Bitcoin Suisse | Decrypt

September 3, 2019 | Season 1 Episode 7

The Identity of the Future

The digital world is becoming increasingly important in our everyday lives. Personal data often needs to be shared over the Internet. What part can blockchain technology play in the protection of identities against theft or fraud?

Written by Dr. Raffael Huber from Bitcoin Suisse Research
and Demelza Kelso Hays and Mark J. Valek from incrementum

More and more personal data is stored all over the Internet. This has made it easier to steal somebody's identity. Personal identification data may be obtained illegally from centralized storage servers or reconstructed using social engineering. In our digitalized world, considerable damage can be caused by impersonating someone else – both from a financial and social perspective, for example by accessing online accounts.

> *"So what is identity theft or fraud? Fundamentally, it's someone other than you trying to "spend" your identity or, put differently, more than one party trying to use the same identity twice. Viewed this way, it's clear that identity fraud is simply a double spend problem."*
> *– Elizabeth M. Renieris*

As such, it is necessary to redesign the current system to account for these modern threats. Blockchain technology may present a solution to this: By decentralizing identity, it is possible to avoid creating data silos which can end up being honeypots for malicious actors. The control of when and how data is shared is put back into the hands of individuals. The potential of *decentralized identities* (DIDs) has been recognized by a consortium of more than 80 industry leaders,[1] who are working together towards creating standards for DIDs.

An implementation of a possible identity standard has been proposed[2] for the Ethereum blockchain in the form of ERC-725 by F. Vogelsteller, the creator of the omnipresent ERC-20 token standard. ERC-725 allows for *self-sovereign identities*: Users have sole ownership over their digital identities and can prove claims about it without needing an intermediary.

Blockchains are immutable by design. While this is a key part of their value proposition, it creates a problem for identity management systems. Identities are mutable – elements such as residence or citizenship may change over the years. Government-issued ID cards expire after a while. Thus, a blockchain-based identity system needs to have functionalities that allow for the updating of the claims or data points about one's identity.

1. https://identity.foundation/
2. https://erc725alliance.org/

Another issue with the concept of decentralized identity is Article 17 of the GDPR, which describes the "right to be forgotten."[3] It dictates that "data subjects" can request erasure of their personal information from services that have collected them. Blockchains, however, do not forget. As such, it is a challenge to use blockchain for identity management while remaining compliant with regulations – personal data must not touch the blockchain in unencrypted form. However, government agencies could provide cryptographic hashes (digital fingerprints) of the personal identity data and digitally sign them to confirm the validity of the fingerprint.

Recent incidents have shown the importance of data privacy – as our digital footprints increase, this will only become more relevant. The business risks[4] of storing personal data have become more apparent, and the trend is reversing from collecting as much user data as possible to as little as needed.

Cryptography also provides a potential solution to this issue: *zero-knowledge proofs*. Zero-knowledge proofs are ways to prove a certain fact without revealing the fact itself. How this is possible can be illustrated as follows: Consider two friends, Peggy (the *prover*) and color-blind Victor (the *verifier*). Peggy has two billiard balls, which are indistinguishable, apart from the fact that one is green and the other is red. Peggy wants to prove to Victor that she can differentiate between the two balls without telling him the colors directly. She hands the balls over to Victor, who puts them behind his back and then reveals one ball to Peggy. He moves the ball behind his back again, and then chooses one of the two at random to reveal. Due to its color, Peggy will easily be able to tell whether Victor has swapped the balls behind his back or not. Her chance to get the right answer with a random guess is 50 %, though – so the process needs to be repeated many times. After 10 iterations, the chance that Peggy randomly guessed them all correctly drops to <0.1 %. As a result, Peggy has proven with high certainty that she can indeed distinguish the balls without revealing any additional information.

Zero-knowledge proofs are broadly applicable. For example, a ticket seller that provides cheaper prices for people older than 65 years does not need to know the exact age of its customer, but only needs to verify the validity of the claim. Another example would be to prove residence in a non-sanctioned country to a cryptocurrency marketplace, without needing to reveal the exact country.

The underlying blockchain protocol that these identity management systems are or will be built on is going to generate plenty of real economic value. This raises the general question: How much of the real economic value that is generated through public blockchains will be captured by its payment or utility coin? We will dig deeper into this in a future episode of Bitcoin Suisse Decrypt.

Breaking Blockchain Myths: Bitcoin Can be Easily Hacked

Newcomers to blockchain hear about hacks and erroneously believe that Bitcoin has been hacked. **For the record, Bitcoin has never been hacked**. Instead, centralized companies that offer cryptocurrency services are being hacked. There are three main types of cryptocurrency hacks: exchange wallets, software bugs on the protocol level, and personal information stored by third party service providers. According to Chainalysis, almost $2 billion worth of cryptocurrencies has been hacked from exchange wallets to date.[5] Exploits of smart contracts, such as the 2016 Decentralized Autonomous Organization hack and the multiple Parity hacks in 2017, account for a total loss of over 4.5 million Ethereum.[6] Finally, user details like passport numbers can be hacked from centralized companies. The most recent example is Binance's hack that leaked the account information of up to 60,000 users.

Data security breaches put our personal information at risk. In 2013, the web services providers Yahoo breached the details of 3 billion accounts – marking the largest corporate hack in history.[7] Chase Bank, Marriot Hotel, and Adult Friend Finder are just a small sample of the online companies that have been successful targets for online hack attacks.

When a credit card number is hacked, the bank can issue a new card with a new number. When a driver's license is lost, the new replacement comes with new numbers. However, social security numbers stay with the same individual for their whole life. In 2017, the US credit bureau Equifax revealed the social security numbers of approximately 143 million Americans. Stolen social security numbers allow thieves to steal billions in government welfare and benefits, to borrow money from banks via fraudulent mortgages and loans and to evade taxation by logging work income to other peoples' social security numbers.

3. https://gdpr.eu/article-17-right-to-be-forgotten/
4. https://www.wsj.com/articles/equifax-reaches-700-million-settlement-over-data-breach-11563798429
5. https://blog.chainalysis.com/reports/crypto-crime-hacks
6. https://cryptoresearch.report/crypto-research/smart-contracts/
7. https://abcnews.go.com/Technology/marriotts-data-breach-large-largest-worst-corporate-hacks/story?id=59520391

Financial loss is not even the largest threat when it comes to social security hacks. Our entire democracy depends on the safekeeping of our personal identification numbers, because most countries link voter IDs to individuals with valid social security numbers. There have been over 130 reported cases of election fraud at the national level[8] meaning that fake ballots are impacting global democracy.

According to a 2018 report by Stanford University, only eight percent of the current blockchain projects are working on digital identity.[9] **The main obstacle: We have not figured out how to build a blockchain that can verify if real-world data like identity of a human is true**. Just storing the personal details of registered voters will not be enough to stop voter fraud. Turing impossible proofs are an avenue of research that is trying to understand how to create proofs that humans can validate easily but that are difficult for artificial intelligence machines to parse. This goal is to stop bots from casting fake votes with fake identities.

> *"Blockchains don't guarantee truth; they just preserve truth and lies from later alteration, allowing one to later securely analyze them, and thus be more confident in uncovering the lies."*
> *– Nick Szabo*

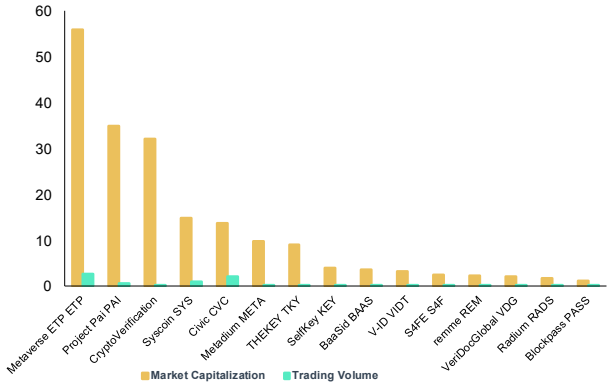
Another avenue is randomization. As Santiago Siri of the Democracy Earth Foundation explained, the Greeks employed a randomization technique called the Kleroterion in order to reduce corruption. By randomly selecting public officials for one-year terms, it made it difficult to bribe the network in order to achieve a particular outcome. A similar system could theoretically be applied to the nodes that store data on each voter's identity.

A third area of research into secure digital storage of each human's identity is trying to completely remove social security numbers from the equation, because social security numbers are inherently easy to hake and fake. Microsoft's Political Economist Glen Weyl prompts us to rethink identity on a philosophical level.

According the Weyl, each person is simply a collection of information, and fragments of this information are sharded across the people that we share our lives with including our family, friends, and colleagues. For example, my mother's birthday is also the date of birth of my mother. This one date connects two people. This is how identity existed prior to social security numbers being issued by centralized organizations. Many cultures linked each person's name to the name of their parent, such as Stepanovich, meaning son of Stepan in Slavic languages, and Nikolajsen, meaning son of Nikolaj in Scandinavian languages. The point is that the more complex the set of data that we use to map a person's identity, the harder it will be to fake and steal. For example, GPS coordinates from cellphones, first grade teacher names, and location of home can all be used to build a robust personal identity. Various companies are trying to build oracles that can work with smart contracts in order to overcome some of the problems associated with first generation blockchains.

Can blockchains achieve social impact and not only financial impact? The verdict is still out. There are 29 digital identity cryptocurrencies that are currently trading. Total market capitalization is $193.92 million with a 7-day sector return of -12.77 %.

Illustration 1: Over 15 exchange traded identity cryptocurrencies have a market capitalization of over one million USD.



Source: cryptoslate.com, Incrementum AG.

8. https://en.wikipedia.org/wiki/List_of_controversial_elections
9. https://www.gsb.stanford.edu/sites/gsb/files/publication-pdf/study-blockchain-impact-moving-beyond-hype.pdf

Bitcoin Suisse AG
CH-6300 Zug
bitcoinsuisse.com

in collaboration with

incrementum