Preamble to my second year report

Anwaar Ali

Abstract

The text contained within this document is fairly informal and intended to be expanded and elaborated later as my formal second year report. Mainly, this document contains an attempt to form my doctoral hypothesis along with the use cases that I am considering to study in detail. I highlight the opportunities for analyses and what sort of results could be gathered that could ultimately be published. You might notice two main themes in this document related to the *extent* and *effectiveness* of policy integration with a blockchain system. The extent part caters to the legal side of things and the effectiveness deals purely with technical side of things and problems related to the Computer Science realm such as system scalability, running time, resource consumption, and adoption (you can have a look at two recent publications, which I refer to later, that I did with the Spanish team to get a sense of this). Finally, at the end, I also provide some critique of my work that could potentially help me to prepare for my second year's viva.

Keywords: Trustless system, Trusted audability, Self-contained, Self-governed decentralised system, Fair and automatic pricing

1. Hypothesis formation

I will begin with what I already have provided by the legacy blockchain concepts and build upon it to motivate my doctoral hypothesis. In summary the overarching theme is *trusted compliance by design with the provision for policy upgrades* motivated by the more popular *privacy by design* principle.

1.1. The main ingredients

- Trustless environment
- Auditability of records
- Decentralised automation (in the form of smart contracts)

1.2. Resource consumption in community networks

I was highly motivated to study this problem during my Spanish Internship. All the three ingredients mentioned above in 1.1 seem to fit quite well to automate a compensation system [1] for community networks (Guifi.net[1] to be specific). These networks require a trustless environment to begin with as different parties (or peers) who pool their resources usually do not know each other and in turn might not want to trust each other as well. In this use case the bandwidth (or radio) is the underlying resource instead of cryptocurrency tokens and transactions are made against this resource. Parties usually report their resource consumption and put forward a claim for compensation. Trusted record keeping of resource consumption and claims put for it is imperative for a fair sustainability of such a system. So far I have managed to publish a paper [2] with the Spanish team which was mainly about deploying blockchain in their existing community network. I intend to reproduce and expand on the sort of analysis performed in this paper for my own research as well. An extension to this paper is currently under review [3]. It is still an on going work. The main part is actually coming up with a good economic sustainability model to make this project adaptable for the community and then implementing it in the form of a set of smart contracts with necessary auxiliary items (such as Oracles as explained later, plus I hinted towards the need for this auxiliary item in my first year report as well Pg. 29 Fig. 3.1 [2]). We began with a toy project[3] which mimics the kickstart project[4] and provides a good substrate to expand on it. Furhter, Jon suggested this paper [4], it is still in the queue to be dissected and get motivation from.

Luckily enough the work so far on community networks seems to fit quite well with what I proposed in my first year report. Please refer to Pg. 29, Fig. 3.1. During my Spanish internship one of the main challenges was to fetch outside data (network measurements to be precise) into the closed-walled universe of a blockchain application (in this case the compensation system automation-led automatic pricing). This is resolved by using Oracles[5].

In terms of system upgradeability of already deployed set of smart con-

[1] https://guifi.net/en/

[2] https://www.cl.cam.ac.uk/~aa980/papers/fyr_final_v1.pdf

[3] https://github.com/StephenGrider/EthereumCasts/tree/master/kickstart

[4] https://www.kickstarter.com/?ref=nav

[5] https://github.com/axic/tinyoracle

tracts, we are currently considering the concept of delegate call. See this footnote [6] for an implmenetation example and this footnote[7] for motivation. Delegate call method preserves the address credentials and the already maintained state of execution for a smart contract with the implementation of new logic at the same time. This is important so that a decentralised app (DApp) in production can handle the seemless calls to its already deployed set of smart contract with less down time if an update to the logic of the smart contracts is required. I had a brief chat this with Jat, a few suspicions were raised which just means I have something more to study and write about in my final thesis which is related to the suitability of using delegate calls to upgrade the logic of the, already deployed, underlying set of smart contracts. Also, delegate call is just one of the methods for the smart contarcts' upgradeability. The main thing is to have the provision of such an update in the first place to make the policy integration process iterative and more informed (please refer to Pg 29, Fig. 3.1 of my first year report).

In conclusion, this use case might just not be *the* killer app for blockchain but so far seems congenial enough that it might allow us to use all the ingredients in the favour of using a blockhain-based systems solution.

1.3. Trusted data provenance for trusted audit

With Oracles, as mentioned above, in place I presume I have the necesary plumbing work in place to integrate Thomas's CamFlow with a blockchain system. However, more work is needed to form transactions and a parallel system, just like the economic model above, to automate a trusted data audit and compliance check.

2. The legal side

The legal side will mainly deal with clarifying different concepts related to a policy set (such as GDPR) with my blockchain-based system. Such as the way Dave explains it in his article here[8] and the discussion in [5] from Section 6.4 onward for different use cases. As far as extent is concerned then the bone of contention is the right to be forgotten. I am almost done with a

[6] https://vomtom.at/address-call-vs-delegatecall-vs-libraries/

[7] `https://medium.com/quillhash/how-to-write-upgradable-smart-contracts-in-solidity-d8f1b95a0e9`

[8] https://thenextweb.com/syndication/2018/07/26/gdpr-blockchain-cryptocurrency/

survey paper I will be sharing with the team soon that, in one of its sections, tries to discuss this issue extensively.

3. Critique

I presume there will be a recurring theme of why use blockchain at all through out my PhD and I am still working on gathering plausible arguments to answer this question. I do not want to sell the blockchain-based system rather a self-contained, self-governed, trusted and auditable system that helps follow the compliance by design principle. Blockchain, as it seems, could help me take a first step towards this goal. The stepping stone could be a well researched compensation model to sustain a community network project.

3.1. Moving ahead

Immediate next step is to patch together different components that I have been working on (Oracles, delegate call, and the kickstart toy problem). Once done, I will be extensively considering a fair resource share/pricing model to implement in the form of smart contracts (some work has already been done and I will soon be sharing that in the form of my finalised Spanish internship report).

I am still very keen to explore the CamFlow's integration with a blockchain for trusted data audit and policy compliance check. I am quite hopeful that once I am done with the community network project it will not be very hard to do.

I am also planning to bring together, yet a bit siloed, London and Spanish teams. Hopefully after my second year's report I will be able to do just that.

Further, one of the more ambitious goals is to formally analyse the functionalities of Oracles and delegate call as well but at this point I am not sure how far I will be able to go with that.

[1] R. Baig, L. Dalmau, R. Roca, L. Navarro, F. Freitag, A. Sathiaseelan, Making community networks economically sustainable, the guifi. net experience, in: Proceedings of the 2016 workshop on Global Access to the Internet for All, ACM, pp. 31–36.

[2] M. Selimi, A. R. Kabbinale, A. Ali, L. Navarro, A. Sathiaseelan, Towards blockchain-enabled wireless mesh networks, arXiv preprint arXiv:1804.00561 (2018).

[3] A. R. Kabbinale, E. Dimogerontakis, M. Selimi, A. Ali, L. Navarro, A. Sathiaseelan, Blockchain for economically sustainable wireless mesh networks, arXiv preprint arXiv:1811.04078 (2018).

[4] J. An, D. Quercia, J. Crowcroft, Recommending investors for crowdfunding projects, in: Proceedings of the 23rd international conference on World wide web, ACM, pp. 261–270.

[5] J. Bacon, J. D. Michels, C. Millard, J. Singh, Blockchain demystified (2017).