Punishment not Reward: Disincentivising Blockchain Application Misbehaviour

DOI: 10.1109/BLOC.2019.8751232

Document Version
Accepted author manuscript

Link to publication record in Manchester Research Explorer

Citation for published version (APA):

Published in:
IEEE International Conference on Blockchain and Cryptocurrency

Citing this paper
Please note that where the full-text provided on Manchester Research Explorer is the Author Accepted Manuscript or Proof version this may differ from the final Published version. If citing, it is advised that you check and use the publisher's definitive version.

General rights
Copyright and moral rights for the publications made accessible in the Research Explorer are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

Takedown policy
If you believe that this document breaches copyright please refer to the University of Manchester’s Takedown Procedures [http://man.ac.uk/04Y6Bo] or contactuml.scholarlycommunications@manchester.ac.uk providing relevant details, so we can investigate your claim.

Download date: 23. Apr. 2020
Punishment not Reward: Disincentivising Blockchain Application Misbehaviour

Richard Banach
Department of Computer Science, University of Manchester, Manchester, M13 9PL, UK
richard.banach@manchester.ac.uk

Abstract—Blockchain architectures and applications emerged from the Bitcoin model, and are still most commonly associated with currency applications, and with financial speculation. This perception has driven the reward mechanisms for the various kinds of coin mining fueled consensus techniques seen in the vast majority of blockchain applications.

As an alternative to reward mechanisms via coin payment, we propose denial of service to the application in question and/or revocation of participant confidentiality as punishment mechanisms for enterprise mission critical blockchain applications, to be used as part of the incentive mix sustaining the application. This obviates or diminishes the need for reward via cryptocurrencies, along with all their attendant volatility, insecure ecosystem and market manipulation demerits.

We emphatically stress the importance of correctly balancing diverse application specific interests in the engineering of blockchain applications.

Index Terms—blockchain, cryptocurrency, ICO, reward, punishment, consensus, denial of service, revocation of confidentiality.

I. INTRODUCTION

The years 2016 and 2017 saw a boom in interest in cryptocurrencies and blockchains. The drive to speculation in Bitcoin specifically, caught the public imagination and caused a bubble in Bitcoin’s value in December 2017. The concept of blockchain underpinning Bitcoin, but with much wider potential application [14], [19], got caught up in this. Consequently, blockchain and distributed ledger technology (DLT) more generally, are conflated with cryptocurrency mechanisms, to the detriment of the understanding of the former (see, for example, the definition in [12]).

Cryptocurrencies are prone to a host of problems which we touch on in the briefest way in Section II. The incisive title of this paper is intended to highlight the opportunities for taking advantage of blockchain/DLT without the involvement of cryptocurrencies provided the incentives are aligned correctly. This possibility has tended to be mentioned rather sotto voce to date. The emphasis on incentive alignment is, for us, crucial. In Section III we outline the essential elements of our scheme for leveraging disincentives such as denial of service and/or revocation of confidentiality to maintain good behaviour in the blockchain, rather than incentives such as a cryptocurrency, which offers the temptation to steal it. We propose enterprise blockchain applications as prime candidates for our approach, and suggest that the startup phase is conceptually problematic, so we consider this too. Section IV concludes.

II. BITCOIN, AND CRYPTOCURRENCIES IN GENERAL

Bitcoin, nowadays a textbook subject (e.g. [25], [3]), was launched in the shadow of the financial crash of 2008, bringing to life the proposal in [24]. It grew into a phenomenon that reached the public at large in say 2016/17. By then its POW had attracted attention for the energy it consumed: Ireland and Denmark were cited as comparable in energy consumption [14], [4]. Its idelitic decentralised view was seen as a counterbalance to the manipulation of fiat currencies after the 2008 crash [35], [31]. Ironically, Bitcoin had its own bubble and crash at the end of 2017, in all respects comparable to historical bubbles and crashes [10], [11], [18], [7], and although this resulted in an uplift in its value compared to earlier, the trend that followed was gently downwards, as many investors have become disillusioned [23], [26].

Ironically too, the drive to greater POW hash breaking power has led to the creation of custom Bitcoin-hash-breaking ASICs [17], and to the fact that Bitmain [5], now controls close to a majority of the world’s Bitcoin creation power: decentralisation morphs into centralisation!

Without doubt, the phenomena alluded to arise because Bitcoin, and cryptocurrencies in general, are unregulated. These days there are many views on this; see e.g. [22], [34]. We do not have space to elaborate further on these points.

III. PUNISHMENT, NOT REWARD

In the previous section, we briefly discussed the pros and cons of cryptocurrencies. These argued that cryptocurrencies are prone to many sources of instability coming from the wider real world context. This being so, any blockchain application for whose working cryptocurrencies are central, will be affected by the same issues to a greater or lesser extent, and this can undermine the viability of the application, even if currency is not its main purpose. The obvious conclusion is to do without cryptocurrencies in blockchain applications, if possible. However, we must still motivate the maintenance of the blockchain and of balancing the interests of all the participants, traditionally achieved via cryptocurrencies.

We do not offer a universal panacea to the issue of blockchain incentivisation, but we outline a class of applications for which a plausible cryptocurrency free scheme for sustaining a blockchain solution can be constructed. The essential elements of the scheme are as follows.

• The entities involved in the scheme must be such that loss from reputational damage outweighs any gain to be had
The key idea of this paper is that blockchain applications should be seen, above all, as application specific (dis)incentive engineering. It is important to do the (dis)incentive analysis thoroughly. Recent history is rife with instances of perverse outcomes spawned by the use of incentive structures to drive behaviour. The health service sphere provides many examples, e.g. in the US [9], or in the much revered British NHS [27].

We extolled denial of service to the application and/or revocation of participants’ anonymity as useful internal mechanisms to encourage good behaviour, in contrast to approaches using cryptocurrencies, which were seen as external mechanisms. These were much more vulnerable to outside attacks that were limited only by the ingenuity of the external attackers, the extremes of whose inventiveness would be hard to defend against absolutely. We identified a number of criteria that were in sympathy with the point of view just described, and coined the term PnR architecture for blockchain systems designed on those principles.

One area we did not have space to explore was the tension between the traditional desire for application details (especially in the commercial sphere) to remain confidential, and the corresponding necessity for details to be made public to enable blockchain verification. It is inevitable that bridging this impasse will call on increasingly sophisticated cryptographic techniques, and what is considered ‘good enough’ from this standpoint will be very much application dependent. The more complex the privacy concerns and interdependencies between the different parts of the application ecosystem, the more subtle will the cryptography need to be. The appreciation of this point in general is not yet as widespread as it needs to be and we leave such concerns to future work.
REFERENCES


