VERIDIUM

Blockchain, Biometrics, and Owning Your Own Identity: The 'Horcrux' Protocol

Currently, we depend on governments to issue identity credentials. These identity documents are physical representations, like passports, birth certificates, and driver's licenses, of information kept by a central authority, typically in protected digital storage today. However, the physical copies are used independently of those centralized systems for identification for convenience and portability. You can open a bank account or travel on an airline by using only your driver's license for identification, as it represents a verified set of data about you.

However, if lost or stolen, these documents can be used by identity thieves to wreak havoc on our lives. Replacing your documents can be an expensive, painful and arduous process.

Proving You Are You

How would you replace your driver's license if lost? Normally, you walk into a government office like the Motor Vehicles Department, fill out a form, and a clerk compares your face with the picture in their system. Your face is partial proof of identity in addition to knowledge of your personal information such as your home address. Your physical presence is also another form of proof of your identity.

Proving and securing your online identity is much more difficult. Can you open a bank account without visiting a branch in person? In most jurisdictions, the answer is no, because banks depend on physical identity credentials to prove you are who you claim to be. Banks depend on reliable proof of identity to fulfill anti-money laundering requirements and enforce know-your-customer compliance. You must appear in person to attest to your identity in the presence of another person. Furthermore, in some jurisdictions, like Mexico and Brazil, banks use biometrics and are required to check all clients against national criminal databases.

In the near future, banks and other institutions will be able to prove your identity online without requiring your physical presence or documents. Biometrics collected securely on mobile platforms will allow institutions to enroll new clients remotely, but linking your biometrics to an existing identity remains a formidable hurdle.

It is now possible to open a bank account online in the Netherlands and comply with national identity requirements via online enrollment. Ironically, the online enrollment process involves a video chat session that still requires you to present a national ID or passport. Instead of the physical document, a trusted authority is needed to broker the enrollment transaction between the user and bank. Indeed, governments (and private companies outsourced to provide such services) are beginning to offer online identity services. However, until recently no standards existed to guide these efforts, so different deployments vary greatly.

Building a Standard for Identity Proofing

Protocols like SAML, OAuth2, and OpenID Connect (OIDC) are first steps to brokering identity online via trusted identity services. These protocols introduce third-party identity providers that can hold your credentials and relieve service providers from having to collect, store and manage identity credentials. Whenever you see "Login with Google" or "Login with Facebook", that's SAML and OIDC in action behind the scenes.

These protocols can also only share those credentials that you approve to share with service providers in order to preserve your privacy. For example, if a website requires you to be over 18 years of age, such protocols can be used only to confirm this (or not) without divulging your birth date, name, or any other sensitive data. They can reliably provide some identity credentials, but only to the account associated with the identity at Google, Facebook, etc. However, these credentials are typically not tied to government identity credentials, so they cannot be used by banks and other financial institutions.

So, who should hold your definitive identity credentials? A company? A local government? Regional? National? An international entity? Any centralized service risks being a single point of failure in the case of fraud or cyber attack. The broad consensus of the identity community for the past few years has been that any such service should be decentralized, enforce information integrity, be resilient to attack, and that the individual user should be the ultimate owner and sovereign controller of their own identity credentials. Their conclusion is that blockchain technologies offer the only solution to satisfying all of these requirements.

Why Blockchain?

Around a dozen companies are currently working on digital identity solutions that exclusively use a blockchain to store identity credentials. Proposed methods, like Decentralized Identifiers (DIDs) by the W3C Credentials Community Group, may be used in the future to secure your identity credentials via blockchain. DIDs are stored on a blockchain and "point" to off-chain objects called DID Descriptor Objects (DDOs). DDOs could represent many types of objects including verifiable claims for a given identity (e.g., proof-of-age). Such claims could be issued by enterprises like banks or government agencies, but remain in a citizen's sovereign control after issuance. Your credentials will be independent of a central authority with added security benefits like integrity and non-repudiation inherent with blockchain technologies.

Note: personally identifiable information (PII) should never be stored on a blockchain. A DID refers to an off-chain DDO that could contain encrypted PII.

Why Identity Matters

Soon after the release of the Bitcoin protocol, many people realized that blockchain transactions can house more than just "coin" transfers – they could represent birth certificates, property deeds, academic credentials, and more. They could be used to record almost anything so that the information attached to a transaction (e.g., via OP_RETURN operands) was highly available, decentralized, and tamper-evident.

Using blockchain for digital identity is the logical next step. Today, your passport, driver's license, birth certificate and other forms of identity are recorded primarily on paper, kept on your person or in filing cabinets in your home or office. Although many of these documents have been scanned as digital images, the metadata associated with these documents is sparse. Over a dozen projects now underway hope to solve this problem by issuing identity credentials via blockchains such that they are highly available, decentralized and tamper-evident. Some of these projects include:

- **Blockstack:** Formerly known as "onename," transactions are recorded on the Bitcoin blockchain to associate an identifier (i.e., a symbolic name) with a local identity stored on your laptop or mobile device.
- **Sovrin:** A permissioned, decentralized identity network based on Hyperledger Indy, an open-source distributed ledger technology. The non-profit Sovrin Foundation has launched the Provisional Network consisting of independently-operated nodes.
- **Veres One:** A blockchain-agnostic method for representing decentralized identity credentials based on the W3C Community Group's work on DIDs and DID Documents.
- **uPort:** A decentralized identity platform built on Ethereum. It provides an open-source SDK for mobile development and authentication for many programming languages.

One goal of all of these projects is to enable self-sovereign identity (SSI) transactions like two-party authentication: You provide your credentials to the service provider directly. Existing protocols like SAML and OAuth require three parties: You, the service provider and the identity provider (i.e., "Login with Google", "Login with Facebook", etc.). Two-party authentication allows you to use blockchain-based credentials to enroll and authenticate with websites without the need for third-party identity providers during an authentication session. Identity records on blockchains may be issued by an authority (e.g., a government), but they are controlled by each individual user. Control means that the private key(s) of the credentials are held by the user, not the issuing authority. Self-sovereign identity is an empowering concept, but many critical issues remain problematic:

Revocation

Identity credentials on blockchains may need to be revoked at some time in the future. For example, a driver's license may be revoked by the DMV due to driving infractions. Verifying that a credential is valid may require validating a digital license credential and checking a list of revocation records as well.

Delegation

Use of credentials may be delegated. For example, issuance of a child's passport may require presentation of that child's digital identity by a parent or guardian. Delegation can be attenuated to specific privileges, capabilities, and time.

Minimization

The purchase of alcohol in many countries requires a "paper" form of identity, such as a driver's license or passport, to verify proof of age via birthdate. But this method divulges too much information because all the clerk needs to know is the veracity of the "claim" that you are of age or not. The W3C Verifiable Claims Community Working Group is tackling protocols and formats for expressing and sharing such claims via self-sovereign identity platforms.

Recovery

Most approaches to self-sovereign identity require ownership of private keys associated with identity credentials issued via blockchains. Such keys can be kept on USB tokens, mobile phones, or paper form.

The recovery issue seems the most difficult to solve: What happens if I lose the mobile device, token, slip of paper or forget the passphrase associated with my private key? Early public-key distribution systems had similar problems and failed to scale because keys could not be shared, revoked or recovered without a trusted but centralized infrastructure. Blockchain technologies promise to solve these problems via novel, decentralized key distribution systems within and across various blockchain ecosystems.

Two approaches have been proposed: Social recovery and biometric recovery. In the case of social recovery, you recruit a handful of friends at enrollment time to attest to your identity and store pieces of your identity credential (or associated recovery credentials). In the case of biometric recovery, you can recover your identity credentials yourself but may require live evidence to prevent spoofing by bad actors. Friends come and go, but your biometrics are relatively stable throughout your lifespan. Thus, biometrics may be the foundational backstop to identity credential

methods when used in combination with other methods including social, token and paper-based approaches.

Securing the Blockchain for Identity Usage

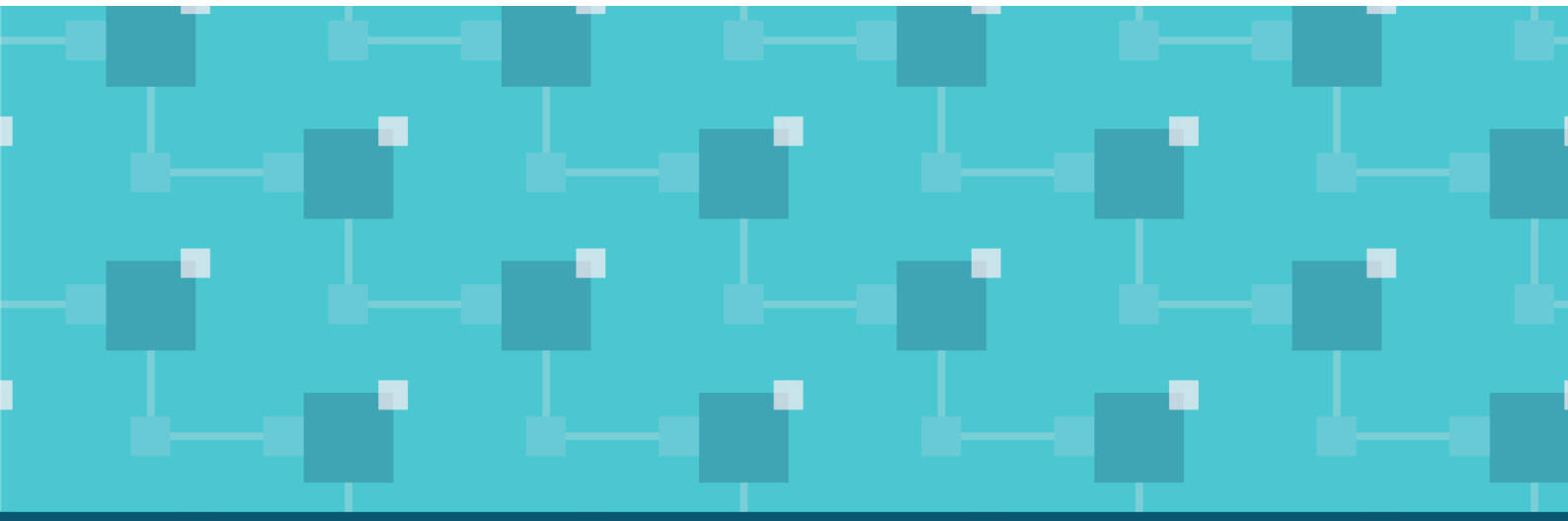
Biometrics will also play a critical role in how you will claim a given identity credential is yours on a blockchain. Blockchains are pseudo-anonymized and designed to be opaque to identity. Can blockchains be used to broker verifiable claims? How will you associate yourself with those claims and prevent others from claiming your credentials? Biometric authentication is the clear answer.

Enterprises will play a critical role in the issuance of verifiable claims and verification of the identities associated with those claims. To be associated with a claim, you must either know something (e.g., a password), have something (e.g., a token) or be something (e.g., biometrics). But if the password for a blockchain credential is lost, it may be very difficult, if not impossible, to recover, because there is no authority to appeal to for replacement. A token can be lost or stolen, so that leaves biometrics as the strongest candidate for identity credential management on blockchains.

The Horcrux Protocol

Most online identity systems are limited in the sense that they can't be tied to your real-world identity. They fail to provide sufficient levels of assurance needed for full digital identity management. Your driver's license, passport or other credentials are based on PII tied to your real identity. Many of the self-sovereign identity projects rely on issuers, who may perform biometric-based identity verification and proofing checks, to create cryptographically sealed identity credentials on a blockchain. At authentication time, the user and relying party use the blockchain-based credentials without the need for an intermediate identity provider. The user (or "holder") provides a DID for the issued credentials to the relying party. The relying party can resolve the blockchain object (a DID Document) to access the user's credentials, initiate the required authentication steps, and grant authorization (or not).

Storing your biometric data on a blockchain is not advised. Any personally identifiable information should be stored in off-chain storage as a verifiable claim with a cryptographic reference to the data placed on a blockchain for integrity and provenance. One could also divide the biometric data into "shares" using Visual Cryptography to further protect the information in separate off-chain records. Secret sharing is a relatively recent technique for dividing up a



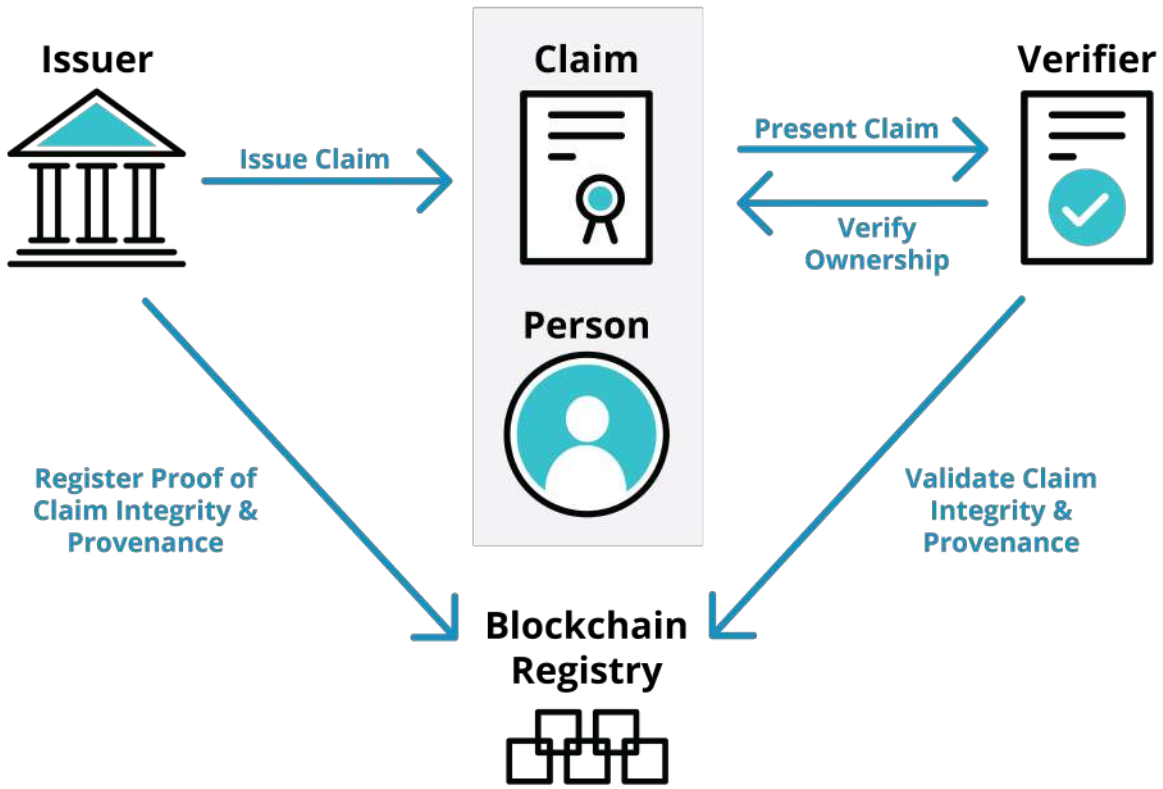
piece of information into two or more shares such that the secret cannot be divulged unless ALL the shares are combined. By securing the shares (hiding, encrypting, etc.), they can be better protected.

In the Harry Potter series, the antagonist, Lord Voldemort, divides his soul and hides the pieces in common objects called “horcruxes” that are hidden around the world. Voldemort cannot be killed unless all his horcruxes are destroyed first. Our idea is similar: Your biometric data, split into shares, is stored separately in off-chain storage that you control and sealed via blockchain references for integrity and provenance. This could provide protection, privacy, and availability even in the case of loss of your device and associated keys.

The Veridium Model

The IEEE 2410-2017 Biometric Open Protocol Standard allows two or more biometric shares to be divided between the mobile device and servers using a secret sharing technique called visual cryptography. In a traditional client-server model, two shares are created upon enrollment of the initial biometric vector (IBV) in which one share is reserved on the mobile device and one is sent to the server. If either share is lost or compromised, the other share cannot be reconstructed, and the original biometric data cannot be recovered either.

This secret sharing technique reduces the risk of compromise in case of exposure of either share separately. At authentication time, the shares are combined for match comparison with a candidate biometric vector. Matching can occur on the mobile device or server. According to the IEEE 2410-2017 standard, the server’s biometric share is stored in a “persistence cluster” that may be implemented by any storage layer such



as an RDBMS, NoSQL database, or distributed file system so long as it meets the encryption requirements for the biometric shares.

This storage layer can also be implemented using a blockchain-based technology such that separate relying parties could access a share via a blockchain given its identifier (like a DID). During enrollment, an IBV share is stored in an off-chain DID Document and digitally signed by the issuer. The corresponding DID is then issued to the user and kept on the enrolled mobile device along with the other IBV share. The blockchain-based share is only accessible via a cryptographic challenge to the mobile device that holds the other share.

At authentication time, the user can give the DID to a new relying party. That party resolves the DID to the corresponding DID Document containing an IBV share. The relying party checks the issuer's signature and authenticates the user's access to the DID Document (e.g., via a mobile device possession verification similar to FIDO UAF). Then, the user's IBV share from their mobile device and the off-chain IBV share are combined and matched to a candidate biometric vector (CBV) for authentication. The match can occur on the server or mobile device depending on the configuration, policies and jurisdictional regulations.

Conclusion

Your personal data, biometric or otherwise, should always remain under your control. Whether stored on a mobile device or a cloud storage provider, self-sovereign identity places that control firmly in your hands. And secret sharing and asymmetric encryption can help secure the data via blockchain-based verifiable claims for integrity and provenance. This doesn't just help prevent injury and loss from third-party data breaches, it maintains privacy in an increasingly digital future.

While we haven't achieved this future yet, self-sovereign identity and the organizations working on blockchain-based identity provisioning are helping usher it forward. Ultimately, by using blockchains and associated storage providers, institutions no longer need to store customers' personal credentials, reducing security risks, increasing privacy, and putting control of our digital identities back in our hands.

www.VeridiumID.com
info@VeridiumID.com

United States

33 Arch Street
Boston, MA 02110
877.301.0299

United Kingdom

119 Marylebone Road
London NQ1 5PU
United Kingdom
+44 1753 208780