Using Smart Contracts for Governance and Identity

Alberto Garcia, Cameron Dennis
Andia

Norma Elva Chavez, Amy Ruckes
West Virginia University (WVU), Blockchain Accelerator Foundation

Eber Betanzos, Saiph Savage
Universidad Nacional Autonoma de Mexico (UNAM)

ABSTRACT

As large-scale cybersecurity attacks continue to violate the fabric of trust in government agencies and technology companies, users look toward a future where they no longer need to disclose sensitive personal information (e.g., driver's license ID) when purchasing regulated or controlled products. To further this vision, we propose the development and deployment of a privacy-preserving digital identity system that uses biometrics, short-term memory neural networks, and reinforcement learning to verify purchasers of regulated products. This blockchain-based system leverages smart contracts to allow users to seamlessly manage their own profile and flexibly decide what data to share and when. Furthermore, our hypothesis was validated that regulated vendors (e.g., cannabis dispensaries and bars) are eager to adopt such a system in order to prevent the sale of a controlled substance to an unauthorized consumer. Our biometric system can also be implemented to regulate the purchase of guns and pharmaceuticals, assist border patrol, manage welfare payments, and enable seamless cross-border movement. Thus, potentially creating harmonious digital bonds between an individual's mobile identity and their identity within society at large.

1. DIGITAL IDENTITY TECHNOLOGY

The motivation for this research focuses on potential cyber security risks. Data on individuals is generally maintained by central parties (e.g., banks and companies) [2], which can face serious security threats and vulnerabilities. Individuals are powerless to control and track the usage of their private data, such as fingerprints. Current practices of identity authentication are not highly effective as evidenced by the exploitation of fake IDs and illegal immigrant identification [8]. Another motivation is the need to facilitate the flow of capital securely and seamlessly on a global basis [1, 6, 7, 5]. As global migration becomes "one of the defining issues of the 21st century [9]" and identity authentication becomes ever more important [8], secure international systems that transcend geographic, societal, cyber, and governmental boundaries are essential [3, 4].

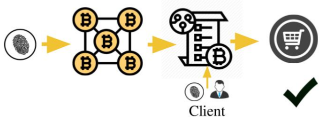

Figure 1: Combining Biometrics and Blockchain for Smart Sales

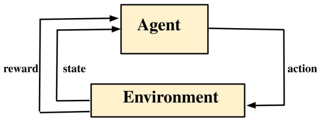

Figure 2: Reinforcement Learning Model to Detect Clients

Biometrics has been increasingly used as a tool for identity authentication. In this project, we propose a novel approach to combine three authentication methods together, namely: something a person knows, e.g., a passphrase; something a person has, e.g., a photo ID; and something a person is, e.g., face pictures. This identification process enables highly secure but privacy-preserving authentication via blockchain/smart contract technology. The basic ideas are a.) to leverage blockchain to store an individual's attestation and the hash value of her biometrics, b.) to use smart contract for controlling the access to the information on the blockchain, c.) to utilize a mobile interface for granting permissions, and d.) to leverage short-term memory and reinforcement learning to enable accurate identity verification.

Our solution involves an easy four step process (see Fig 1). The client inputs her biometric data into the blockchain. The blockchain enables a distributed, trusted way to store people's biometrics. When the client wants to buy a certain product, she inputs her biometrics and the system uses Smart Contracts on the blockchain to decide whether the person should be allowed to buy it. Any store can use the system to intelligently decide whom to sell to based on previous financial transactions and behavior.

Using a reinforcement learning model enables our system to learn to detect clients from the individual's attestations and biometrics stored in the ground truth information in the blockchain. This machine learning iteration process is used to better track clients and improve the accuracy of the system. A demonstration of our technology is available through the link provided[1].

Acknowledgements. This work was partially supported

Third International Symposium on Foundations and Applications of Blockchain (FAB '20) May 1, 2020, Santa Cruz, California, USA.

[1] Check out the demo at https://andia.gitbook.io/mobile/

by an NSF CITeR grant and NSF grant FW-HTF-19541.

2. REFERENCES

[1] Chiang, C.-W., Betanzos, E., and Savage, S. Blockchain for trustful collaborations between immigrants and governments. *arXiv preprint arXiv:1805.01512* (2018).

[2] Chiang, C.-W., Betanzos, E., and Savage, S. The challenges and trends of deploying blockchain in the real world for the users' need. *Journal of Cyberspace Studies 3*, 2 (2019), 123–136.

[3] Chun, W. C., Eber, B., and Saiph, S. Deploying real world blockchain systems. *Cyberspace studies* (2019).

[4] Chun-Wei, C., Eber, B., Michael, A., and Saiph, S. Designing blockchain technology to transform rural communities. In *CHI conference on Human Factors in Computing Systems* (2019).

[5] Forum, W. E., and Accenture. The known traveller unlocking the potential of digital identity for secure and seamless travel, Jan 2018.

[6] Hardjono, T., and Pentland, A. Verifiable anonymous identities and access control in permissioned blockchains. *arXiv preprint arXiv:1903.04584* (2019).

[7] Hardjono, T., Smith, N., and Pentland, A. S. Anonymous identities for permissioned blockchains, 2014.

[8] Jacobovitz, O. Blockchain for identity management. *The Lynne and William Frankel Center for Computer Science Department of Computer Science. Ben-Gurion University, Beer Sheva* (2016).

[9] Rubinstein, A., and Orgad, L. Global migration crisis.