Security, Confidentiality, and Anonymity in Permissionless Blockchains with Smart Contracts

Robert Muth, supervised by Florian Tschorsch
Distributed Security Infrastructures, Technische Universität Berlin
{muth, florian.tschorsch}@tu-berlin.de

***Abstract*—Permissionless blockchains such as Ethereum allow anyone to actively participate and therefore to read, propose, and validate transactions. Since this requires transactions to be fully traceable, anonymity and confidentiality are severely limited, making blockchain-based applications, for example secret ballots, difficult to realize. With smart contracts, which can execute arbitrary Turing-complete code, it is possible to implement privacy-enhancing technologies, though. The PhD thesis investigates existing permissionless blockchains including their security and develops new design recommendations for anonymous and confidential applications with smart contracts.**

I. Motivation

While the concept of smart contracts is not new [1], and Bitcoin already implements a limited scripting language for transactions [2], the crypto-currency Ethereum has drawn some attention by implementing Turing-complete smart contracts [3]. With smart contracts it is possible to implement blockchain-based applications, even though they were not implemented natively. Moreover, they enable to eliminate the need for a trusted third-party (TTP) and therefore can lead to more autonomous decision making.

A prime example are voting systems, specifically secret ballots. Compared to a TTP that is responsible to maintain ballot secrecy and correctness, permissionless blockchains disclose all data publicly, but thereby increase transparency. The nature of blockchains and permissionless access allow to verify the correct code execution and therefore impede fraud. Hence, counting votes for a ballot could be secured by blockchains, due to the fully verifiable history which cannot be manipulated retrospectively. On the other hand, one does not want to disclose individual preferences. Therefore, the history must remain verifiable but should not reveal any personal preferences—only the final results. Ballot secrecy therefore has to protect voters' right to vote freely without any external coercion possible. A similar situation applies to other blockchain applications, including anonymous bulletin boards, chats or pin boards, where it might be important to hide sender identities but share messages publicly.

Encryption can hide data from the public, e. g., individual votes, but at the same time hinders processing them—for instance, counting votes might be impossible without decrypting them first. Homomorphic encryption schemes might solve this problem as they allow to perform arithmetic operations like addition, multiplication, or both, *on encrypted data*. Accordingly, homomorphically encrypted votes can be saved in a blockchain and tallied, while only the final results need to be decrypted.

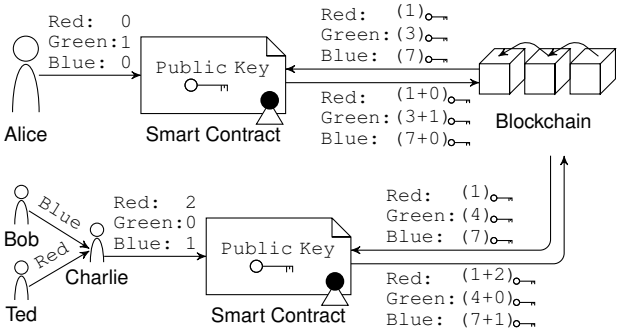

Fig. 1. Exemplary anonymous voting scenario with blockchain and smart contracts using homomorphic encryption.

II. Research Challenges

For this PhD project multiple use cases requiring anonymity will be evaluated. Our primary use case is secret ballot with saving individual votes in a blockchain. Figure 1 shows an exemplary voting for a color (red, green or blue) with using blockchain, smart contracts, and homomorphic encryption. The votes will be saved publicly in the blockchain, but they are protected with encryption. The smart contract contains the public key for encryption and its needed algorithms. In the example, Alice votes for green and submits the corresponding tuple (red: 0, green: 1, blue: 0) to the smart contract, which itself is stored in the blockchain. The votes will be protected locally with asymmetric homomorphic encryption, before they will be added to already submitted votes. The homomorphic encryption allows to add a single vote to already encrypted votes (red: 1, green: 3, blue: 7), so no one without the corresponding private key can read the votes in cleartext. At the end, the elections' initiator can reveal the final results and no-one but them can see single votes, even with public access to the blockchains' data. But the voters' secrecy directly depends on the trust to the private key owner, who actually could decrypt single votes due to the blockchains' inherent change history. Another approach shows multiple voters Bob, Ted, and Charlie combining their votes before submitting them to the smart contract and the blockchain. The smart contract could help to group voters and to enforce k-anonymity for example. As a consequence, the private key owner cannot figure out individual votes anymore.

Unfortunately, many problems are still unsolved or restrain practical applications. For instance, homomorphic encryption

is still not as powerful or fast as probably needed. It also may need a source of secure randomness, so the same cleartext encrypted consecutively is different: $\texttt{homom\_encrypt}(x) \neq \texttt{homom\_encrypt}(x), x \in \mathbb{Z}$. Also, the whole process must remain secure against conventional computer-security attacks, like Sybil attacks or malicious voters manipulating their votes. Especially because the smart contract's source code is publicly accessible and cannot be protected against brute-force attacks, its security evaluation is very challenging.

III. State of the Art

Anonymity is a relatively new field of information security, compared to confidentiality [4]. Many new and already well established privacy-enhancing technologies (PET) like Zero-knowledge proofs [5], homomorphic encryption [6], probabilistic data sketches [7], Differential Privacy [8] or k-anonymity [9] offer yet unevaluated potential for anonymity with smart contracts. The Agora voting system [10] for example uses a custom blockchain with zero-knowledge proofs and its own Mix-network for anonymization of voters. The authors however also point out the potential of other encryption methods in their whitepaper. Moreover, cryptocurrencies also adapted anonymity techniques, e. g., Monero (CryptoNote [11]), and Zerocash [12] using ring signatures and zero-knowledge proofs respectively in order to anonymize coin transactions. The main difference to our approach is the usage of PET *inside of smart contracts*, which is not natively implemented by the blockchain itself.

Compared to traditional voting schemes and end-to-end auditable voting systems, our approach does not necessarily require a declared TTP, or any physical receipts. Instead, the blockchain replaces the trusted party, while the transactions act as verifiably receipts. Blockchains are no universal solution, though. They exhibit issues like limited transaction throughput and long-term storage problems. Overall, these challenges will likely result in trade-offs between, among others, transaction capabilities, transparency and immutability, and trust in third-party authorities.

IV. Research Goals

In this PhD project, we are going to investigate various blockchain technologies and evaluate their feasibility to implement privacy-enhancing technologies. In particular, the anonymity and privacy-enhancing properties of homomorphic encryption will be evaluated. One of the main research goals will be to assess its applicability to blockchains and smart contracts.

To this end, we will start by implementing voting systems with different features, including secret ballot, hiding preliminary voting tendencies, deniability of votes, transferability of voting rights and voter registration (respectively identity disclosure). The aim of the study is to provide first-hand experience of homomorphic encryption as a method to realize security, confidentiality, and anonymity in permissionless blockchains. We also strive to gain experience using smart contracts in various other scenarios beyond voting.

The third-party funded research project B_B_Blockchain, which explores the potential of blockchain technologies in urban development, will serve as a real-world case study. Among others, we will develop a polling feature that allows citizens of Berlin to vote anonymously on aspects of an urban development project.

Other research challenges and directions include voter identification and geolocation-based voting permission.

References

[1] N. Szabo, *Smart contracts*, https://web.archive.org/web/20160323035617/http://szabo.best.vwh.net/smart.contracts.html, Accessed: 2019-01-04.

[2] N. Atzei, M. Bartoletti, T. Cimoli, S. Lande, and R. Zunino, "Sok: Unraveling bitcoin smart contracts," *IACR Cryptology ePrint Archive*, vol. 2018, p. 192, 2018.

[3] V. Buterin, *A next-generation smart contract and decentralized application platform*, http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf, Accessed: 2018-12-23.

[4] P. Syverson, "Why i'm not an entropist," in *Security Protocols Workshop*, ser. Lecture Notes in Computer Science, vol. 7028, Springer, 2009, pp. 231–239.

[5] J. Quisquater, M. Quisquater, M. Quisquater, M. Quisquater, L. C. Guillou, M. A. Guillou, G. Guillou, A. Guillou, G. Guillou, S. Guillou, and T. A. Berson, "How to explain zero-knowledge protocols to your children," in *CRYPTO*, ser. Lecture Notes in Computer Science, vol. 435, Springer, 1989, pp. 628–631.

[6] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*. Chapman and Hall/CRC Press, 2007.

[7] P. Flajolet and G. N. Martin, "Probabilistic counting algorithms for data base applications," *J. Comput. Syst. Sci.*, vol. 31, no. 2, pp. 182–209, 1985.

[8] C. Dwork, "Differential privacy," in *ICALP (2)*, ser. Lecture Notes in Computer Science, vol. 4052, Springer, 2006, pp. 1–12.

[9] L. Sweeney, "K-anonymity: A model for protecting privacy," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10, no. 5, pp. 557–570, 2002.

[10] *Agora Whitepaper 0.2*, https://www.agora.vote/s/Agora_Whitepaper.pdf, Accessed: 2019-01-04.

[11] N. van Saberhagen, *CryptoNote 2.0*, https://cryptonote.org/whitepaper.pdf, Accessed: 2019-01-04.

[12] E. Ben-Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from bitcoin," in *IEEE Symposium on Security and Privacy*, IEEE Computer Society, 2014, pp. 459–474.