Right to be Forgotten in Interoperating Permissioned Blockchains

One of the primary enablers for Web 3.0 is the ability of multiple blockchains to seamlessly interoperate in a fully decentralized manner [11]. Several advances have recently been made towards interoperability between public permissionless blockchains through atomic transfer of assets [13], and also among multiple instances of permissioned blockchains [5], essentially providing secure interoperability and resource sharing while retaining autonomy. Around the same time, as the second generation permissionless blockchains like Ethereum [1] and permissioned blockchain projects like Hyperledger [4] were developed (2014-2017), some of the data privacy regulations also came into effect in various parts of the world. Notable ones are: (1) the GDPR [2] for the European Union, which was adopted in 2016 and became enforceable in 2018, and (2) several federal and state-level privacy regulations in the USA including the California Consumer Privacy Act (CCPA) that came into effect in 2018 [3]. While the success and widespread adoption of blockchains is often attributed to the properties of immutability and verifiability of blockchain transactions, they are often in direct conflict with the data privacy requirements of most of the above-mentioned privacy regulations. In this project, we specifically consider an important privacy property required in both the GDPR and CCPA - the *Right to be Forgotten* (RTBF) [10]. Essentially, RTBF ensures a consumer has the right to have her personal data deleted from a repository with which it was previously shared. However, in a cross-organizational setting with interoperating blockchains, once a transaction has been executed to its completion on inter-operating blockchains, it is challenging to enforce RTBF. This is because, since an individual's data has already been shared (For example, a patient's allergy history in an emergency between hospitals in an interoperating permissioned blockchain scenario), if the data has to be redacted, it has to be removed from all the participating blockchains. Moreover, a proof for the same has to be made available to the concerned person. This RTBF problem will become increasingly pertinent in Web 3.0 where several blockchain networks are likely to interoperate for effective data exchange.

Even though there is a significant volume of work on RTBF for centralized data repositories, few have addressed the problem in the context of blockchains [15]. One such approach [7] handles this important privacy guarantee for a single healthcare blockchain. Bayle et al. [8], in contrast, records all the interactions between data providers and consumers using a blockchain without storing any sensitive data on-chain. A recent paper reviews the gap between use of blockchains and GDPR regulations [12], but it does not specifically suggest any method for enforcing RTBF for permissioned blockchains in an enterprise context. In contrast, Li et al. [14] consider the problem in permissionless blockchain setting and suggest a method for instant redaction for both proof of work and proof of stake based consensus mechanisms. Hence, all of the prior work addresses the RTBF problem within an individual blockchain, but has not considered it in the interoperating blockchain setting.

Proposal Description

This project will address the above problems of ensuring RTBF in an interoperable blockchain environment. An overview of the tasks are shown in Figure 1, where we assume that two hospitals A and B host their data on permissioned blockchains PB_A and PB_B, respectively, using individual security and privacy policies. Bob, whose health records are maintained in Hospital A and hence a user of PB_A, gets admitted to the ER of Hospital B. In such an emergency situation, PB_A shares allergy information of Bob with PB_B after getting consent from Bob/his representative. A consensus view of the data is moved from PB_A to PB_B during the treatment process through inter-blockchain transfer. After recovery, Bob wants his allergy data to be deleted from PB_B. Also, he should get a tamper-evident certificate that the deletion has indeed been done. This will honor Bob's Right to be Forgotten from Hospital B's repository. The identity of every user including Bob for inter-blockchain data transfer needs to be handled using an identity management service as shown in the figure. Note that, while we have shown the flow in two blockchain networks for the sake of brevity, the project will consider a multiple network scenario. The specific tasks are identified below as different Work Items (WIs):

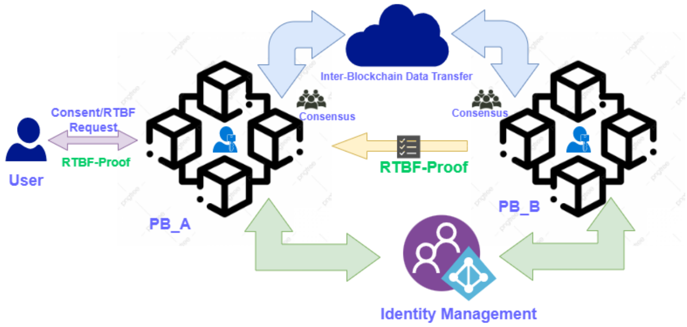

Figure 1: Supporting RTBF in Permissioned Blockchains

WI_1: *Develop Protocols and Formal Proofs for Enabling RTBF* We will first formalize the RTBF problem in the context of intra-enterprise as well as inter-enterprise permissioned blockchain environments. This includes identifying the repository hosting private data that needs to be redacted (whether the blockchain ledger itself stores the sensitive data or any other file system like IPFS that stores the data keeping the hashes on the ledger), attestation requirements, etc. After the problem is formally defined, we will develop algorithms for collective signing of the private data so that the target network can verify the validity of the information it receives. Alongside, protocols will be developed for inter-blockchain transfer of data committed using a consensus protocol in the source network to be included in the ledger of the target network through its consensus mechanism and data acceptance policies. To accomplish a user's request for the data to be forgotten, we will first develop protocols for propagating such requests to the destination network and develop algorithms for redacting the data from the repository. This will depend on the design of the schema for data storage as mentioned above. Once the data is redacted in the target blockchain network, its proof representing a consensus view of the deletion will have to be sent back to the user in the source network. The structure and method for such proof will have to be designed from scratch since there is no existing work yet in the literature. Techniques such as zero knowledge proofs can ensure that the deletion certificate can be verified by a third party without divulging the data itself or the identity of the user. This additionally requires appropriate management and transfer of identities across multiple blockchain networks since the user sets may be different in each of the participating blockchains.

WI_2: *Security and Privacy Analysis of Protocols* Besides developing protocols for enforcing RTBF, it is equally important to establish their security and privacy guarantees under various threat models. This includes presence of ill-formed smart contracts that could leak information, as well as untrusted entities involved in the process of inter-blockchain data exchange. Once the threat models are identified, we will use formal methods for showing whether the desired property is achieved. For example, if a claim is made that the desired data has been redacted in a destination network, it must be guaranteed that such a claim is the consensus view of the network and not done by an individual node. Similarly, the redaction certificate will carry sufficient information to the user that the deletion indeed was done. At the same time, if this certificate is viewed by other users of the network, the private information should not get divulged to them. Efficient public key cryptography will be used to ensure the same. We plan to use formal methods like symbolic protocol verification similar to what was done by [9] in the Tamarin tool. The possibility of using AVISPA [6], which takes input in a High-Level Protocol Specification Language and supports several built-in model checking tools including a SAT based model checker, will also be explored. It is also imperative that the developed protocols be implementable in real blockchain networks running in enterprise settings. Hence, they should not adversely affect the latency and throughput of such networks.

WI_3: *Implementation on Enterprise Blockchain Networks* Finally, we plan to carry out extensive performance and scalability studies. Considering the current state-of-the-art in research on interoperability in enterprise blockchains, we will set up a test bed with multiple Hyperledger Fabric networks and Hyperledger Indy pool of identities. This will enable us to carry out extensive experiments with benchmarking tools like Hyperledger Caliper for quantitative evaluation of performance of the proposed method. Implementation of the algorithms and protocols developed as part of WI_1 will involve writing smart contracts and deploying them in several blockchain nodes either running on a high end server as individual processes or on a cloud platform running in separate VMs. Besides, we also envisage the need for making some changes in the Hyperledger Fabric source code itself for the requirements that cannot be handled only through smart contracts. The results of our experiments are expected to lead to further changes in the protocol for improving its efficiency, Overall, it will be an iterative process till an optimum performance level is achieved.

All the developed code will be made publicly available through github repositories to support the open source initiative of various blockchain projects. The results of the work done in the project will be published in high impact conferences/journals.

References

[1] https://ethereum.org/en/.

[2] https://gdpr-info.eu/.

[3] https://oag.ca.gov/privacy/ccpa.

[4] https://www.hyperledger.org/.

[5] Ermyas Abebe, Dushyant Behl, Chander Govindarajan, Yining Hu, Dileban Karunamoorthy, Petr Novotny, Vinayaka Pandit, Venkatraman Ramakrishna, and Christian Vecchiola. Enabling enterprise blockchain interoperability with trusted data transfer (industry track). In *Proceedings of the 20th International Middleware Conference Industrial Track*, Middleware '19, page 29–35, New York, NY, USA, 2019. Association for Computing Machinery.

[6] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuellar, P. Hankes Drielsma, P. C. Heám, O. Kouchnarenko, J. Mantovani, S. Mödersheim, D. von Oheimb, M. Rusinowitch, J. Santiago, M. Turuani, L. Viganò, and L. Vigneron. The avispa tool for the automated validation of internet security protocols and applications. In Kousha Etessami and Sriram K. Rajamani, editors, *Computer Aided Verification*, pages 281–285, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg.

[7] Eugenio Balistri, Francesco Casellato, Carlo Giannelli, and Cesare Stefanelli. Blockhealth: Blockchain-based secure and peer-to-peer health information sharing with data protection and right to be forgotten. *ICT Express*, 7(3):308–315, 2021.

[8] Aurelie Bayle, Mirko Koscina, David Manset, and Octavio Perez-Kempner. When blockchain meets the right to be forgotten: Technology versus law in the healthcare industry. In *2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI)*, pages 788–792, 2018.

[9] Colin Boyd, Kristian Gjøsteen, and Shuang Wu. A Blockchain Model in Tamarin and Formal Analysis of Hash Time Lock Contract. In Bruno Bernardo and Diego Marmsoler, editors, *2nd Workshop on Formal Methods for Blockchains (FMBC 2020)*, volume 84 of *OpenAccess Series in Informatics (OASIcs)*, pages 5:1–5:13, Dagstuhl, Germany, 2020. Schloss Dagstuhl–Leibniz-Zentrum für Informatik.

[10] Aloni Cohen, Adam Smith, Marika Swanberg, and Prashant Nalini Vasudevan. Control, Confidentiality, and the Right to be Forgotten. arXiv, 2022.

[11] Amber Group. Decentralized identity: Passport to web3, 2022.

[12] Sejin Han and Sooyong Park. A gap between blockchain and general data protection regulation: A systematic review. *IEEE Access*, 10:103888–103905, 2022.

[13] Maurice Herlihy. Atomic cross-chain swaps. In *Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing*, PODC '18, page 245–254, New York, NY, USA, 2018. Association for Computing Machinery.

[14] Xin-Yu Li, Jing Xu, Ling-Yuan Yin, Yuan Lu, Qiang Tang, and Zhen-Feng Zhang. Escaping from consensus: Instantly redactable blockchain protocols in permissionless setting. *IEEE Transactions on Dependable and Secure Computing*, pages 1–20, 2022.

[15] Eugenia Politou, Fran Casino, Efthimios Alepis, and Constantinos Patsakis. Blockchain mutability: Challenges and proposed solutions. *IEEE Transactions on Emerging Topics in Computing*, 9(4):1972–1986, 2021.