DD2485 - Programmable Society

Digital Passport - Better Security and Privacy with Blockchain Technology

Fabian Zeiher
December 3, 2023

1 Introduction

International Border Crossings remain a daunting procedure for many even in the "globalised" world we live in today. Outside of supranational organisation (e.g. European Union) we rely on our passports and Visas to regulate entry, exit and duration of stay in a foreign country. Often important information like work-permits and state social welfare benefits are only granted to holders of specific Visas. Many processes today are still largely paper based which comes with major risks and inefficiencies [1].

International travellers have experienced queuing at immigration and organisations have confirmed a need to increase capacity in order to meet future travel demand [2]. In case a passport is lost or stolen, the process of re-issuing the passport including the connected Visa is often long and stressful because of a lack of information exchange between countries [1]. Another major risk is identity theft which can be very dangerous for the legitimate owner if their identity is used to commit crimes. For states the forgery of passports and Visa is also a problem they try to mitigate.

Today the Machine Readable Travel Document (electronic passport) and Machine Readable Visa (electronic Visa) is the defacto standard, where personal information of the user is stored together with the cryptographic public key of a trusted issuing authority. "A major advantage of the electronic passport lies in the fact that it improves significantly the protection against falsification. This level of security is based on Public Key Cryptography, which guarantees integrity, authenticity, and confidentiality of stored data." [3]. However, even if our data is securely stored on a chip, travellers are often forced to hand data over to organisations, airlines, car-rentals, etc. where we have no insight into the security of their infrastructure. Successful hacking attacks, with data breaches where sensitive private data is stolen from users happen because many database systems in use today are not secure enough, according to David Treat, a managing director and global blockchain lead at Accenture [4].

Distributed Hyperledger Technology (DLT), which is currently synonymous with Blockchain technology, can improve the current situation significantly in two ways. First, it can provide a single storage layer for travellers' identity data that is durable, always accessible as well as attack proof. Sensitive data does not need to be copied and stored many times at different organisations, lowering the opportunities for data breaches significantly [5]. Secondly it presents an opportunity for the individuals to regain full control over their private data [6]. This is facilitated once again by Private Key Cryptography as mentioned above for electronic passports, but in the context of blockchain a much more powerful concept called zero-knowledge proofs can be utilised [7]. Users could simply submit a proof of access, or proof of visa instead of providing their data to the verification agency to check their eligibility for access or authenticity of visa documents.

However, Blockchain based solutions are not infallible either [5]. Implementations need be checked thoroughly, as the devil is in the details with safety critical software. In the following chapters we will first dive into digital self-sovereign identity (SSI) systems based on DLTs. Next we will explore the opportunities of zero-knowledge proofs, especially with regards to to data privacy and sovereignty. We explore biometrics as a posssible solution to the core problem of unique identity in SSI systems. The chapter on State of the Art (SOTA) will outline an already existing implementation of a blockchain based digital passport system. Finally a Reflection and Opinion chapter will present personal thoughts and considerations.

2 Digital Identity

The core building block to a digital passport / digital Visa is a digital (personal) identity. This is also a much more active research and development area with a number of publications every year and multiple promising implementations already in production or under development. A well known blockchain powered digital identity platform is the Estonian ID card.

Following Sullivan and Tyson [5] I define digital identity as a set of digital data that can establish an individuals identity for official purposes. Christopher Allen [8] and later extended by Stokkink and Pouwelse [9] have defined 11 criteria that self-sovereign identity (SSI) systems must adhere to. The following descriptions where shortened by the author.

1. **Existence** - unique identifier attached to a real life identity

2. **Control** - user must have full control
3. **Access** - user must have unrestricted access
4. **Transparency** - SSI system must be open-source
5. **Persistence** - identity must be durable
6. **Portability** - identity must not rely entirely on a third party
7. **Interoperability** - protocol must be interoperable
8. **Consent** - any manipulation of the identity must be consented by the user
9. **Minimisation** - minimal information is shared
10. **Protection** - legitimate rights of users must be protected
11. **Provability** - user claims must be verifiable

Most SSI systems today use decentralised identifiers based on public-key cryptography and so-called verifiable assertions [10]. Decentralised identifiers are used to identify an individual and associate attributes to them. The verifiable assertions (also called attestations) are essentially stamps of approval by a trusted organisation that has verified a claim by a user about themselves as being true [9]. While these systems are powerful, they still require the user to reveal personal information to the verifier in order to collect assertions [10].

3 Zero-knowledge proofs

Zero-knowledge proofs (ZKP) can be added as an additional layer to existing SSI solutions. "Zero-Kowledge Proof protocols pave the way toward technologies embedding privacy-first principles for data transmission." [10]. In all zero-knowledge proof systems, a prover can convince a verifier that a specific statement is true without leaking any additional information to the verifier [7]. E.g. a traveller could proof to be more than 18 years old without disclosing their actual age. This allows travellers to remain anonymous and avoid revealing unneeded information while verifying agencies still receive all necessary proofs to satisfy security procedures. For these systems to scale it is important to use non-interactive ZKP protocols like the current SOTA: zkSNARKs [11], BulletProofs [12] and skSTARKs [13]. Thinking this further, the implications for passport and Visa systems are exciting. Individuals could submit a verifiable proof of their access rights to immigration without disclosing who they are and how they obtained their access rights. One could proof to a potential employer that one has the right to work without sharing the work permit itself, which may contain sensitive personal information. The zero-knowledge proofs can also be engineered in such a way, that they expire after the verifier has verified them. This is supported by the idun3 protocol[1]. Another existing SSI system that utilises ZKPs is SelfKey [14].

4 Unique Identity

A major challenge for SSI systems is to ensure that each digital identity represents a unique human being, called proof of personhood (PoP). Most systems rely on existing government issued documents for this, e.g. passport number, social security numbers, etc. [9]. SelfKey [14] have proposed a novel anti-bot / anit-forgery system which they claim ensures PoP. The solution is build on community driven re-verification of credentials. Every credential that is created must be backed by a collateral in the form of their native cryptocurrency. If community members can detect and proof a fraudulent or invalid credential they receive a part of that collateral as a reward. This makes creating false identities costly and creates an incentive to actively seek and remove them from the system.

Another interesting opportunity to create unique identities for SSI systems are biometrics [15]. Biometrics could solve the unique identity problem by creating cryptographic identifiers from biological features that uniquely identify individual humans. We all know these from our smartphones in the form of fingerprint readers or Apples FaceID system. In the SSI space a very prominent example of such a system is Worldcoin with their WorldID project[2]. They created an instrument that scans the iris in the human eye. These iris scans are used to create an IrisHash which uniquely represents a single iris. However, like many biometrics systems WorldCoin has also been in the critique over privacy and how the company acquires the data necessary to train the machine learning based iris scanner [16].

5 SOTA

There already is a functioning implementation of a Digital Passport concept called Known Traveller Dig-

[1] https://iden3.io

[2] https://worldcoin.org

ital Identity [2] backed by the World Economic Forum that allows paperless travel between selected airports in Canada and the Netherlands. The projects primary goals are to increase capacity at airports to cope with future travel demand and to enhance security. The core idea is that travellers collect so called attestations which the travellers can choose to share with authorities and companies. Attestations are a verified claim - e.g. proof of citizenship, proof of entry, etc. - issued by a trusted entity and stored on a blockchain together with the public key of the trusted entity to proof the authenticity of the claim. Verifying organisations can trust these attestations and therefore skip the step of re-validating original documentation during each interaction. It must be noted, that no personal traveller data is stored on the blockchain, but only shared directly between verifying agency and traveller, if requested by the organisation and approved by the traveller. The finished prototype was never put to the test as travel was heavily restricted during the Covid 19 pandemic [17].

6 Reflection / Opinion

Digital Passports are very likely the future of international travel for many people around the world. If not for the honourable reason of enabling control for individuals over their own data, then because forgery of digital documents will be much harder while efficiency and security of external border controls can be improved. This is why it is crucial that the general public gets involved into the development of this technology as early as possible in order to ensure a result that is desirable for the general public. In my opinion, implementations like KTDI [2] are already moving forward in an undesirable direction, that does not increase self-sovereignty over individuals data. There is no clear definition about what constitutes a trusted organisation and who decides who is a trusted organisation? To collect the attestations in the KTDI system, travellers still need to share their personal data without ZKPs protecting their privacy. I argue that zero-knowledge proof layers are not just an optional layer to digital passport systems in order to improve privacy, but a necessity to ensure self-sovereignty and security. We should aim for a system where individuals prove their access rights threw zero-knowledge claims while keeping their identity data private. Projects like iden3[3] advance the field with interesting concepts that are also very relevant for digital passports. For example, non-reusable proofs, that cannot be taken by a verifier and presented to a third-party [18]. Further, it is crucial that no personal data is stored in a centralised system, be it encrypted or not, which is especially true for biometrics data, which currently collected into massive centralised databases by governments worldwide posing major privacy risks and ethical concerns [19]. A major benefit of the paper passport is the fact the we can take it home with us and store it safely, a feature that we should keep in the digital version.

7 Conclusion

Digital passports are a promising solution to improve security and privacy. A good digital passport solution should be DLT based and include a zero-knowledge proof layer. Major challenges especially around Proof of Personhood and data privacy remain unsolved. It is important that the general public gets involved into the development of this technology as early as possible in order to ensure a result that is desirable for all.

8 Academic Misconduct

I certify that generative AI, incl. ChatGPT, has not been used to write this essay. Using generative AI without permission is considered academic misconduct.

References

[1] S. Panchamia and D. K. Byrappa, "Passport, VISA and Immigration Management Using Blockchain," in *2017 23RD Annual International Conference in Advanced Computing and Communications (ADCOM)*, Sep. 2017, pp. 8–17. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8691939

[2] "KTDI." [Online]. Available: https://ktdi.org/

[3] D. Butnaru, "The Electronic Visa – Solutions to Shift from Paper to Chip," in *ISSE 2011 Securing Electronic Business Processes*, N. Pohlmann, H. Reimer, and W. Schneider, Eds. Wiesbaden: Vieweg+Teubner Verlag, 2012, pp. 330–337. [Online]. Available: http://link.springer.com/10.1007/978-3-8348-8652-1_29

[4] S. R. Kelleher, "Paradigm Shift: Biometrics And The Blockchain Will Replace Paper Passports Sooner Than You Think,"

[3] https://iden3.io

Jun. 2019. [Online]. Available: https://www.forbes.com/sites/suzannerowankelleher/2019/06/28/paradigm-shift-biometrics-and-the-blockchain-will-replace-paper-passports-sooner-than-you-think/

[5] C. Sullivan and S. Tyson, "A global digital identity for all: the next evolution," *Policy Design and Practice*, vol. 6, no. 4, pp. 433–445, Oct. 2023, publisher: Routledge _eprint: https://doi.org/10.1080/25741292.2023.2267867. [Online]. Available: https://doi.org/10.1080/25741292.2023.2267867

[6] N. Sahi, A. Liang, W. Van Devanter, K. Oikonomou, and P. Zhang, "Self-Sovereign Identity in Semi-Permissioned Blockchain Networks Leveraging Ethereum and Hyperledger Fabric," in *2023 IEEE International Conference on Digital Health (ICDH)*. Chicago, IL, USA: IEEE, Jul. 2023, pp. 315–321. [Online]. Available: https://ieeexplore.ieee.org/document/10224738/

[7] M. Petkus, "Why and How zk-SNARK Works," Jun. 2019, arXiv:1906.07221 [cs, math]. [Online]. Available: http://arxiv.org/abs/1906.07221

[8] C. Allen, "The Path to Self-Sovereign Identity," Apr. 2016. [Online]. Available: https://www.lifewithalacrity.com/article/the-path-to-self-sovereign-identity/

[9] Q. Stokkink and J. Pouwelse, "Deployment of a Blockchain-Based Self-Sovereign Identity," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1336–1342. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8726562

[10] M. Dieye, P. Valiorgue, J.-P. Gelas, E.-H. Diallo, P. Ghodous, F. Biennier, and E. Peyrol, "A Self-Sovereign Identity Based on Zero-Knowledge Proof and Blockchain," *IEEE Access*, vol. 11, pp. 49 445–49 455, 2023, conference Name: IEEE Access. [Online]. Available: https://ieeexplore.ieee.org/document/10105959

[11] C. Reitwiessner, "zkSNARKs in a nutshell," Dec. 2016. [Online]. Available: https://blog.ethereum.org/2016/12/05/zksnarks-in-a-nutshell

[12] B. Bünz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, and G. Maxwell, "Bulletproofs: Short Proofs for Confidential Transactions and More," 2017, publication info: Published elsewhere. Minor revision. 39th IEEE Symposium on Security and Privacy 2018. [Online]. Available: https://eprint.iacr.org/2017/1066

[13] E. Ben-Sasson, I. Bentov, Y. Horesh, and M. Riabzev, "Scalable, transparent, and post-quantum secure computational integrity," 2018, publication info: Preprint. MINOR revision. [Online]. Available: https://eprint.iacr.org/2018/046

[14] "SelfKey Foundation Whitepaper." [Online]. Available: https://selfkey.org/whitepaper/

[15] O. Delgado-Mohatar, J. Fierrez, R. Tolosana, and R. Vera-Rodriguez, "Blockchain and Biometrics: A First Look into Opportunities and Challenges," in *Blockchain and Applications*, ser. Advances in Intelligent Systems and Computing, J. Prieto, A. K. Das, S. Ferretti, A. Pinto, and J. M. Corchado, Eds. Cham: Springer International Publishing, 2020, pp. 169–177.

[16] E. Gent, "A Cryptocurrency for the Masses or a Universal ID?: Worldcoin Aims to Scan all the World's Eyeballs," *IEEE Spectrum*, vol. 60, no. 1, pp. 42–57, Jan. 2023, conference Name: IEEE Spectrum. [Online]. Available: https://ieeexplore.ieee.org/document/10006664

[17] C. Burt, "No plans to revive World Economic Forum's user-controlled airport digital ID pilot | Biometric Update," Oct. 2022. [Online]. Available: https://www.biometricupdate.com/202210/no-plans-to-revive-world-economic-forums-user-controlled-airport-digital-id-pilot

[18] J. Baylina, "IDEN3: Scalable distributed identity infrastructure using zero-knowledge proofs to guarantee privacy," Oct. 2018. [Online]. Available: https://slideslive.com/38911825/iden3-scalable-distributed-identity-infrastructure-using-zeroknowledge-proofs-to-guarantee-privacy

[19] R. D. Labati, A. Genovese, E. Muñoz, V. Piuri, F. Scotti, and G. Sforza, "Biometric Recognition in Automated Border Control: A Survey," *ACM Computing Surveys*, vol. 49, no. 2, pp. 24:1–24:39, Jun. 2016. [Online]. Available: https://dl.acm.org/doi/10.1145/2933241