[[1]](#footnote-1)

Implementing Blockchain Technology to Comply with GDPR Legislation, a Simple Solution

Andy Ho, An Nguyen and Jodi Pafford

*Abstract*— Blockchain is a highly attractive new technology, due to its security features, in a time where concern for consumer data protection is on the rise. The immutability of blockchain through its decentralized framework is an appealing option for conforming to regulations protecting consumer data privacy such as the European Union’s (EU) General Data Protection Regulation (GDPR) and similar legislation proposed in the United States (US), however companies needing to conform to regulations will likely need to keep costs as low as possible and solutions simple. Although many other proposals have introduced the idea of a blockchain-database hybrid or a mutable blockchain, this paper seeks to implement a third, more simple solution.

# INTRODUCTION

Blockchain technology has attracted interests from a wide span of industries; mainly due to its ability to operate in a decentralized fashion [1]. A blockchain utilizes a digital ledger of transactions where all participants edit in a secure way and is shared over a distributed network of computers [2]. The blockchain has an append-only structure, which helps it protect old data against modification or deletion [3]. In order to make changes, all the nodes present in the network must evaluate, verify, and match the transaction information; if the majority of the nodes agree a new block is added to the chain [2]. Considering several recent highly publicized data breaches raising public concern, and in the face of looming legislative changes in the United States [4, 5], after the implementation of the General Data Protection Regulation (GDPR) [6], this extra-secure framework is an attractive one.

Some possible challenges for companies trying to conform to GDPR-like legislation include the “Right to be forgotten” where citizens are given strict control over their personal data [7]. Conforming to a GDPR-like regulation and securing the data are two dynamically opposed paradigms that must be reconciled with each other.

One solution that has been presented includes implementing a blockchain-traditional database hybrid where user data is stored on a traditional database and modifications are recorded on the blockchain [8, 7]. Alternatively, another solution is a blockchain with the ability to forget has been proposed. This proposal uses the pruning features of traditional blockchains like Bitcoin or newer smart-contracts like Ethereum to remove blocks in a traceable way [3].

In this paper, we will give a brief overview of the blockchain and its background. We will give a condense summary of the European Union’s GDPR. Following this, we will discuss the different methods proposed and their weaknesses. The remainder of this paper will contain our proposal, its implementation and drawback.

# Related works

With the growing interest in blockchains as a information storage system and the growing concern for user data privacy research into designing a blockchain based system that are compliant with privacy laws such as the GDPR have begun. Here we identify two strategies proposed by researchers to answer the “right to be forgotten” clause of the GDPR. One proposal by Farshid et al. is to use a pruning algorithm on a smart contract based blockchain, such as Ethereum, and will be describe in the following section [3].

Smart contract based blockchains have the additional attribute of being able to execute code. All the nodes and blocks together makeup one instance of a virtual machine. This machine can store all account balances and active codes. Once deployed smart contracts only has write-access and cannot be updated or changed. Smart contract based blockchain is attractive because the virtual machine does not require a transaction history to operate but only the current state of the machine. The researchers made use of the pruning algorithm in two Ethereum implementations to delete as much state data as possible without breaking the functionality of the blockchain. Furthermore, the researchers deleted all historical blocks and logs leaving only the current state active. With these changes it was shown that a five host machines were able to form a network and perform basic transactions. They were able to show that an account can be changed and then the history of the exchange deleted. Contracts were able to be created and then the creation transaction be deleted. Figure 1 is a before and after screenshot of an account balance and creation of a smart contract with their transaction history deleted.

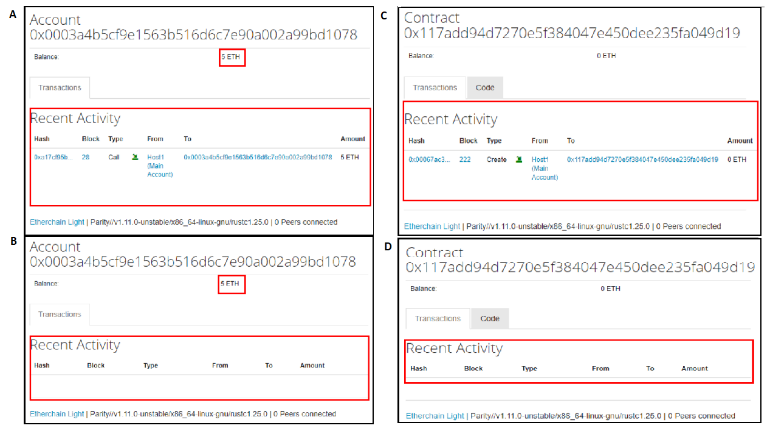


Figure . A and B, account with balance and deleted transactions. C and D, creation of contract and deleted transactions.

There are several limitations to this approach pointed out by the authors. One, no new nodes can be added to the network. This is because the information needed to derive the current state of the virtual machine no longer exist. Two, there is no way to prevent individuals from creating backups of old data before it gets deleted.

References

|  |  |
| --- | --- |
| [1] | K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access,* vol. 4, pp. 2292 - 2303, 2016. |
| [2] | S. Singh and N. Singh, "Blockchain: Future of Financial and Cyber Security," in *2016 2nd International Conference on Contemporary Computing and Informatics (IC3I)*, Noida, India, 2017. |
| [3] | S. Farshid, A. Reitz and P. Roßbach, "Design of a Forgetting Blockchain: A Possible Way to Accomplish GDPR Compatibility," *Hawaii International Conference on System Sciences |,* pp. 7087-7095, 2019. |
| [4] | National Conference of State Legislatures, "Data Disposal Laws," National Conference of State Legislatures, 04 January 2019. [Online]. Available: http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx. [Accessed 1 January 2019]. |
| [5] | National Conference of State Legislatures, "Security Breach Notification Laws," National Conference of State Legislatures, 29 September 2018. [Online]. Available: http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx. [Accessed 31 January 2019]. |
| [6] | THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, *REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR),* L 119 ed., 2016. |
| [7] | F. Coelho and G. Younes, "The GDPR-Blockchain Paradox: A Work Around," in *Workshop on GDPR Compliant Systems*, Rennes, France, 2018. |
| [8] | C. Molina-Jiménez, I. Sfyrakis, E. Solaiman, I. C. L. Ng, W. Meng, Wong, A. Chun and J. Crowcroft, "Implementation of Smart Contracts Using Hybrid Architectures with On-and Off-Blockchain Components," *ResearchGate,* pp. 1-12, 2018. |

1. MSDS 7349 – Network and Data Security – Spring 2019 [↑](#footnote-ref-1)