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.

978-1-7281-1328-9/19/$31.00 ©2019 IEEE

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 idealitic 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

from gaming the system. The potential consequences of loss of reputation following from misbehaviour, needing to be severe enough to lead to organisational damage, constitute the major stabilising force motivating good behaviour. Examples of such entities include: health service entities, educational entities, professional services e.g. the law and accountancy, commercial entities for whom ethical considerations are an integral component of their public image, etc.

■ The scheme is focused on running an application and enterprise specific permissioned blockchain. In this manner, all entities involved have a similar cost/benefit spectrum of incentives and disincentives for participation. Also the major scalability challenges of running a massive all-purpose blockchain are avoided.

■ The application must support a mission critical part of the participant entities' working, or must support a functionality whose forfeit would result in a serious loss of some kind.

■ The immutability properties of the blockchain should give a significant non-repudiation added value to entities' automated processes that would be hard to achieve by other means. Concomitantly, all entities must agree to accept the consequences of the inability to forget old information on the blockchain (especially in the light of regulatory developments such as GDPR in the EU [33], or CCPA in California [32]). Similarly, any application specific requirements for auditing [30], must be explicitly built into the blockchain protocol from the outset.

■ If particular parts of the application specific protocol are best served by micropayments to participating entities, these can be managed by cryptocurrency-like mechanisms, on the understanding that the payments refer to fiat currencies and are intended to be settled in bulk periodically, when the accumulated amounts justify fiat currency transaction charges.

■ The protocol managing the blockchain application must monitor entities' behaviour in respect of them discharging their obligations to maintain the viability of the blockchain. Failure to discharge agreed obligations results in **denial of service to the application** and/or **revocation of anonymity**, thus impacting on defaulting entities' interests. The tension between knowing entities' identities (so they can be punished if need be) and keeping details of entities' business appropriately confidential must be explicitly considered and resolved.

■ While the protocol managing the application must cater for a range of expected eventualities, it is unlikely that every possible contingency can be foreseen and programmed at the outset. So there should be recognised error exits in the protocol machine to allow for exceptional circumstances, to be handled by exiting automated working, and having recourse to human mediated legal or commerial techniques.

We see in the above a balancing of incentives and disincentives that does not use cryptocurrencies (except trivially). Instead of hoping to promote good behaviour, we punish bad behaviour by confounding access to the application itself — which, since entities chose to participate, they would find undesirable. The other advantage of this approach is that it is based on mechanisms that are purely *internal* to the application (relying on entities' presumed desire to benefit from using it), rather than trying to forsee threats which in large measure may be based on *external* circumstances. The internal focus implies that with *one* internal punishment mechanism we are able to counter *many* external threats (by eliminating their possibility).

The need to be able to enforce denial of service and/or revocation of anonymity impacts the blockchain protocol. Some kind of committee based policing is needed to approve normal participation and to punish misbehaviour. Natural candidates are Delegated Proof of Stake [13], [15], Proof of Authority [28], or Algorand [2]. Hyperledger [20], [21], is a framework within such approaches could be housed. Wider discussions of consensus mechanisms include [29], [36], [6], [8].

When a new blockchain application (running on a fresh blockchain) is made live, one of the most common problems encountered is a dearth of 'hashing power' or its analogue (according to the consensus protocol used). In the PnR scheme just described, the problem is exacerbated by the intention to keep the blockchain permissioned and (relatively) special purpose. The lack of distributedness (and the dearth of trust that it engenders) can be partially assuaged by regularly posting a transaction on an established blockchain (e.g. Ethereum [16]) that contains a hash of the PnR chain's latest block.

IV. Conclusion

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

[1] Against the 'Putrid' Euro, https://cointelegraph.com/news/against-the-putrid-euro-naples-mayor-plans-to-launch-autonomous-cryptocurrency.

[2] Algorand, 2018, https://www.algorand.com/ https://medium.com/algorand/secure-blockchain-decentralization-via-committees-7602f598a0a9 https://medium.com/algorand/algorands-instant-consensus-protocol-e66ac5807e37 https://eprint.iacr.org/2018/377.pdf.

[3] A. Antonopoulos, *Mastering Bitcoin*. O'Reilly, 2017.

[4] Bitcoin's insane energy consumption, explained, https://arstechnica.com/tech-policy/2017/12/bitcoins-insane-energy-consumption-explained/.

[5] Bitmain, https://www.bitmain.com/ https://en.wikipedia.org/wiki/Bitmain.

[6] V. Buterin, "On Stake," 2014, https://blog.ethereum.org/2014/07/05/stake.

[7] E. Chancellor, *Devil Take the Hindmost: A History of Financial Speculation*. Plume Books, 1998.

[8] Consensus: Immutable Agreements for the Internet of Value, 2016, https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/kpmg-blockchain-consensus-mechanism.pdf.

[9] Cook, P., "How Perverse Incentives are Ruining Healthcare," *rheumatology network*, http://www.rheumatologynetwork.com/healthcare-policy/how-perverse-incentives-are-ruining-healthcare.

[10] R. Dale, *The First Crash: Lessons from the South Sea Bubble*. Princeton University Press, 2016.

[11] M. Dash, *Tulipomania: The Story of the World's Most Coveted Flower and the Extraordinary Passions it Aroused*. W&N, 2010.

[12] S. Davidson, F. De Filipi, and J. Potts, "Disrupting Governance: The New Institutional Economics of Distributed Ledger Technology," https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2811995.

[13] Delegated Proof of Stake, https://coincentral.com/what-is-delegated-proof-of-stake-exploring-the-consensus-algorithm/ https://www.mycryptopedia.com/delegated-proof-stake-dpos-explained/.

[14] Distributed Ledger Technology: Beyond Block Chain, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf.

[15] EOS, https://eos.io.

[16] Ethereum, https://www.ethereum.org/.

[17] Google search: cryptocurrency mining rig.

[18] Great Britain. Ministry Of Transport. Financial And Statistical Dept, *Railway Returns: Returns of the Capital, Traffic, Receipts, and Working Expenditure, Etc, of the Railway Companies of Great Britain*. Ulan Press, 2012.

[19] G. Hileman and M. Rauchs, "Global Blockchain Benchmarking Study," Cambridge University, Judge Business School https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-09-27-ccaf-globalbchain.pdf.

[20] Hyperledger, https://www.hyperledger.org.

[21] Hyperledger fabric, https://www.hyperledger.org/projects/fabric.

[22] T. Kwiat, "Beyond Bitcoin: Issues in Regulating Blockchain Transactions," *Duke Law Journal*, vol. 65, pp. 569–608, 2015.

[23] C. Mackay, *Extraordinary Popular Delusions and the Madness of Crowds*. Wordsworth Editions, 1995.

[24] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," https://bitcoin.org/bitcoin.pdf.

[25] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press, 2016.

[26] New Satesman, "How Bitcoin Resembles the South Sea Bubble," https://www.newstatesman.com/politics/economy/2017/12/how-bitcoin-resembles-south-sea-bubble.

[27] C. Paton, "Present Dangers and Future Threats: Some Perverse Incentives in the NHS Reforms," *BMJ*, vol. 310, pp. 1245–1248, 1995.

[28] Proof of Authority, https://medium.com/poa-network/proof-of-authority-consensus-model-with-identity-at-stake-d5bd15463256 https://wiki.parity.io/Proof-of-Authority-Chains.

[29] M. Rauchs, A. Glidden, B. Gordon, G. Pieters, M. Recanatini, F. Rostand, K. Vagneur, and B. Zhang, "Distributed Ledger Technology Systems: A Conceptual Framework Report," Cambridge University, Judge Business School https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2018-08-20-conceptualising-dlt-systems.pdf.

[30] M. Smith, "The Blockchain Challenge Nobody is Talking About," 2017, http://usblogs.pwc.com/emerging-technology/the-blockchain-challenge.

[31] J. Stiglitz, *The Euro: And its Threat to the Future of Europe*. Penguin, 2017.

[32] The California Consumer Privacy Act, 2018, https://www.caprivacy.org/ https://searchsecurity.techtarget.com/blog/Security-Bytes/Is-the-new-California-privacy-law-a-domestic-GDPR https://www.firstsanfranciscopartners.com/blog/california-consumer-privacy-act-of-2018-vs-gdpr/ https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375.

[33] The EU General Data Protection Regulation, 2018, https://www.eugdpr.org/ https://gdpr-info.eu/ https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en.

[34] UK House of Commons Treasury Committee Report: Crypto-Assets, https://publications.parliament.uk/pa/cm201719/cmselect/cmtreasy/910/910.pdf.

[35] Y. Varoufakis, *And the Weak Suffer What They Must?: Europe, Austerity and the Threat to Global Stability*. Vintage, 2017.

[36] R. Wattenhofer, *The Science of the Blockchain*. Inverted Forest Publishing, 2016.