self-funding on an ongoing basis. Similarly, a percentage of revenue paid for ID verification will be shared 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. By giving biometrically verifiable identity to individuals, and collectively in organizations in emerging markets, with the ability for institutions
anywhere in the world to create smart contracts with those orgs and individuals, industrialized societies will perceive 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.

3. Principles

A The principles guiding the technical and governance design of EverID reflect the Principles for Identity for Sustainable Development\textsuperscript{2}. 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 and 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 and transparency.

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 user
- The system should be resilient against attack
- The system should be able to bridge to other systems
a. Organizational Principles

- **Inclusion** - The Identity Network is built to address the needs of a world with a projected 10+ billion population. As wealth gaps continue to strain market access for those in the global base of pyramid[^1], EverID leverages the strength of international organizations, non-governmental organizations, governments and foundations to address the needs of the poorest and most vulnerable. The goal is to elevate **all of humanity into the global market**, thereby providing access to a robust set of services to enhance livelihoods and build resilience equitably. Our principle of inclusion is also reflected and integrated into 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 an SDK to add identity validation to devices for banking, government services, healthcare, and more. The Bridge Service allows a user to securely access and use their data on another device that they do not own. IN is architected as a platform in which any individual, with or without a device (currently, there are only 2.1 billion smartphones) can possess digital identity and a wallet with just their biometrics, thus reaching all 7+ billion human beings.

- **Longevity** - The Identity Network non-profit foundation will be endowed and continually funded to exist indefinitely and continue to provide identity verification services to users. The internal governance of the foundation is constructed to provide a clear, standard operating procedures and a mechanism to perpetuate, operate, govern and evolve to be relevant and secure.

- **Specificity** - the key to any economic exchange is knowing the specific individual you are dealing with and with whom you want to transact. To accomplish this, multiple types of biometric information for each identity are recorded and stored in the IN. Legacy identity documents, including national ID cards, driver’s licenses, passports, voter ID cards, etc. are captured, as are 3rd party attestations by cryptographically signing those affirmations of claims.

● **Security** - all information is stored on the user’s devices and in the Identity Network. The system stores the individual’s information in a proprietary encrypted datagram. That datagram is then stored on a decentralized, encrypted, user-controlled storage array, and behind sets of challenge-response locks.

● **Control** - the individual’s data is recorded in a manner that allows the individual (not a government, an organization, or a company, etc.) granular control of how it is shared, with whom, and for how long. This sharing mechanism is enforced by smart contracts per transaction, with automatic resolution.

● **Ownership** - to fulfill the Principles of Identity for Sustainable Development Goals, users must own their own databases, both on-device and on-network. It is no longer prudent to entrust ownership of one’s biometrics and other identity metadata to centralizing forces.

**b. Operational:**

● **Organizational Structure** - EverID is a for-profit organization that is funding the non-profit Identity Network foundation. The IN foundation, is designed to ensure transparency, neutrality, security and longevity of The Identity Network. The economic model will enable the perpetuity of this organization by earning market rates for identity verification. The IN foundation will have an independent board of directors, drawn from internationally and regionally recognized international organization, NGOs, IGOs and philanthropic organizations with the same principles as EverID.

● **Management Team Structure** - the management of the IN foundation and the EverID operating company are mostly different, as their primary focus is different. The IN foundation is governed by a board of Caretakers whose mission it is to ensure the transparency, neutrality, security and 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 is required 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:

<table>
<thead>
<tr>
<th></th>
<th>Centralized Architecture - a central hub coordinates activity within the system.</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Decentralized Architecture - not centralized, not distributed - some centralized resources, some distributed resources. Centralized resources are for coordinating the connections between the distributed resources.</td>
</tr>
<tr>
<td>B</td>
<td>C - a peer-to-peer, mesh network without a centralized resource.</td>
</tr>
<tr>
<td>C</td>
<td></td>
</tr>
</tbody>
</table>
d. Technological Principles

- 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 Identity Network is built on top of the Ethereum Enterprise blockchain, a private blockchain instance hosted on IN foundation 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 to an 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. 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 Identity Network platform 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 Identity Network infrastructure is designed to integrate with other data sources external to the system through the Conduit System and API.

b. Platform

The Identity Network 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 system is always available, the Identity Network foundation will operate hardware clusters to host various software components of the Identity Network 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 Supemode. 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 Identity Network platform.

- Ethereum Blockchain - EverID is built on top of the private Ethereum blockchain, a blockchain instance hosted on Identity Network foundation operated infrastructure and distinct from the public Ethereum blockchain.²

- EverID Supernode - a hosted service environment for the Identity Network 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

² Please note, the private blockchain uses a proof-of-authority system. The Identity Network 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.
The Identity Network 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 IN platform through the EverID API).

Information is able to flow into an EverID 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’s Decentralized Identity Platform, the “Identity Network”

EverID makes the Identity Network, 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 makes 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 Identity Network and consists of: EverID Creation & Management, EverID Validation, EverID Transaction, EverID Remote Management, and Organizational EverID.
• EverID Identity Blockchain records the location of the EverID Datagrams

• IPFS Storage Array 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 Identity Network platform

b. EverID Technology Stack Diagram
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 file 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 4 - 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\(^3\) (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.

h. EverID Core Smart-contracts

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

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

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. Please Note: Organization EverID identity smart contract is covered in Addendum 2.

**EverID Core Smart-Contract Utilization Matrix**

<table>
<thead>
<tr>
<th></th>
<th>Creation &amp; Management</th>
<th>Validation</th>
<th>Transaction</th>
<th>Remote Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>EverID created from DApp</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>EverID created from Agent DApp</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>EverID API Validation</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>EverID API Remote Management</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

**i. Ethereum Private Blockchain**

The EverID decentralized identity platform and associated transaction record are captured and stored in a set of private Ethereum\(^4\) blockchains\(^5\), 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.

---

\(^4\) [https://ethereum.org/](https://ethereum.org/)

j. EverID Supernodes

The Identity Network 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 Identity Network platform. These centralized services include: private Ethereum blockchains, the IPFS storage array for 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 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 EverID 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 EverID Validator service takes care of validation requests to the system and is the first step in nearly all transactions on the 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

1. Individual will have agreed to TOS, EULA and PP in appstore download process
2. Individual provides identity data and scans documents and biometrics
3. Individual’s EverID Datagram created in EverID DApp
4. New EverID is enrolled in ID Blockchain, triggering a write to the Transaction Blockchain of the association between the ID enrolled and the EverID Datagram stored in the IPFS Storage Array
5. Confirmation of the completed new enrollment is added to EverID data in ID Blockchain, and status indicated in the EverID DApp
b. Agent Enrollment of an EverID

1. Agent starts new ID enrollment and enters information provided by Individual
2. Individual provides identity data, and Agent scans documents and biometrics
3. Individual’s EverID Datagram created in EverID Agent DApp
4. New EverID is enrolled in ID Blockchain, triggering a write to the Transaction Blockchain of the association between the ID enrolled and the EverID Datagram stored in the IPFS Storage Array
5. Confirmation of the completed new enrollment is added to EverID data in ID Blockchain, and status indicated in the EverID Agent DApp
6. User is coached on how to use EverID app, how to hail an Agent, how to sign out
7. Agent compensation is contingent on ID validation measures and a minimum time
c. Validation of the EverID

Validating using EverID

- External Request for Validation presented to user
  - Validation Request Response = Public Key + Biometric Capture 1 + PIN returned
  - If Biometric Capture 1 and PIN both match with Biometric Token Array for Public Key = VALID
  - For access to Demographic Data, the user will need to provide Biometric Capture 2
  - If Biometric Capture 2 matches the Biometric Token Array for Public Key = VALID
  - For access to Personal Data, the user will need to provide Password
  - If Password Challenge matches the Password for Public Key = VALID
  - For access to Private Data, the user will need to provide Biometric Capture 3 (1+2 concatenated, resampled)
  - If Biometric Capture 3 matches with Biometric Token Array for Public Key = VALID
  - To recover the user's EverID Datagram from Bridge Service the user will need to provide the User Mnemonic from theirSignup Flow
  - If User Mnemonic matches Mnemonic for Public Key = VALID
7. EverID Economy: ID token + CRDT currency

EverID is the creator and enabler of a new economy, one that has never existed before: the $20 trillion-dollar economy of countries in “emerging markets” will be transformed into $40+ trillion when identity is fixed, true value transfer possible, and human potential realized. By building an identity ecosystem that leverages the power, transparency and security of the blockchain, EverID will catalyze dormant value exchange into a vibrant economy. In order to reshape over 20% of the global economy, EverID utilizes both a utility token, the ID, and a credit or currency, 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 currency that Users & Institutions use to verify identities and exchange value through all the interactions in an economy.

All large organizations that want to transfer value to users encounter issues such as leakage, fraud, friction, verification, data access, cost-effective reach and more. EverID solves these problems for NGOs, IGOs, governments, banks, hospitals, agencies, etc., by cost-effectively verifying user identity with 100% certainty, and tracking service delivery and consumption, verify funds are securely delivered to the “right person”. By permitting users to control access to their biometrics, institutions will be able to validate individual identities with webcams, fingerprint readers or standard feature-phones (users don’t need to have smart phones). 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). With identity validation, users are able to open bank accounts, receive aid, selectively share data with hospitals, e-commerce and other organizations. Thus, creating a platform for institutions and end-users to exchange value in existing economies with full sovereignty, anywhere in the “economic stack.”
Example applications that require ID tokens + CRDTs are below:

- **Cash Transfer** = deliver vouchers with or without conditions
- **Bank accounts** = enable people to set up bank accounts
- **Remittances** = deliver money securely, cheaply anywhere with verification
- **Healthcare** = manage records, validate vaccines and maternal care
- **Land** = ensure titles and deeds are attached to people, making the property bankable
- **Political & legal rights** = vote, file petitions, inherit
- **Payments** = send money: user-to-business or p2p transfer of money, tokens, value
- **KYC/AML** = verify users and institutions comply with banking laws in each jurisdiction
- **Credit scores** = open up financing to individuals and small businesses
- **Complex smart contracts** = establish escrow accounts based on multiple variables
- **Zero-knowledge proofs** = enable institutions and users to verify attributes without giving up privacy
- **Integration into other apps** = accounting, small business and others
- **Storing and managing docs** = birth certificates, refugee status cards, diplomas, certificates
- **Incentivizing & managing users** = rewards programs
- **Refugees** = give a global digital identity w/ wallet & ability to get paid
- **Family reunification** = track loved ones and reunify if separated
- **Food** = disperse food efficiently by verifying biometry
- **Age Verification** = protect women from early marriages, or authorization to enter
- **Gender targeting** = send money to women and ensure only they spend it
EverID will utilize (1) its own token (“ID”) and (2) a credit ("CRDT") strategy as follows:

**IDs** are a utility token enabling access to the network and a myriad of applications and services – literally every exchange of value in an economy. Varying levels of access to network resources are distributed to the holders of the ID tokens. For example, institutions need to stake varying large amounts of IDs to gain tiered levels of access for a limited amount of time (i.e. SDK, API, etc.) and additional amounts of IDs for functions like market-specific applications (medical records, land title, voting eligibility), aggregated data, anonymous geographic market research, credit scores, smart contract functionality beyond simple cash transfer, etc. Additionally, a user may need to stake 1-100 IDs in their wallet if they want to send (not receive) Remittances or Payments from the platform. Since the atomic-level of any economy is identity verification, upon which all value transfer is possible, we anticipate that institutions and users will quickly consume the supply of ID tokens.

a. **Holding ID Tokens**

Institutions which wish to access the various applications in the EverID economy or operate Observer/Transaction Nodes will require the holding of 1,000 to 250,000 IDs, (depending on the size of the institution, user base, access to higher service levels, intended use, etc.), in their EverID Wallet. Such a construct will allow banks, governments, NGOs, hospitals, rewards programs, other large organizations that want to transfer value to verified identities tiered, time-based access to the network and applications.

To most large organizations, the purchase of IDs will look like a non-recurring engineering expense or setup fee, both of which they are accustomed to. With inherent benefits of biometric verification & deduplication, and the cryptography & immutability of the blockchain, EverID will reduce the leakage in cash transfer for institutions, all of whom are required to purchase ID tokens for said benefits. IDs provide differentiated levels of access based upon the amount of IDs maintained in the holder’s wallet. There is no requirement to hold IDs to receive value on the Identity Network, however, it requires IDs to send value or create transactions. Like all economies, the higher levels of data, complexity, visibility & targeting require a larger stake, up to 250,000 IDs. A detailed table follows.
### ID Token Grants Differentiated Access Levels

<table>
<thead>
<tr>
<th>Amount of ID Tokens held in wallet</th>
<th>Access Levels provided</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 ID</td>
<td>Receipt of vouchers</td>
</tr>
<tr>
<td>5 ID</td>
<td>Remittance $1,000 and under</td>
</tr>
<tr>
<td>25 ID</td>
<td>Remittance &gt;$1,000</td>
</tr>
<tr>
<td>100 ID</td>
<td>Organization access to verify IDs</td>
</tr>
<tr>
<td>250 ID</td>
<td>Organization access to send $ no conditions</td>
</tr>
<tr>
<td>500 ID</td>
<td>Organization API access w/ low speed</td>
</tr>
<tr>
<td>1,000 ID</td>
<td>Organization API access w/ medium speed</td>
</tr>
<tr>
<td>5,000 ID</td>
<td>Organization API access w/ high speed</td>
</tr>
<tr>
<td>10,000 ID</td>
<td>Organization access to send vouchers with simple conditions</td>
</tr>
<tr>
<td>50,000 ID</td>
<td>SDK access</td>
</tr>
<tr>
<td>75,000 ID</td>
<td>Observer Node access</td>
</tr>
<tr>
<td>100,000 ID</td>
<td>Organization access to send vouchers with complex conditions</td>
</tr>
<tr>
<td>150,000 ID</td>
<td>Custom smart contracts</td>
</tr>
<tr>
<td>250,000 ID</td>
<td>Full tracking and targeting with market sector specific applications</td>
</tr>
</tbody>
</table>
b. CRDT Economy

By selling ID tokens, EverID will raise capital to establish a CRDT-based economy. The CRDT will be used as a digital credit or currency that allows institutions and end-users who have access to the platform to purchase services and applications on the Identity Network including all of the aforementioned applications. 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. Basic operations on the EverID platform will require the spending of CRDTs and 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).

In the process of institutions paying for identity verification, sending of money, managing of documents, etc., EverID will earn revenue in US dollars or other liquid currencies, which will be converted to CRDTs. 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.

An example of the market for identity verification can be found in India, where identity verification costs $0.015 to $0.077 per verification; as of February 2017, there were 16 million verifications per day, and currently averaging 139 million per month of the roughly 1 billion identities. Over $3.3 billion dollars has been sent over such a platform, reducing leakage & fraud and increasing payouts by 12-20%. EverID will offer similar services and share in the savings. 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 EverID will earn a good percentage (i.e. 30% or $45 million) of the transfer savings. Similarly, managing documents for institutions, like governments, banks and hospitals requires storage, conditional access & permissions, all services which institutions pay for (i.e. a health agency in a given country will pay USD $100s of millions for such a platform).

In the future, EverID may engage in micro-financing by loaning CRDTs, which is a more stable exchange of value than many others. The combination of financial services on smart contracts with biometrically verifiable and traceable transactions, establishes EverID as the standard in user-centric identity that is able to bridge to existing institutions. In offering a stable form of exchange and 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.

c. 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.
Where possible, the CRDT will be tradable into local currency or cell phone minutes to provide support for universal basic income.

End-users do not need to own IDs to receive value as a consumer on the network. Transactions can only be done in CRDT credits/currency, and incentive rewards are based in CRDTs. For example, when a consumer registers and opens an EverID wallet, EverID could deposit 10 CRDTs in their wallet. When they validate their ID, they could get another 10 CRDTs, when they invite a friend who signs up, 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 currently pegged to the USD and can be used to transact on the Network or can be cashed in for fiat less a transaction fee.

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

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 and 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.

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.
d. ID and CRDT Token Example 1:

To send money back to her parents in her home country, Susanna purchases and holds the required 5 ID tokens in her EverID wallet unlocking the “Send Funds” functionality in the EverID DApp. She is able to take the CRDTs earned by participating in the EverID economy as well as her income from various side jobs and send them to her mother’s EverID wallet. Her mother receives notification on her feature phone (via SMS) that she has a new EverID notification awaiting her. She then goes to her local EverID Agent, logs into her EverID, and indicates that she wants to withdraw the CRDTs as local currency. The EverID Agent receives her CRDTs and hands her the equivalent amount of the local currency at today’s exchange rate (provided by the EverID Agent DApp). If the mother has her own smartphone, she is able to receive CRDTs directly into her wallet, and either spend them with other CRDT users or convert them into fiat currency via a local agent.

e. ID and CRDT Token Example 2:

A large organization is using EverID to manage sending funds to beneficiaries in many countries as well as to pay their local agents and employees in each of the countries. The organization is holding 250,000 IDs in their Organizational EverID wallet. When approved, this affords them access to the API to be able to integrate data exchange with their legacy systems. It also allows them to integrate the EverID verification capabilities into their own applications via the SDK and API. They are also able to create custom smart contracts for their uses, like a 90% attendance requirement for their agents and employees to earn bonuses at the end of the year, or an integrated supply chain feedback loop based upon how many children are showing up to school each week. Through the management portal they are also provided with the deepest levels of data analysis and additional insights based upon system-wide statistical analysis. The purchase and holding of the ID tokens are similar to the up-front license for an SDK or prepaid fee for access to an API, so they are easily able to manage the accounting of this in their finance department. When the large organization verifies identities, sends money, manages docs or otherwise conducts value exchange over the platform, they pay market rates in fiat currencies, which are converted into CRDTs; and a percentage of those CRDTs are given to each user that the organization verifies or deals with.
- Institutions/senders buy ID tokens to access network
- Institutions pay for various applications in USD. EverID converts USD into CRDT currency to drive ecosystem
- Each transaction carries a smart-contract to give a % of profits to User

<table>
<thead>
<tr>
<th>Service</th>
<th>CRDTs Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID verification</td>
<td>2</td>
</tr>
<tr>
<td>P2P Payments</td>
<td>3</td>
</tr>
<tr>
<td>Doc Agent</td>
<td>25</td>
</tr>
<tr>
<td>Remittances</td>
<td>35</td>
</tr>
<tr>
<td>B2C Money Transfer</td>
<td>100</td>
</tr>
</tbody>
</table>
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 a 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 technology life cycles of decentralized computing, biometrics, mobile devices, and wireless networks are sufficiently mature to support widespread adoption - the time is ripe for a distributed, encrypted, user-owned identity database platform. Decentralized computing is a viable store of value and application platform with the creation of Bitcoin and Ethereum, and is now considered to be sufficiently mature technologies to be the foundation of other solutions. Mobile telephony devices have increased in capability to the point that local biometric systems are able to be used, and the processors are able to calculate cryptography sufficiently quickly to handle the associated tasks on demand. The EverID protocol and platform have been purpose-built to instantiate the Principles of Identity for the Sustainable Development Goals, and build a scalable, robust and equitable economy for the planet.
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 - Financing

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. 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 and June, 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.

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. 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. Roughly USD $25M to $50M will be offered in a Presale round at a 25% discount.

Reserve: 25% of IDs are allocated for future employees, other value exchange and future sales.

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 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 use of funds 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 and Crowdsale, EverID will offer up to the remaining IDs of the 400,000,000, that were not sold in the seed round.

Funding the Identity Network Foundation

EverID will fund the Identity Network foundation to set up and 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.

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, autonomous network.

- **Board of Directors**:

  EverID Whitepaper
○ 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
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 contact. 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.

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

**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:**

<table>
<thead>
<tr>
<th>Resource URI</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/search</td>
<td>Search the database using a string query for {name} (user name) and PIN, which returns a public key for biometric challenge.</td>
</tr>
<tr>
<td>/v1/search/{name}?pin={pin} (GET)</td>
<td></td>
</tr>
<tr>
<td>/everid</td>
<td></td>
</tr>
<tr>
<td>/v1/everid/validate/publickey?bt={token},pin={pin} (POST)</td>
<td>Perform a validation of the biometric token {token} and {pin} for an individual's public key.</td>
</tr>
<tr>
<td>/v1/everid/retrieve/publickey?url={datagramuri},part={part} (POST)</td>
<td>Retrieve a {part} of an EverID from its IPFS storage array location {datagramuri} for an individual's public key.</td>
</tr>
<tr>
<td>/transaction</td>
<td></td>
</tr>
<tr>
<td>/v1/transactions/create/publickey?txid={txid} (POST)</td>
<td>Creates a transaction {txid} for the individual who's public key is given in the request URI.</td>
</tr>
<tr>
<td>/v1/transactions/retrieve/publickey?txid={txid} (POST)</td>
<td>Retrieves the status of a transaction {txid} for the individual who's public key is given in the request URI.</td>
</tr>
<tr>
<td>/v1/transactions/update/publickey?txid={txid} (POST)</td>
<td>Updates a transaction {txid} for the individual who's public key is given in the request URI.</td>
</tr>
<tr>
<td>/v1/transactions/close/publickey?txid={txid} (POST)</td>
<td>Closes a transaction {txid} for the individual who's public key is given in the request URI.</td>
</tr>
<tr>
<td>xid={txid} (POST)</td>
<td>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 &quot;close&quot; to stalled transactions may be necessary.</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>/v1/transactions/status/publickey?txid={txid} (GET)</td>
<td>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.</td>
</tr>
<tr>
<td>/config</td>
<td></td>
</tr>
<tr>
<td>/v1/config/reportencoding (POST)</td>
<td>Set the error report MIME type.</td>
</tr>
<tr>
<td>/v1/config/reportlocation (POST)</td>
<td>URI to send error reports.</td>
</tr>
<tr>
<td>/v1/config/debug (POST)</td>
<td>Enable or disable debugging output, which is sent using the report encoding and report location parameters for delivery format and location.</td>
</tr>
</tbody>
</table>
Addendum 5 - EverID Use Cases

a. Individual:

   i. Individual Enrollment (Agent)
ii. Identity Verification, Healthcare & Food Assistance

1. 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 rescans 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

Service delivery in office is more timely as the user’s identity is digitally validated and other systems are directly integrated into process.

**IF AN INDIVIDUAL DOESN’T HAVE A PHONE OR FIRST TIME REGISTRATION**

- An individual with EverID and a mobile phone...
- Receiving notification of a renewed energy service grant...
- Scans their biometrics to confirm their identity...
- Enters PIN & Password...
- Accepts renewed energy service grant...
- Updating the user’s EverID and pushing data to integrated organizations

**Energy Agency**
Energy subsidy granted to
EverID mh7/slikj554 renewed on DATE
for use at ADDRESS accepted on DATE

**IF AN INDIVIDUAL HAS A PHONE... renewals with EverID require no office visit - completely automated on user’s device**
b. Organizational:

i. Subsidized Vaccination Distribution Program

The Global Alliance for Vaccines and Immunization (GAVI) wants to deliver measles vaccines to rural Ghana. To ensure that all eligible individuals receive their vaccine, GAVI is using EverID to identify each individual.

- Local agents are at clinics to enroll any users without EverID
- Healthcare workers have EverID terminals

When patients visit the clinic, at check in they are biometrically scanned by clinic staff to confirm their appointment, identity and eligibility for vaccination.

- User biometric identity validation
- Secondary photo confirmation of patient
- Retrieval of records and verification of eligibility status

The healthcare worker biometrically scans the patient to validate identity, then scans the dose of vaccine to be administered, then gives the shot.

- User identity validation
- Vaccine inoculation recorded
- Vaccine deducted from inventory
- Vaccine delivery recorded

GAVI is able to track vaccinations delivered in Ghana by:

- Healthcare facility
- Healthcare worker
- Individual patient
- Vaccine production lot
- Budget allocation

ii. Refugee Enrollment and Service Delivery

Refugee identity enrollment at a facility is being conducted with EverID

- Some refugees have IDs or documents from their home country
- Some have phones or smartphones with or without service
- Some have family members

Refugees are enrolled with the documentation they have, if any

- User biometric identity capture
- Secondary backup of identity with documentation
- Capture of contact information for phone
- Capture family structure

Social proof for identity is reinforced with secondary interviews or attestations

- Identity confirmed by other members of their refugee community
- Attestations are recorded for both parties

Now that the refugee has a biometrical verifiable identity, they are able to access services:

- Healthcare
- International aid
- Employment services
- Family unification
- Food aid
- Financial aid
iii. Refugee Employment Services

Many of the refugees are educated and have skills that they can put to use to earn a living in their new country.

- EverID will act as the source of identification for their employment.
- EverID act as their wallet to receive the payment for their work.
- EverID will work with refugee programs to onboard these people into online employment platforms like upwork.
- The individual’s skill set will be recorded into the employment platform and documentation of previous experience.
- Individuals will be identified by their EverID, get paid, and receive messages about employment in their EverID DApp.

The refugee program will work with the individuals to secure employment if their skills were not suitable for online employment platforms.

- They will use EverID for identification for other employment service providers.

iv. Land Enrollment Platform

1) Homeowner or Developer wants $$
2) Surveyors & Valuers input property data to blockchain platform
3) EverID coordinates with local bank or supplies $$ directly
4) Agent attaches user’s biometrics to land title, property data and contract

6) EverID or local bank supplies $$ to Homeowner or Developer
5) EverID App saves immutable user, property contract data

EverID unlocks value of land with reduced risk of fraud or title dispute
i. Micro-insurance Platform

**Sell**

1) Agent sells insurance with app, registering ID, collecting money & giving Anna a smart-contract tied to her biometrics

2) Insurance Co. collects premiums, along with smart-contract info.

**Service**

1) Anna gets sick, goes to hospital

2) Doctor at hospital attests that Anna is sick & "cryptographically signs" w/ his/her biometrics

3) When claims come, verifies costs, attestations, issues claim per contract

4) Agent & Anna receive confirmation that premium has been paid digitally or in fiat

Micro-insurance w/ biometrics + smart contract platform

---

i. Conditional Cash Transfer

1 A woman is interested in getting assistance (i.e. food)

2 An "agent" registers her identity & gives her an EverID wallet

3 WFP leader has $100k budget for food to disperse. Typically, only 60-70% makes it to end-user

WFP leader sends food voucher to registered users in a smart-contract. 100% transparency on money sent!

4 Food voucher sent to woman's ID/ biometrics & wallet

5 The woman scans face or fingers, or uses phone to retrieve/spend her voucher. 100% verification. 100% of budget delivered.

Manage service & cash delivery to users over EverID smart contract platform
Addendum 6 - Bibliography

Cryptocurrencies:


Farell, Ryan; "An Analysis of the Cryptocurrency Industry", 2015, Wharton Scholarly Commons https://repository.upenn.edu/wharton_research_scholars/130/


https://themerkle.com/what-is-a-pegged-cryptocurrency/
**Biometrics:**


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


**Digital Identity in Markets:**


Makaay, Esther; Smedinghoff, Tom; Thibeau, Don; "Trust Frameworks for Identity Systems", 2017, www.openidentityexchange.org
