The Digital Avatar on a Blockchain

E-Identity, Anonymity and Human Dignity

UNIVERSITÄT GRAZ
UNIVERSITY OF GRAZ

Mag.[a] Nora Schreier (University of Graz) *nora.schreier@uni-graz.at*
Dr. Robin Renwick (Trilateral Research) *robin.renwick@trilateralresearch.com*
Univ.-Prof.[in] Dr.[in] Tina Ehrke-Rabel (University of Graz) *tina.ehrke@uni-graz.at*

TRILATERAL RESEARCH

INTRODUCTION

With the rise of new technologies, the way individuals interface with reality has significantly changed in the 21st century: Personal data is constantly being gathered and transmitted by way of data subjects' mobile devices. Efforts of business operators to link different sets of personal data "scattered" in the digital realm have led to an increasing power imbalance between data subjects and respective business operators. [1] Current developments in the finance sector focus on the establishment of secure, robust and persistent identifiers for customers. However, technological, legal and ethical questions are still to be answered concerning topics such as privacy, data protection, inclusivity, human rights, and finally, human dignity. This is especially the case in the finance sector, where private business operators play an important role for the functioning of the economy and act, partially, as agents of the state.

DLT AS ONBOARDING FRAMEWORK IN THE FINANCIAL SECTOR

A Distributed Ledger Technology (DLT) infrastructure provides an architecture to store information regarding onboarded customers of financial institutions in a transparent, tamper-resistant and decentralized way. [2] Due to its distributed character, the ledger is highly resilient to cyberattacks as stored data is distributed across multiple nodes. [3] In the finance sector, DLT can be used as an evidential framework for attested credentials issued by financial institutions in regard to personal data collected from financial institutions' customers. The processing of personal data is based on the obligations to "Know Your Customer", laid down in Anti-Money Laundering Law. The potential of DLT is to put the financial services user in control of their own personal data and thus, their digital identity. [4]

THE MOBILE DEVICE AS INTERFACE

Acting as a gateway to the digital domain, the mobile phone is an important tool for financial service providers to mitigate security concerns. Financial service providers are motivated to mitigate security risks through data-led techniques including location-based tracking, network log analysis, and biometric authentication, and potentially extending measures to include analysis of mobile phone or social network usage, messages and behavioural biometrics. [5] In order for customers to prove that certain credentials have been issued and stored on the blockchain, public key infrastructure may be used. The management of the users' private keys in these systems are often left to wallet providers, which constitutes a single point of failure. [6] Moreover, in most cases the users will access the blockchain by using an application on their mobile phone. Since digital applications enable the invisible and multi-faceted collection of the device users' data, their use can create delicate privacy issues. [7]

ACKNOWLEDGEMENT

SOTER

This poster is based on research undertaken in the EU-funded SOTER project which has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 833923

LEGAL CHALLENGES

If a permissioned blockchain architecture is used as evidential framework for customer onboarding in finance, legal challenges arise from different factors: the specific properties of DLT as a technical framework for identity management, the sensitivity of the collected personal data, the extent to which it may be processed and the qualification of financial services as essential services, and the governance and trust frameworks in place for sharing data, and ensuring proper legal liabilities and accountabilities are maintained.

<u>Main regulatory challenges:</u>

- DLT infrastructure
  - Allocation of legal responsibility to ensure fundamental rights' protection
  - State supervision of financial institutions participating in the network
- Mobile Devices as interfaces
  - Ensure that consent is informed and freely given
  - Central management of the users' private keys by a wallet operator entails security and privacy risks
- Human Dignity at Risk?
  - Massive data collection through digital applications entails the risk of permanent surveillance and thus endangers the concept of human dignity as enshrined in our liberal democratic society's DNA

CONCLUSION

Although the idea to grant the customer more control over their personal data can benefit from distributed ledger technology, the legal framework has yet to evolve in order to ensure adequate protection of the customer against an infringement of their fundamental rights. There might even have to be a change in current interpretation of fundamental rights – leaving behind a strictly formalistic approach and turning towards a more holistic understanding of the concept of human dignity at the very heart of a free and democratic society.

REFERENCES

[1] Abulaziz Alzubaidi & Jugal Kalita, *Authentication of Smartphone Users using Behavioural Biometrics*, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, Mar. 2, 2016, at 1998; Ahmed Mahfouz et al., *A Survey on Behavioral Biometric Authentication on Smartphones*, 37 JOURNAL OF INFORMATION SECURITY AND APPLICATIONS 28, 31–35 (2017); Karen Yeung, *Five Fears about Mass Predictive Personalization in an Age of Surveillance*, 8 INT'L DATA PRIVACY LAW, Sept. 15, 2018, at 258; SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR THE FUTURE AT THE NEW FRONTIER OF POWER (2019).

[2] Jean Bacon et al., *Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers*, 25 RICH. J. L. & TECH. 1, 21–22 (2018); Primavera De Filippi & Aaron Wright, Blockchain and the Law 34 (2018); Dirk A. Zetzsche et al., *The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain*, U. ILL. L. REV. 1361, 1374 (2018).

[3] De Filippi & Wright, *supra* note 1 at 34.

[4] Alan Morrison, *Biometric Data Matching Risks and the Rise of Self-Sovereign Identity*, *in* Autonomous systems and the law 99, 102 (Nikita Aggarwal et al. eds., 2019).

[5] Uri Rivner, *Identity Crisis: Detecting Account Opening Fraud in the Age of Identity Commoditisation*, 1 CYBER SECURITY: A PEER-REVIEWED JOURNAL 316, 321–322 (2018).

[6] Kelvin F. K. Low & Eliza Mik, *Pause the Blockchain Legal Revolution*, 69 INT'L & COMPAR. L. Q. 135, 158 (2020).

[7] MIREILLE HILDEBRANDT, SMART TECHNOLOGIES AND THE END(S) OF LAW: NOVEL ENTANGLEMENTS OF LAW AND TECHNOLOGY (2015).