Governance with Consensus Mechanisms for Blockchain: Overview and Trends

Stephane Caporali, Caporali Conseil

April 7, 2022

Abstract

In the period that has passed, many projects in the form of proof of concept have been developed, and the most famous blockchain like Bitcoin and Etherium are old enough to start thinking about industrial projects and research trends in a more mature approach. This document aims to ask questions from the perspective of the relationship between consensus mechanisms and blockchain governance tools, starting from industrial issues towards research themes. Two research trends are presented, as likely to emerge in the coming years. This article ends with a reflexion on the life cycle of blockchain technology, regarding the current period.

Keywords: Blockchain, governance tools, consensus mechanism, on-chain, off-chain, timestamping, dating, ordering, quantum consensus mechanism.

1.Governance of consensus mechanisms

Introduction

Blockchain governance begins with a challenge, perhaps the challenge of all challenges: how to reconcile governance and decentralization. The title of this paragraph may surprise because we do not regulate the consensus mechanisms. However, the problem is that in a blockckchain project, the implementation and the technical choices involve taking into consideration the choice of the consensus mechanism.
The property of the consensus mechanism that interests us in this document is the property of ordering: the consensus is the agreement that the chain contains a coherent order of transactions. We sometimes find the term : consensus algorithms, instead of consensus mechanisms. In this document, I use both terms in the same sense.

First approach: use of a consensus mechanism classification tool

Governance accompagnies the life cycle of the blockchain. In the implementation stage of a project, the choice of a consensus algorithm is crucial. A blockchain project generally begins with the choice of the consensus algorithm. At this stage, a tool of classification is a governance support tool. However, the question is: according to what criteria?

- A possible criterion is the technical family of the consensus mechanism: for example, Nakamoto Consensus vs Byzantine Agreement.
- Another possibility is to classify by use case. For example, in the field of energy where a lot of small connected objects (IoT) are used, specific consensus algorithms could be used, for example PoET.

Second approach: support by a blockchain service provider

A frequently asked question is: how am I going to choose the right consensus mechanism if I don't have the technical background to choose? In this case it is possible to have a blockchain service provider and to entrust him with the choice of the consensus mechanism. In this case the choice of the consensus mechnaism is transparent for the client. The question in this case is: is it really decentralized governance? Who trusts
the provider?

Conclusion We see that no solution is ideal. However, the type of consensus mechanism involves the characteristics of the blockchain. For example, a Byzantine agreement is generally associated with small blockchains in private mode due to the limitation of the model with a large number of nodes.

2.Governance with consensus mechanisms

Introduction

It is clear that we govern the blockchain, we govern the consensus mechanism, in the sense that we choose the specifications, and not the contrary. but is it so clear? Perhaps we should be more pragmatic and admit that we have to govern *with* the limits that the technique imposes on us in our way of governing. How is it possible?

Illustration: the issue of the dating in the chain

Property of ordering of events in the chain

In traceability, the case of timestamp is fundamental, and pioneering works before the creation of the blockchain by Satoshi Nakamoto were carried out in particular by Stornetta and Habert (1990) [9] on the subject of timestamping. The question is: what is the relationship between the consensus mechanism and the timestamp? Consider the first role of the consensus mechanism is to ensure the order of events. This is why in the case of proof of work:

- The rigidity of the chain is the result of the one-way function associated with the hash function.
- The rule of the longest chain associated with the proof of work (the consensus mechanism) is the guarantee that the chain is not a fork: the risk of 51 % attack exists, but the risk is more limited the longer the chain. It is this sequentiality that constitutes the trust. Can we consider this order as sufficient to guarantee the dating of an event?

Principe of network adjusted time and decentralized time

The date is written in the block by the miner. However, the mechanism is that of the network adjusted time: the miner will somehow look for the date in its external environment, i.e. the adjacent nodes. Here's how it works: according to Bitcoin Wiki (2022) [1] a timestamp is accepted as valid if it is greater than the median timestamp of previous 11 blocks, and less than the network-adjusted time + 2 hours. The network-adjusted time is the median of the timestamps returned by all nodes connected around. It is easy to understand that under these conditions the timestamp is not precise and the inaccuracy can go up to one or two hours. Note that this is a decentralized way of acquiring the date and that's what's important: not totally decentralized but it goes quite far in decentralization.

Nature of the property of dating

Where is really the trust? In the date or in the order of the events of the sequence? According to Ladleif and Weske (2020) [11] the trust is well in the ordering, even if accuracy is in the dating (table II).
Blockchain's security function is an integrity function, and it is about the ordering, more that the dating. In this sense, the date is an additional parameter: in addition to the ordering, the date parameter is a form of control: in that sense, dating is linked to an objective of governance.

Governance and tools

The term governance is used in the sense of IT governance: to define it, ISO (2015) [2] states that governance is a system by which the current and future use of IT is directed and controlled. However, the expression used
in this document is: governance tools. Governance tools are governance support tools. For example, a smart contract, as a program running on-chain, can be a governance tool. In a technical environment, governance relies more and more on tools. It is almost impossible to govern without tools.

Ordering and dating classification table

Combining the function of dating with a governance tool is the vision developed in this document. Intuitively, we would rather say that the function of dating is a security function. But on the contrary, the point of view presented in this document is that the associated security function is the function of ordering. By extension, the reliability of the ordering between events in the chain is a particular form of integrity as presented table 1.

Property	Associated function proposed	Domain proposed	Implementation
Dating	Control	Governance	On-chain or/and off-chain
Ordering	Integrity	Security	On-chain

Table 1: Ordering and dating classification table

The purpose of this paragraph is to highlight that there is an underlying technical structure to governance, in the form of governance tools, and this will require research in the years to come.

On-chain vs off-chain governance tools

The notions of on-chain/off-chain are often used concerning the transaction: a transaction can be realized on-chain or off-chain. Off-chain transactions are not the original spirit of blockchain, in the sense of Satoshi Nakamoto, however it is sometimes used:

- Facing scalability issues
- To support the transactions when an external data is needed.

It is not necessarily related to governance. However, it can be accepted that:

- On-chain governance tools are based on smart contract.
- Off-chain governance tools are based on legal and institutional tools.

However, the question arises: Are there specific on-chain and off-chain governance tools? The question is not so easy. What is the problem?

Different dating techniques

Another way to get the dating is to go through by an external time server via an oracle, as describe by Ladleif and Weske (2020) [11].
Note that we find the usual differentiation on-chain/off-chain governance tools if the dating is a tool, except that off-chain is not legal or institutional data but a server, an architectural device. We can roughly summarize, following with Ladleif and Weske
(2020) [11] :

- On-chain approach: network adjusted time approach or parameter added in smart contract.
- On-chain and off-chain approach: external server with the use of an oracle.

This leads us to have another angle of view on what an on-chain or off-chain governance tools is: the notion can be extended, for example to a time server.

Concept of isolation by design and implications for governance

Introduction

The concept of isolation by design exists with the blockchain and the idea is to know in what sense it is used, how the consensus mechanism is engaged and what are the consequences on the governance tools.

Isolation from the outside of the blockchain

On-chain transaction is isolated by design. This expression isolated by design is written by Ladleif and Weske
(2021) [12] who present the characteristic of a closed world by reasons of integrity: the data must not be altered by a centralized external source that does not respect for the decentralized nature of the blockchain. The same idea is developed by Caldarelli (2022) [4] who defines the blockchain as a closed ecosystem, the open characteristic being linked to the property of the content to be freely accessible (readable). In this sense, the blockchain is not natively prepared to deal with external events. The oracle is a service that updates a blockchain using data from the off-chain environment, for example for the need of an on-chain confined smart contract. The typical example of the oracle as explained by Caldarelli (2022) [4] is when there is a need for a transaction between two cryptocurrencies, and there is a need to know the rate of exchange between the two, in real time. This information must be collected externally. In the case of timestamp, an oracle could be used to take the timestamp from a external time server, as described by Ladleif and Weske (2020) [11] where smart contracts are described as passive and executed between discrete transactions. The limit of an oracle is that it introduces a form of centralization with a new trusted intermediary. Who will trust the oracle? as express Caldarelli (2022) [4] . Thus a weakness of the blockchain in supply chain applications is inherent in the trust that we can have in the oracle.

Isolation between transactions in the chain

This second aspect is particularly subtle and the main subject of the issues developed in this document. A smart contract is started with a transaction and stops when the transaction is completed. The result of the execution of the code of the smart contract can be written in the chain. The isolation could be considered by isolation by design, but not between a transaction and the outside world, but between two transactions. This aspect exists in the idea developed by Ladleif and Weske (2021) [12]. This is the property of the consensus mechanisms and the fact that validating not the content but the ordering of the transaction "take times" (for example nearly 10 minutes for the proof of work): this discrete aspect exists. The term discrete is used in the mathematical sense, when we say that a sequence of data is discrete, it means that it is discontinuous, and this discontinuity is a kind of isolation by design between the entities, here represented by the transactions. This have an obvious effect on what we can do with a smart contract, in a transaction. Now we understand that the limit imposed on us by the consensus

algorithm is this specific temporality and by consequently this isolation by design within the limit of governance. How to use governance tools in an isolated environment?

Conclusion

The temporality specific to the blockchain and imposed by the consensus mechanism limits the freedom we have within a transaction, in the use of smart contract in support of governance objectives. This aspect is structural to the blockchain and means that we cannot separate the governance from the underlying technology. This goes beyond mere isolation with the external world and engages the sequenciality of the chain itself.

3.Blockchain and approach by experience

The End-to-End Principle

During the 1980, in particular by Saltzer and al. (1984) [20] a legal approach states the end-to-end principle: it should not be intermediate like the routers between two users of the Internet network. This is a network approach, in the technical sense of the security network, and legal at the same time. The idea is to give control to the end user. This is a reaction to the fact that the network is moving towards a centralized architecture.

The Man-in-the-Middle attack

In network security, when someone intercepts data in a communication channel, it is a man-in-the-middle attack. Fundamentally, the TCP/IP protocol itself is concerned with the fact that the TCP acknowledgment can be corrupted. This poses the problem of the trusted intermediary.

Some previous work on timestamping

In the field of cryptography, earlier work by Stornetta and Habert (1990) [9] describes the creation of the chain through the use of the hash function. It is not yet the blockchain, imagined by Nakamoto (2008) [17], but a chain in the form of a series of blocks linked by the properties of the hash function. However, the audacity of the proposed solution concerns more the transaction than the consensus itself, even if Stornetta and Habert proposed in their work a probabilistic consensus. The works of Stornetta and Habert were not alone at that time, but they had the merit to clearly posing the problem of the TSS : the trusted intermediary of the time service provider with the underlying question : who will trust the trusted intermediary ?

The Byzantine general’s problem

Related to the work in the distributed system, and in particular of Lamport and al. (2019) [14] the Byzantine General's problem statement is an illustration of the problematic of achieving consensus in a distributed environment. There followed other rich works that enriched the theory of distributed systems, often qualified as a Byzantine approach. However, the Byzantine formalism is applicable to all types of consensus mechanisms.

The financial crisis of 2008 and the empirical approach

It is remarkable that bitcoin was shortly preceded by the financial crisis of 2008, and Satoshi Nakamoto's (2008) white paper [16] is not that difficult to read: the paper is relatively short and concrete, despite its disruptive nature. Satoshi Nakamoto not only wrote the white paper, but also developed the bitcoin, and communicated in a specialized forum until he announces his withdrawal a few months later. It is gradually and because "it works" that bitcoin attracts the attention of the academic and financial world first, and then of the general public. It is the experience of its functioning, its resilience, its solidity, which made bitcoin what it is.

The intersection of several technical influences

Sometimes a theory gives birth to a concrete application, but in the case of the blockchain, it is on the contrary bitcoin as an application which subsequently led to a lot of theoretical work, and there is still a lot to be done. This is what I mean in this part of the document by the previous historical reminders is that, in a certain way, bitcoin and by extension the blockchain value the experience. The bad side is that we are in a situation where, despite the high number of research works in recent years, blockchain in general is still a young field where we need theoretical developments. What are the new research trends that can change the things? The first could be the emergence of new consensus algorithms, and the second the raise of an abstract framework. Without being exhaustive, the following paragraph does not present a comprehensive state of the art but focuses on two trends because their possible relationship with the convergence of consensus mechanisms and governance tools. My preparatory work preceding the writing of this document consisted of monitoring research work on subjects related to consensus mechanisms, and secondly to promote two qualitative directions because of their strategic or innovative aspects. This should not overshadow the importance of other directions of work, for example the improvement of the existing consensus mechanism (for example about the scalability problem), or the design of new consensus mechanisms combining two existing ones such as Proof of Stack and Byzantine agreement. However, four years ago, the question of trends blockchain consensus mechanisms

came to me, characterized in my opinion at that time by the emergence of the alternative Nakamoto Consensus (proof of...) and the renewal of the Byzantine agreement.

4.Two research trends

Quantum consensus mechanisms

Issue

Are new consensus algorithms possible? A fairly recent subject, the quantum blockchain and the associated consensus mechanisms deserve our interest. Not to be confused with attacks against a blockchain by a quantum computer. Quantum blockchain may introduce new consensus mechanisms and by extension a new area of research for the next years. This could lead to an alternative to proof of work, characterized by its high energy consumption and scalability problem. The introduction of new quantum based consensus mechanisms, if confirmed in the coming years, will involve new possibilities and constraints of governance due to their technical characteristics. Academic work on quantum blockchain is a recent topic, some of them are particularly interested in the consensus mechanism.

Some recent works

- Wen et al. (2022) [24] design a new consensus mechanism of quantum blockchain based on the randomness and the irreversibility of quantum measurement and quantum zero-knowledge proof. According to the author, by this way a great deal of computing resources and energy can be saved.
- Nilesh and Panigrahi (2022) [18] propose a model of quantum blockchain based on generalized Gram-Schmidt procedure utilizing dimensional lifting, which is practically realizable. The consensus consists of the following three steps- the proposing step, the voting step, and the decision step.
- Chen et al. (2021) [6] propose new post-quantum proof of work (post-quantum PoW) consensus algorithm for security and privacy of smart city applications. According to the authors, it can be used to supply memory mining. In this case, the basic puzzle objects of this new PoW algorithm are a system of multivariate quadratic equations.
- Rajan and Visser (2019) [19] focuse on the case of quantum entanglement: for the quantum blockchain, they replaced the important functionality of timestamped blocks and hash functions linking them with a temporal GHZ state with an entanglement in time. The quantum network uses the _-protocol, which is a consensus algorithm where a random node in the quantum network can verify that the untrusted source created a valid block.
- In this work, Faridi et al. (2022) [7] present a systematic literature review starting with identifying the research questions. At the question: Frequency Analysis of Solution for the Discussed Challenges, "new consensus" represents 14 % (Figure 4).
- In their paper, Ullah et al. [23] evaluate the performance of various quantum Byzantine agreement(QBA) protocols in terms of their scalability, security, and decentralization for blockchain consensus.

Algebra, state machine and other theoretical approaches

Issue

The blockchain is composed of different parts:

- The decentralized consensus Resulting from work in distributed systems (Byzantine approach).
- The chain with the hash function Coming from the field of cryptography, which started with symmetric then asymmetric cryptography, then the development of the hash function
- The distributed storage Distributed network is a type of networks used in the internet network, in particular database provider, the distributed data is a way to be sure not to lose the data, by duplicating the data in different places in the network.

Note that if the validation is decentralized, the storage is distributed: the two notions should not be confused. Each of the three domains has its own formalism, and this the difficulty. There is not a domain divided in three parts, but three very different parts from each other, and the "miracle of the blockchain" is that put together it works. The problem then is to create an underlying theoretical structure. To what extent could or could not the consensus mechanism support this structure?

Some recent works

- Lambert (2021) [13] presents a reformulation in topos logic of a safety result arising in an abstract presentation of blockchain consensus protocols.
- Shapiro (2021) [21] present a Multiagent Transition System Protocol Stack. The framework also offers formal | yet natural and expressive | notions of faults, fault-resilient implementations, and their composition.

- In this paper, Zha (2020) [25] presents the first study on the algebraic structure of blockchains with an emphasis on the internal properties under algebraic groups.
- In this work Gabbay (2021) [8] condenses the theory of UTxO blockchains down to a simple and compact set of four type equations (Idealised EUTxO), and to an algebraic characterisation (abstract chunk systems).
- Shorish (2018) [22] presents a formalization of blockchain as a state machine. Further, this interesting work associate state machine and governance concepts (Figure 1).
- Lin et al. (2020) [15] investigate the relationship between underlying blockchain mechanism of cryptocurrencies and its distributional characteristics.
- Hennebert (2020) [10] applies the rigourous standardized methodology of the common criteria to consensus mechanisms.

5.Main questions and perspectives

Finally, can we summarize the aspects developed in this document into main questions? Some possible questions are:

- Is on-chain governance limited by the fact that a transaction is isolated by design?
- Are on-chain and off-chain separated by different temporalities? Is the oracle enough to unify the two? This is one issue of the decentralized governance.
- Is there a technical framework in accordance with the two temporalities?
- Is it possible to switch from one consensus mechanism to another using this technical framework (consensus agnostic)?

In my point of view, a framework is not a technique but a mode of representation. The purpose of this document is to present the problem of building a framework consensus agnostic in order to have a sustainable blockchain. A framework whose objective is to reconcile governance and decentralization. Today beyond the proof of concepts the objective is to see the behaviour of a blockchain in a long term, in accordance with the requirement of durability and its sub-part the resilience of a technical system, such as its ability to withstand fluctuations as I have presented in my previous document. [5] Perhaps blockchain technology is in a transition phase, with a new cycle of experimentations, research and innovation that will lengthen, as we will increasingly understand the technology in its complexity in the coming years, in parallel with more mature industrial projects. The experience of the development of the Internet network has shown that there is a general tendency to underestimate the duration of technical cycles. In a different context, this was also the case in the quantum field where the foundations were laid in 1927 both during the Solvay Conference, and from the debate on non-locality as explained by Valentini and Bacciagaluppi (2009) [3], but the concrete applications of quantum calculation (which use the property of entanglement) did not arrive until the end of the 20th century (preceded it is true by the development of electronics also based on quantum effects). The past few years may have been a golden period for blockchain where everyone was talking to everyone and a technical foundation was possible based on consensus of experts from all walks of life in a short period of time. However, research and experimentation need more time, and innovation must follow its own pace. Maybe we are at the beginning of a new cycle of the blockchain.

References

[1] Block timestamp-bitcoin wiki. https://en.bitcoin.it/wiki/Block_timestamp. (Accessed on 04/07/2022).
[2] ISO-ISO/IEC 38500:2015-Information technology-Governance of IT for the organization. https://www.iso.org/standard/62816.html (Accessed on 03/23/2022).
[3] Bacciagaluppi, G. and Valentini, A. (2009). Quantum theory at the crossroads : reconsidering the 1927 Solvay conference. Cambridge University Press.
[4] Caldarelli, G. (2022). Formalizing oracle trust models for blockchain-based business applications. An example from the supply chain sector. arXiv preprint arXiv:2202.13930.
[5] Caporali, S. (2020). Time, consensus and governance by design for blockchain and DLT. Orvium, pages 10{11.
[6] Chen, J., Gan, W., Hu, M., and Chen, C.-M. (2021). On the construction of a post-quantum blockchain for smart city. Journal of Information Security and Applications, pages 3,9.
[7] Faridi, A. R., Masood, F., Shamsan, A. H. T., Luqman, M., and Salmony, M. Y. (2022). Blockchain in the quantum world. International Journal of Advanced Computer Science and Applications, page 549.
[8] Gabbay, M. J. Algebras of UTxO blockchains. Mathematical Structures in Computer Science, pages 1-56.
[9] Haber, S. and Stornetta, W. S. (1990). How to time-stamp a digital document. In Conference on the Theory and Application of Cryptography, pages 437{455. Springer.

[10] Hennebert, C. (2020). A first step towards a protection profile for the security evaluation of consensus mechanisms. In 2020 7th International Conference on Internet of Things: Systems, Management and Security (IOTSMS), pages 1-6. IEEE.
[11] Ladleif, J. and Weske, M. (2020). Time in blockchain-based process execution. arXiv preprint arXiv:2008.06210, page 5.
[12] Ladleif, J. and Weske, M. (2021). Which event happened first? Deferred choice on blockchain using oracles. arXiv preprint arXiv:2104.10520, page 2.
[13] Lambert, M. (2021). A topos view of blockchain consensus protocols. arXiv preprint arXiv:2111.07461.
[14] Lamport, L., Shostak, R., and Pease, M. (2019). The Byzantine Generals Problem, page 203{226. Association for Computing Machinery, New York, NY, USA.
[15] Lin, M.-B., Khowaja, K., Chen, C. Y.-H., and H□ardle, W. K. (2020). Blockchain mechanism and distributional characteristics of cryptos. arXiv preprint arXiv:2011.13240.
[16] Nakamoto, S. (2008a). Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review, page 21260.
[17] Nakamoto, S. (2008b). Bitcoin p2p e-cash paper. https://users.encs.concordia.ca/~clark/biblio/bitcoin/Nakamoto%202008.pdf. (Accessed on 04/07/2022).
[18] Nilesh, K. and Panigrahi, P. (2021). Quantum blockchain based on dimensional lifting generalized gram-schmidt procedure. arXiv preprint arXiv:2110.02763, page 7.
[19] Rajan, D. and Visser, M. (2019). Quantum blockchain using entanglement in time. Quantum Reports, page 4.
[20] Saltzer, J. H., Reed, D. P., and Clark, D. D. (1984). End-to-end arguments in system design. ACM Transactions on Computer Systems (TOCS), 2(4):277{288.
[21] Shapiro, E. (2021). Multiagent transition systems: Protocol-stack mathematics for distributed computing. arXiv preprint arXiv:2112.13650.
[22] Shorish, J. (2018). Blockchain state machine representation. Technical report, Center for Open Science.
[23] Ullah, M. A., Setiawan, J. W., ur Rehman, J., and Shin, H. (2022). On the robustness of quantum algorithms for blockchain consensus. Sensors, page 2.
[24] Wen, X.-J., Chen, Y.-Z., Fan, X.-C., Zhang, W., Yi, Z.-Z., and Fang, J.-B. (2022). Blockchain consensus mechanism based on quantum zero-knowledge proof. Optics & Laser Technology, 147:107693.
[25] Zhao, D. (2020). Algebraic structure of blockchains: A group-theoretical primer. arXiv preprint arXiv:2002.05973.