The Study of Integrating Policy and Law into the Blockchain Technology

Anwaar Ali

Abstract

Blockchain implements trust in a distributed and peer-to-peer financial transaction networks without the interference of a third party. Transaction records are stored in chain of blocks or a ledger. Every peer in such a network has a copy of this chain that gives the ledger the characteristic of being *distributed*. Each such copy gets updated at the same time with no provision of retroactive mutations in records. Blockchain or distributed ledger based systems have the potential for many applications. Specifically, governments can make of use of this technology for various purposes such as: voting systems, citizens' id record system, and fraud detection system etc. The distributed nature of blockchain-based systems are inherently democratic which also lessens the chance of forceful censorship by entities such as governments.

I. Motivation

A. Third party interference vs personalized services

In this data rich age where one signs up for many software applications and makes an agreement with third party service providers to allow the use of one's data for personalized services. These services can take the form of personalized recommendations e.g., on websites like Amazon and IMDb. There is also a concern of third parties using or selling a user's data for selfish, wrongful or for spying purposes. This raises the issue of user privacy in such data powered soft-systems.

A recent digital economy bill in the UK is a topic of the debate these days [1]. The debate is over the data gathering from multiple sources to track a select group of people (e.g., immigrants using the UK's National Health Service (NHS)). The question is whether the owners of this data know of this snooping? Is it even legal for the UK (or any other country in a similar way) to do so?

Another case that can be considered for the motivation is a simple sign up process on many web and mobile applications. If a user, along the way, does not feel comfortable with the type of personal information sharing she agreed on while sign up the only choice that remains with her is to re-sign up. There should be a system that allows users to control and own their data all the time yet at the same time giving third parties a set of permissions to use their data. This set should be modifiable on the go with the extreme case of this set being empty, i.e., a user can revoke a service/application's right to access her data at anytime she wants [2].

Blockchain or distributed *public* ledger technology is a peer-to-peer networked system in which transactions can be made in a secure manner without the need for a third party (who might or might not be trustworthy). Cyptocurrency networks like Bitcoin [3] make use of this technology to make their transactional process fair and trustful in a purely decentralized manner. However, this technology can be used for many other applications as well where the underlying resource does not necessarily has to be a currency.

Realizing the importance of the distributed ledger technology to make systems/processes fair, transparent and democratic (because of the decentralized nature and the consensus among the nodes of the network) the UK Government's Chief Scientific Adviser published a report [4] highlighting the important of the technology, different use cases and many potential application areas where this technology can be used to deploy fair and transparent government processes e.g., voting, tax collection, land registries.

Challenge: One important challenge to consider here is the *public* nature of the distributed ledger technology. It is true that this technology provides trustful transactional accuracy but every transaction made in such a system is always public. If one wants to implement privacy coupled with customized applications, in which third parties can use a user's data in a secure but private manner, then the blockchian technology has to be coupled with other techniques. Among these techniques can be off-blockchain storage solutions [2]and smart contracts [2]. I will discuss these two in a bit more detail in the next section.

The conclusion of this section is: there is no denying the importance and luxury of personalized services, however, the data that power these services (either private or governmental) should be owned and controlled at all times by its rightful owner(s). There should always be *second chances* for the owners of the data to either modify or completely revoke the permissions related to their data. These permissions can be modified/revoked in a per-service manner or in a collective way (same action that affects permission level of all the services at the same time). Deploying blockchain related solutions keep the third party service providers out of the loop of data ownership so that there is no need to do any legislative work or draft long sign up agreements that a user may or may not read.

II. Ways to Integrate Law/Policy in the Blockchain Technology

As described in the previous section that the blockchain technology has the potential to make a process fair in decentralized manner. There is still a need, however, to overlay this technology with other techniques that can be used to deploy custom applications with the assurances of e.g., privacy. I will discuss two such overlay solutions here: i) off-blockchain storage solution ii) smart contracts.

A. Off-blockchain Storage Solution

Since the nature of the traditional blockchain-based systems is public a user's data can not be stored as transactional data on it. However, as the approach taken in [2], blockchain can instead be used as an *access control manager*. This will still keep the third party service providers out of the loop and the data storage and retrieval tasks will be performed as transactions on the blockchain. These transactions can then be routed to an external storage such as a distributed hashtable (DHT) based key-value data store. Another type of transaction that can be made on this blockchain is access control transaction by the owner of data. In this transaction a user gets to modify the permissions on her data for a particular service.

The way this system works is it creates what is called a *compound identity* by coupling a user (data owner who gets to be the owner of this compound identity as well) and a service(s) (the guests in this compound identity). Then a *policy* is set between a user and each of the services. This policy is a set of permissions related to a particular type of user data e.g., it can be $\{location, contact\}$. Any data access transaction made by a service on blockchain will be wrapped inside this policy set. This paper has discussed the case of one user-one service case. What I see is that it can be extended to one user-multiple services , and multiple users-one service cases as well. Also the way *policy* dependent transactional procedure on blockchain is implemented can be considered to program our custom policy procedures. This hints towards an interface that can be designed as per the local laws. Another one of the extensions that the paper [2] itself mentions is that when a service makes a data access transaction on a blockchain then instead of providing atomic data (i.e., just location or contact information as an example) a result based on data analysis of different streams of data collected from a user can be provided as an answer. Also (I think it might be interested in the particular Microsoft's cloud perspective)a cloud service can also be used as an off-blockchain solution. But, this would require certain amount of trust on the third party (this problem can be made part of my doctoral investigations).

B. Smart Contracts

Smart contract are used on top of blockchains so that different parties can do business with each other without the need to trust one another. One important thing to note here is that blockchains are only used in this perspective to provide correctness and availability of transactions. Privacy, the particular terms and conditions of a contract and contractual security still need to be programmed on top of a blockchain. One of the papers that I base my discussion in this subsection is Hawk [5]. Hawk is a platform that can be used to write contracts in a high level language in an intuitive way. The Hawk compiler then implements this contract in a cryptographical manner on top of a blockchain. Two types of security guarantees are provided in Hawk i) on-chain privacy and ii) contractual security.

i) On-chain privacy: Hawk cryptographically hides the transactional data of the parties involved in a contract onto a blockchain. This is done so that only the parties involved in the contract are aware of the actual data of their transaction and yet at the same time the underlying blockchain is being used to ensure the correctness of the transactions. This way if a party wants to abort it may have to pay for it.

ii) Contractual security: This guarantee implements fairness and protects the interacting parties from each other (in contrast to the outside world like discussed in the previous paragraph).

In general the schematic in Fig. 1 can be consulted to see how we can integrate laws policies with blockchains. I would like to adopt a more generic approach during my PhD. I would like to work on such an interface that can be programmed as per a specific context that can take any form.

III. Potential Application Areas for the Use of Blockchains/Distributed Ledgers

The blockchain and distributed ledger technology has the potential to find applications other than their traditional use in the peer-to-peer crypto-currency networks like Bitcoin [3]. This report outlines many potential application use cases [4] like e.g., creating fairness, transparency and trust in various government processes like voting, citizen record keeping etc. In my doctoral thesis I would like to take a more generic approach like the approach of Universal Composability (UC) taken while designing the cryptographic model on blockchains by the Hawk platform [5]. Specially, I would like to work on an interface, as shown in Fig. 1, that can contain policy/contract details. This will be coupled by the customized transaction from the owners of the data to set certain permission on their data. The third parties will then be able to get the data that will comply with both the policies and the user permissions.

In order to sustain and make new collaborations during my PhD pursuit my interest will lie in particular in the following two aspects (potential projects) as my potential use cases.

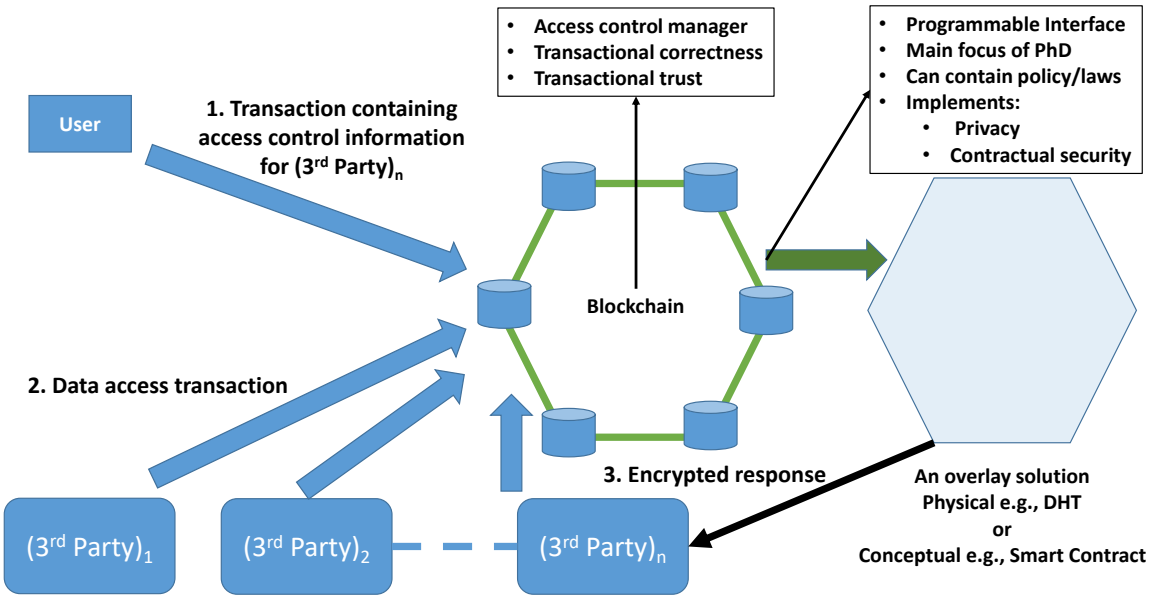

Fig. 1: Adapting Blockchain to Intergrate Custom Policy/Laws

A. AIMO: Internet Measurement Data Collection

The African Internet Measurement Observatory (AIMO) can be a potential beneficiary of my doctoral research. Using the techniques I develop/study an efficient Internet data collection mechanism can be deployed that will be in compliance with the local laws and policies (these might simply be plugged in the programmable interface shown in Fig. 1). In addition to that the blockchain with access control transactions made by the the users let them own and control their data will ensure that users always own their data and know how it is being used, by whom and for what purpose.

B. 5G: Cognitive Radio Perspective

Opportunistic spectrum access and automatic pricing while doing so can be implemented using smart-contract-based approach. In this perspective the spectrum itself can take the role of underlying resource while the secondary users can be treated as the third parties interested in this resource owned by a primary user. The transactions will involve leasing the spectrum to secondary users (while all the other secondary users are aware of it) in exchange for money to the primary user (automatic billing) that can be automated using a smart contract based approach.

IV. Knowledge Base Required

A good knowledge base in probability and statistics is required. I have studied this course in both my undergraduate and graduate degrees and I am supervising Computer Systems Modeling (taught by Ian Leslie) this term that involves studying computer systems in terms of stochastic processes and queuing theory. This background could be quite helpful during my doctoral investigations.

The other aspect is of cryptography. Though, I have not taken any course formally on this topic but I know some basic concepts like hashing, public key encryption etc. I believe with some effort I can also cover up for this during my PhD.

Also, for something hands on, this basic open-source implementation of blockchain[1] (which is also very good to get the basic and visual idea of how blockchains/distributed ledger systems work) and ethereum [6] (that provides programmability on blockchain-based system to deploy our own smart contract-based applications)[2].

V. First Year's Tentative Plan

First Quarter: Enhance the literature review. This quarter will be dedicated to reviewing the related literature along with highlighting the main techniques (mathematical and simulation) that could be use to help in my doctoral investigation of my topic. The topic itself will be decided in an iterative way, in consultation with you (my supervisor), ideally in the third quarter of my first year.

[1]https://anders.com/blockchain/
[2]https://www.ethereum.org/

Second Quarter: In this period I will try to develop some analytical models, based on the knowledge base I build in the last quarter, to help understand and shape my doctoral problem in a better way. In this quarter I will also try to experiment with different simulation and software tools as well to decide what my proof-of-concept system would be like at the end of my doctoral studies.

Third Quarter: Third quarter will be dedicated to the lessons learnt from the hands-on nature of its predecessor. I will try to outline the lessons learnt and any modification, again with your consultation, that can be made in our original premise for my doctoral investigation.

Final Quarter: I will dedicate this time slot solely to write my first year's report that might ultimately qualify me to further continue my doctoral research.

VI. Summary and Concluding Remarks

In summary, blockchains have the potential to integrate policies and laws on top of them. In a stand alone manner, however, blockchains can guarantee transactional correctness and trust but privacy and particular contractual terms and policies have to be programmed on top of them. There is already an interest among the research community and the UK government itself to work on this aspect. What I see right now is to build/investigate an interface to a physical or conceptual system that can be overlaid on a blockchain that can guarantee privacy and contractual fairness and programmability.

References

[1] "The guardian view on the digital economy bill: a last chance to get it right, accessed 08-february-2017." [Online]. Available: https://www.theguardian.com/commentisfree/2017/feb/05/the-guardian-view-on-the-digital-economy-bill-a-last-chance-to-get-it-right

[2] G. Zyskind, O. Nathan *et al.*, "Decentralizing privacy: Using blockchain to protect personal data," in *Security and Privacy Workshops (SPW), 2015 IEEE*. IEEE, 2015, pp. 180–184.

[3] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[4] M. Walport, "Distributed ledger technology: Beyond blockchain," *UK Government Office for Science*, 2016.

[5] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *Security and Privacy (SP), 2016 IEEE Symposium on*. IEEE, 2016, pp. 839–858.

[6] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, 2014.