Five Things You Should Not Use Blockchain For

Martin Gilje Jaatun*†, Peter Halland Haro‡ and Christian Frøystad§
*University of Stavanger, Norway
†SINTEF Digital, Trondheim, Norway
‡SINTEF Nord, Tromsø, Norway
§Secure Practice AS, Trondheim, Norway

***Abstract*—The Bitcoin fever notwithstanding, the underlying blockchain technology cannot solve all data exchange and product needs, as some seem to believe. This paper provides examples of problems that we believe are poorly suited to a blockchain solution.**

***Index Terms*—Blockchain, Security, Privacy, Suitability, Applicability**

I. Introduction

The Bitcoin [1] cryptocurrency keeps cropping up in the news. Cryptocurrencies are based on blockchain, a digital, public distributed ledger. Their main reason for being relate to uncertainties related to intermediaries. Many are now advocating using blockchain as a universal solution for transactions, whether it is goods, services or information that needs to transferred or exchanged. Unfortunately, it's not that simple [2].

II. The Great Big Spreadsheet in the Sky

What is a blockchain [3]? Some people compare them to giant spreadsheets, where all transactions between given parties are registered and approved. Every time a new transaction is performed, it is added to the blockchain – and also copied to all users.

The result is a solution that is independent from intermediaries – all the blockchain participants have the same information at a given time, which enables making the majority adjudicate any disagreements.

Running a blockchain is not free, however, and there are some strict requirements on the operations the users must perform. This contributes to making blockchains unsuited to delivering on some of the expectations they are met with (table I).

TABLE I
Five things you should steer clear of on the blockchain

Application	Why not
General monetary system	Latency and fundamental structure
Sensitive Personal Identifiable Information	The right to be forgotten
Digital elections	You need to trust the other elements
Users with poor internet	No way to ensure consensus
Distributed calculation	Redundancy, no parallelism, no coordination, poor efficiency

III. Do You Need a Blockchain?

Wüst and Gervais [4] helpfully provided a flow chart, which we have re-created in Fig. 1. Peck [5] provides a similar, but slightly different flowchart. The key takeaway here is that you don't need a blockchain if you can solve your problem with a trusted third party and a database.

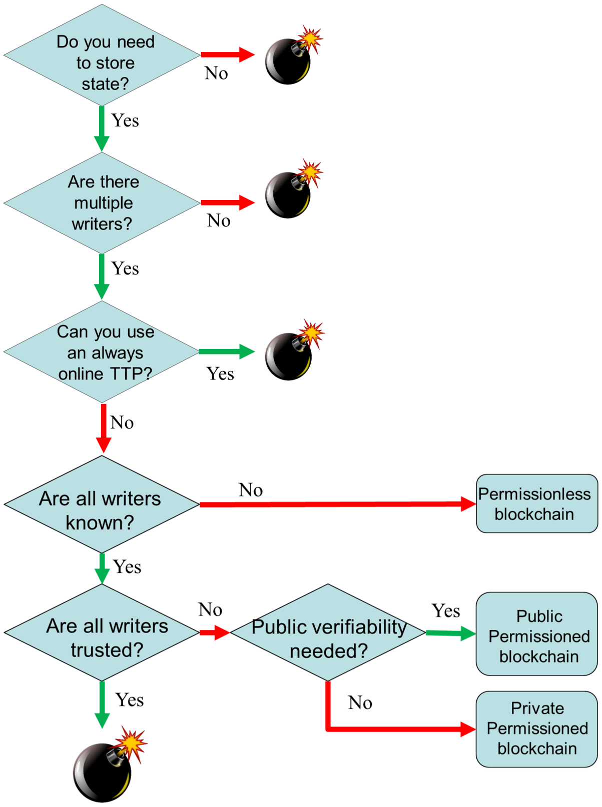
Do you need to store state?
No
Yes
Are there multiple writers?
No
Yes
Can you use an always online TTP?
Yes
No
Are all writers known?
No
Permissionless blockchain
Yes
Are all writers trusted?
No
Public verifiability needed?
Yes
Public Permissioned blockchain
No
Private Permissioned blockchain
Yes

Fig. 1. Flowchart: Do you need a blockchain?

IV. Blockchains Are Unsuited For...

In the following, we dive deeper into the five things mentioned in Table I.

A. Replacement of current monetary systems

First of all, crypto currencies will primarily remain an object for speculation [6]; they will never take over as a general payment system. This is due to some of the inherent properties of blockchain.

Crypto currencies exist because some people do not trust banks or intermediaries such as Visa, MasterCard and recipients that incur extra costs for transactions.

It is said that because blockchains are decentralized, they are tamper-proof. However, many currency miners pool resources in order to minimize the risk of loss; this has led to the establishment of cartels with so much computing power that they theoretically could manipulate transactions. This actually give the cartels more control over the currency than the banks currently have over traditional currency, since the banks need to collaborate internationally. Furthermore, there is a difference between something being tamper-proof and being *tamper-evident* – blockchain can never promise more than the latter.

B. Storage of confidential and time-limited data

The requirement that all users need to have a copy of all the data in the blockchain, makes handling of confidential data difficult. You could of course always encrypt the sensitive data, but then you get the additional challenge of key management, which counteracts the decentralized principle. Furthermore, nothing that is put in a blockchain can ever be removed without breaking the protocol, and due to the natural development in processing capabilities and key length requirements [7], the chosen encryption will inevitably weaken over time, eventually becoming practically broken.

Another thing is that putting encrypted data on the blockchain removes an important transparency and verifiability aspect - by using a suitable one-time pad, any stored data could decrypt to anything, i.e. ”The answer to life, the universe and everything is 42” is equally likely as ”Donald is a really nice guy who just wants 2 have fun”.

Storing of sensitive Personal Identifiable Information (PII) on blockchains is also challenging, if not impossible, precisely because information cannot be removed once it has been added. The EU General Data Protection Regulation [8] causes this to be a problem, due to its requirement that PII shall be completely erasable on request (also known as ”the right to be forgotten”).

C. Digital elections

In a digital election, the voters need to trust a central actor that ensures that the election is held, that digital ballots are created, and that those that are eligible to vote can be authenticated. If citizens choose to trust that this is done correctly, they have no reason to distrust the same actor's ability to count votes. Blockchains will thus add little extra value.

Furthermore, there is the issue of voter anonymity, which currently has no good solution on the blockchain.

D. Servicing users with no or poor internet

If blockchains are meant to function as intended, then all involved need to be able to continually communicate in order to achieve consensus on the current content of the chain, and a continuous internet connection is required. Environments such as ships, airplanes and anything involving distributed sensors will struggle complying with this requirement.

If we turn to the Internet of Things (IoT), the blockchain will never control the interface between the physical and digital world. If you compromise the ”thing”, all bets are off.

E. Distributed networks for calculations

It has been claimed that blockchains will revolutionize the need for computing power, by allowing ordinary people to form global computational networks that can tackle enormous challenges without specialized equipment, but this is incorrect. A blockchain will represent an enormous redundancy of computing power, no real parallelism, no coordinated operations, and thus no efficiency.

F. Even more things

We could go on, but before closing we will mention a few more things.

1) Supply-chain management: If all parties can be trusted to contribute to the final product, why not to write supply-chain data? There will after all always be an interface between the physical and digital world. To put it another way: we can use the blockchain to track the progress of a product ID across the globe, but how can we be sure that this product ID is only associated with the physical product we hold in our hand? What prevents someone from copying a valid product ID?

2) Detecting counterfeit drugs: This is just a special case of supply-chain management. Why not use an ordinary signature?

V. Discussion

One important issue is that the blockchain is not your only tool. Thus, rather than asking the question ”can we use blockchain to solve this problem?”, you should be asking ”is blockchain the most appropriate solution to solve this problem?”

VI. Conclusion

Blockchain is a fascinating technology, but cannot be compared to the revolution that the Internet represented. It has uses within logging and tracing, signing and sharing of certificates, in addition to cryptocurrencies for investment purposes. The limitations of the technology imply, however, that blockchain is not the answer to all transactions. Blockchains should thus not be the only tool in the IT toolbox of the future.

Acknowledgements

This paper is funded in part by the SINTEF strategic project SiChain.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system, http://bitcoin.org/bitcoin.pdf," 2008.

[2] N. Weaver, "Risks of cryptocurrencies," *Commun. ACM*, vol. 61, no. 6, pp. 20–24, May 2018. [Online]. Available: http://doi.acm.org/10.1145/3208095

[3] D. J. Yaga, P. M. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview." [Online]. Available: https://doi.org/10.6028/NIST.IR.8202

[4] K. Wüst and A. Gervais, "Do you need a blockchain?" in *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, 2018, pp. 45–54, https://eprint.iacr.org/2017/375.

[5] M. E. Peck, "Blockchain world - do you need a blockchain? this chart will tell you if the technology can solve your problem," *IEEE Spectrum*, vol. 54, no. 10, pp. 38–60, October 2017.

[6] C. Frøystad and P. H. Haro, "Dette er blokkjeder uegnet til," *Dagens Næringsliv*, 2018. [Online]. Available: https://infosec.sintef.no/informasjonssikkerhet/2018/09/dette-er-blokkjeder-uegnet-til/

[7] M. Blaze, W. Diffie, R. L. Rivest, B. Schneier, and T. Shimomura, "Minimal key lengths for symmetric ciphers to provide adequate commercial security. a report by an ad hoc group of cryptographers and computer scientists," INFORMATION ASSURANCE TECHNOLOGY ANALYSIS CENTER FALLS CHURCH VA, Tech. Rep., 1996.

[8] EU, "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)," *COM*, vol. 11, no. Final, 2012.