Blockchain and the Right to Privacy: A Critical Analysis

A Thesis Prospectus
In STS 4600
Presented to
The Faculty of the
School of Engineering and Applied Science
University of Virginia
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Science

By
Lucas Banerji

May 9, 2022

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

ADVISORS

S. Travis Elliott, Department of Engineering and Society

Introduction

Blockchain has been a volatile topic. For a period, many felt like it was going to be the solution to every business and technology problem, and almost as quickly, it felt that plans around the technology had quieted. Even so, big tech companies such as Amazon, Samsung, IBM, and Microsoft have all launched competitive blockchain services. This is because Blockchain has tremendous potential, but there are still many questions standing in the way of its adoption on a mass scale. One fascinating area where blockchains may have significant implications is in the field of personal and data privacy. Technologists believe that blockchain could someday replace things like usernames and passwords by providing the general populace encrypted digital identities that we can use to manage everything from online information to our personal medical records. Blockchain could track and store all the data personal to us, and because of its immutable nature, that information will remain safe and secure.

So, could personal privacy protection with blockchain be the thing to push the tech into the mainstream? In this paper, I will explore the implications of blockchain technology on privacy and some potential applications. Using the Social Construction of Technology framework, this paper will also aim to explain how different discourses are creating new meanings about this technology, focusing on the issue of privacy and data protection.

Background

Blockchain is the secure ledger behind Bitcoin, the legendary cryptocurrency. Despite its association with bitcoin, it turns out blockchain has a plethora of uses beyond the secure management of a digital currency. Because of the way blockchain works—creating an immutable ledger of information—it makes user fraud incredibly difficult. That means it can be

used to prove the authenticity of pretty much anything it tracks, and it can bridge the "trust gap" in any business exchange. There are many different properties that blockchain technology provides to any area where it is desired to apply, ranging from service availability to the persistence of validated information in the system. In the aspect of security, the blockchain technology has very specific characteristics: immutability, transparency, auditability, privacy, and anonymity, among others.

It is also important to recognize that there are two types of blockchains: public and private. A public blockchain is permissionless. Anyone can join the network and read, write, or participate within the blockchain. It is decentralized and does not have a single entity which controls the network. Data on a public blockchain are secure as it is not possible to modify or alter data once they have been validated on the blockchain. A private blockchain is a permissioned blockchain. They work based on access controls which restrict the people who can participate in the network. There are one or more entities which control the network, and this leads to reliance on third parties to transact. In a private blockchain, only the entities participating in a transaction will have knowledge about it, whereas the others will not be able to access it.

With blockchain applications "users are not required to trust any third-party and are always aware of the data that is being collected about them and how it is used" (Zyskind et al, 2015, p.184). In addition, the blockchain recognizes the users as the owners of their personal data. "The rise of self-sovereign identities (SSIs) based on blockchain technologies provides individuals with ownership and control over their personal data and allows them to share their data with others using a sort of digital safe" (Benchaya et al, 2022, p.402). Companies, in turn,

can focus on utilizing data without being concerned about properly securing and compartmentalizing them. These developments change the relationship between government, companies, and individuals. Some technologists claim that blockchain and cryptocurrencies can realign capitalism thanks to blockchain's alternative trust-based, peer-to-peer systems. With its tracked, audited, and publicly communicated information, blockchain may be able to rebuild the bridges between centralized systems and the people they serve.

SCOT

The development and adoption of blockchain, like most technologies, has important rhetorical and social elements that will shape its meaning and use. The Social Construction of Technology (SCOT) framework provides a valuable lens through which to examine the various discourses that shape the development and understanding of blockchain technologies. SCOT posits that technologies do not exist in a vacuum but are rather socially constructed by different stakeholder groups who interpret and ascribe meaning to them based on their specific interests, needs, and agendas. In the case of blockchain technologies, key stakeholders such as developers, government regulators, businesses, and end-users engage in ongoing debates about the technology's potential to address privacy and data protection concerns.

Developers and technologists often emphasize the potential of blockchain technologies to enable greater privacy and data protection through decentralization, encryption, and immutability. By eliminating the need for central intermediaries, transactions and data storage become more secure and resistant to tampering, while cryptographic techniques ensure that information remains private. This discourse, driven by the technological community, posits

blockchain technologies as a solution to many of the privacy and data protection issues associated with traditional centralized systems. On the other hand, government regulators and law enforcement agencies raise concerns about the potential misuse of blockchain technologies for illicit activities, such as money laundering, tax evasion, and the financing of terrorism. They argue that the same features that enhance privacy and data protection can also be exploited by bad actors, necessitating regulatory measures that might undermine some of the technology's privacy-enhancing characteristics. Meanwhile, businesses and organizations are faced with the challenge of navigating the complex landscape of privacy and data protection regulations while leveraging the benefits of blockchain technologies. This group's discourse often focuses on finding the optimal balance between privacy, security, and regulatory compliance, fostering innovation in the development of privacy-preserving technologies, such as zero-knowledge proofs and confidential transactions. Lastly, end-users, whose needs and preferences are often overlooked in the debates surrounding technology, have their own interpretations of blockchain technologies in relation to privacy and data protection. While some users view the technology to regain control over their personal information, others may be wary of its potential implications for surveillance and control by governments and other powerful entities.

The Social Construction of Technology framework demonstrates that the meanings and understandings of blockchain technologies, particularly in relation to privacy and data protection, are shaped by the complex interplay of various stakeholder discourses. As these discourses continue to evolve, so too will the social construction of blockchain technologies, reflecting the dynamic nature of technological development and its impact on society.

Analysis on Application Domains

There exist fields where blockchain technology is being implemented to respond to situational changes and new challenges arising from the continuous advancement as well as new needs regarding privacy and information security. Among these fields of work, the following stand out:

- Health field: Where new challenges, security and privacy requirements must be addressed for successful large-scale data exchange. Health information needs to have adequate privacy. When blockchain is used to store health data, a public key is associated with the individual's identity to protect his or her true identity through a pseudonym (Gordon et al, 2018, p.4). There is a risk of re-identification through public data in the blockchain which would allow the true identity of the individual to be known, which is a serious problem. In addition, there is the possibility that different records may be accessible to different health professionals, which is difficult to achieve through a blockchain and would need to be implemented.
- IoT: The blockchain technology has revolutionized the IoT with its efficiency and scalability. "It tries to give a solution to the way in which the different devices that are related create an environment of reliability and security as well as the transfer of information between devices in a reliable way; however, there are unresolved limitations to improving the scalability of IoT devices; this is being approached from a new perspective of distributed ledger under the IOTA project (Rathore et al, 2020, p.21)". The work in Banerjee et al highlights the need to develop a standard for sharing IoT data sets in order to take advantage of the "blockchain potential to facilitate the safe exchange of data as well as to secure the IoT system itself (2018, p.2)". One of the most important problems to be solved would be device impersonation, false authentication or unreliability that could occur in the data exchange.
- Big Data. The approach taken in this area with respect to the use of blockchain technology is to increase the level of confidentiality, especially of the information being shared. "The fact of storing large amounts of information and combining this with blockchain technology presents the disadvantage of the capacity that can support each transaction, so storage off-chain appears as a solution", which in turn raises issues such as security and data privacy (Reyna et al, 2018, p.4).
- Ad hoc vehicular network: In the case of Liu and Lu in *A Privacy-Preserving Trust Model Based on Blockchain for VANETs* (2018) , where vehicles are used as nodes in a network, the focus is on trust and privacy, as they remain open issues, and it is crucial to prevent vehicles from sending false messages while preserving privacy from the different types of possible attacks. The work in Xu et al's *A Remote Attestation Security Model Based on Privacy-Preserving Blockchain for V2X* (2018) has researchers focus attention on the communication between vehicles and devices of the environment, of the smart city, is the Internet of the Vehicles (IoV). Communications should be anonymous to preserve the privacy of the vehicles but, on the other hand, this anonymity is needed to ensure that the authorities are able to obtain information from them in the event of a dispute. To achieve this, a blockchain-based anonymous reputation system (BARS) is

> proposed in which a certification authority (CA), law enforcement authority (LEA), roadside unit (RSU) as well as the vehicles are defined as model components. In this model, CA and LEA are responsible for initializing the system, updating certificates, and revoking public keys. In this case the public keys act as a pseudonym to preserve the identity of the vehicles.

Depending on the implementation of blockchain, some privacy issues may arise, making it possible to trace the transactions of a given entity. A case that stands out occurs in Gordon and Catalini's work in *Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability.* When the public key of an entity coincides with its identity in the blockchain system, which would make it possible to know all the transactions associated with that public key. This case would be catastrophic in the public blockchain type and could also be a problem in the private blockchain, as it may be necessary for not all members to have access to the transaction data. In this situation, the work in the paper refers to certain blockchain implementations that allow selective disclosure of private information and based on zero-knowledge cryptography to provide verification. How to deal with the right to forget a patient's data, as required by the GDPR, is one of the disadvantages shown when implementing blockchain in the health field. Among the disadvantages of using blockchain technology are the cost of verifying associated data, the cost of auditing different entities and transactions, and the cost of interoperability given to the network of participants. "The pseudonym does not guarantee the privacy of transactions and it would even be possible to de-anonymize a user's identity by analyzing the incoming and outgoing transactions" (Gordon et al, 2018, p.5). Another issue would be that "malicious participants could participate on equal terms within the blockchain, which would jeopardize the correct identification of the IoT devices, which is the main requirement in most cases of use of these systems (Hammi, 2018, p.1)". In this same field of IoT, the high heterogeneity of the IoT devices and the reliability of the data they offer should be

highlighted, making it possible for corrupt or low quality data to appear which would lead to errors in the devices, whether they are sensors or actuators.

Regarding the storage of information and big data, the problem of permanently storing transactions from all of a user's devices in the public blockchain is highlighted as it could compromise the user's privacy in the following ways. "Linking multiple transactions generated by the same user makes possible de-anonymization possible (Dorri et al, 2017, p.8)". Monitoring the frequency with which a user stores transactions, even when encrypted, reveals sensitive information about the interactions. Miners could obtain the private information of the node, which could be a violation of privacy.

Conclusion

Blockchain allows the implementation of anonymization of the transactions involved, but also exposes certain risks of traceability that could expose the real identity of the members of the blockchain involved in the transaction. This aspect differentiates between public, private and licensed blockchains, the former being the most exposed to de-anonymization. Some inconveniences have appeared that could endanger the privacy and anonymity of the entities participating in the blockchain and even of the information involved in a given transaction. Given the possibility of tracing the transactions of a given entity, possible selective disclosure of private information or even de-anonymization can occur. Other aspects to be highlighted as inconvenient would be the high computational and interoperational costs. In the case of IoT the high heterogeneity between devices participating in a blockchain increases the risk of lack of confidence in the information at stake.

It is clear that there is a need to move towards global legislation on privacy and anonymity. With regard to data with greater confidentiality, such as health data, more secure mechanisms must be provided to guarantee privacy and anonymity in the face of possible security risks or attacks. Difficulties have been encountered in adapting blockchain to GDPR because of the intrinsic characteristics of blockchain would make it impossible, for example, the right to be forgotten. Finally, new proposals for fields of application for blockchain technology and future implementations that improve the characteristics that this technology currently presents should be advanced.

References

Banerjee M., Lee J., Raymond Choo K. *A blockchain future for internet of things security: A position paper*. Digit. Commun. Netw. 2018;4:149–160. doi: 10.1016/j.dcan.2017.10.006.

Benchaya Gans, R., Ubacht, J., & Janssen, M. (2022). *Governance and societal impact of blockchain-based self-sovereign identities*. *Policy and Society, 41(3),* 402-413. https://doi.org/10.1093/polsoc/puac018

Dorri A., Kanhere S., Jurdak R. MOF-BC: *A memory optimized and flexible blockchain for large scale networks*. Future Gener. Comput. Syst. 2017;92:357–373. doi: 10.1016/j.future.2018.10.002.

Gordon W.J., Catalini C. *Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability*. Comput. Struct. Biotechnol. J. 2018;16:224–230. doi: 10.1016/j.csbj.2018.06.003.

Hammi M.T., Hammi B., Bellot P., Serhrouchni A. *Bubbles of Trust: A decentralized blockchain-based authentication system for IoT*. Comput. Secur. 2018;78:126–142. doi: 10.1016/j.cose.2018.06.004.

Lu Z., Liu W., Wang Q., Qu G., Liu Z. *A Privacy-Preserving Trust Model Based on Blockchain for VANETs*. IEEE Access. 2018;6:45655–45664. doi: 10.1109/ACCESS.2018.2864189.

Rathore H., Mohamed A., Guizani M. *A Survey of Blockchain Enabled Cyber-Physical Systems*. Sensors. 2020;20:282. doi: 10.3390/s20010282.

Reyna A., Martín C., Chen J., Soler E., Díaz M. *On blockchain and its integration with IoT. Challenges and opportunities*. Future Gener. Comput. Syst. 2018;88:173–190. doi: 10.1016/j.future.2018.05.046.

Xu C., Liu H., Li P., Wang P. *A Remote Attestation Security Model Based on Privacy-Preserving Blockchain for V2X*. IEEE Access. 2018;6:67809–67818. doi: 10.1109/ACCESS.2018.2878995.

Zyskind, G., Nathan, O., & Pentland, A. “Sandy.” (2015). Decentralizing privacy: Using blockchain to protect personal data. 2015 IEEE Security and Privacy Workshops, 180–184. https://doi.org/10.1109/SPW.2015.27