Blockchain Consensus Protocols
Towards a Review of Practical Constraints for Implementation in Developing Countries

Hadja F. Ouattara[1], Daouda Ahmat[2], Fréderic T. Ouédraogo[3],
Tegawendé F. Bissyandé[1,4](✉), and Oumarou Sié[1]

[1] Université Ouaga I Pr. Joseph Ki-Zerbo, Ouagadougou, Burkina Faso
hadja.ouattara@gmail.com, oumarou.sie@gmail.com
[2] Virtual University of Chad, N'Djamena, Chad
daouda.ahmat@uvt.td
[3] Université Norbert Zongo de Koudougou, Koudougou, Burkina Faso
ouedragoft@gmail.com
[4] SnT, Université du Luxembourg, Esch-sur-Alzette, Luxembourg
tegawende.bissyande@uni.lu

Abstract. There is currently a big rush in the research and practice communities to investigate the blockchain technology towards leveraging its security, immutability and transparency features to create new services or improve existing ones. In developing countries, which are seen as a fertile ground for field testing disruptive technologies, blockchain is viewed as the "trust machine" that is necessary for accelerating development. Unfortunately, the internal working of blockchain as well as its constraints are often overlooked in the design of services. This, in conjunction with a poor regulatory framework, slows down any concrete attempt to build upon the technology. In this paper, we contribute towards accelerating the concrete adoption of blockchain by making explicit the constraints that affect their practical use in the context of developing countries such as African sub-saharan countries. Overall we recommend that the technology should be adjusted to the real-world constraints, in particular those that we currently witness on network latency, computation power as well as cultural gaps.

Keywords: Blockchain · Developing countries · Adoption constraints

1 Introduction

The history of technology has shown that any of its revolutions can drastically change societies [1,2]. For the first time in the history of information technology (IT) revolutions, a single one, beyond the Internet revolution, has the potential "to act on the top-down and centralised authority that States exercise on currency, that banks exercise on financial transactions, that notaries exercise on

V. Odumuyiwa et al. (Eds.): AFRICOMM 2017, LNICST 250, pp. 304–314, 2018.
https://doi.org/10.1007/978-3-319-98827-6_29

real-state transfers, that energy monopolies exercise on electricity and fuel distributions"[1]. No other technology before the advent of blockchain has provided so many opportunities to rethink existing trust processes.

Briefly summarized, blockchain is a technology for information storage and transmission, which presents three key features: transparent, secured and decentralized. Actually, a blockchain is an immutable digital database that supports facilities for consensual validation of transactions into the database. blockchain appeared concurrently with the Bitcoin cryptocurrency in 2008. Indeed, the blockchain—originally block chain [3]—was first defined as the virtual infrastructure that enables the mining and transfer of bitcoins.

Because blockchains are *secured by design*, and shows high byzantine fault tolerance, they are increasingly used in various industries, most notably the security-sensitive financial domain. The immutability property is also relevant for establishing permanent records of any transaction. Finally, the transparency in the distributed model is essential for setting up public (e.g., national) databases accessible to all stakeholders including citizens.

This paper focuses on a central element in blockchain implementation: the *consensus protocol*, which eventually allows *people/machines who do not know or trust each other, to build a dependable ledger*. Our main contributions include:

- a comparative enumeration of state-of-the-art consensus protocols
- an assessment of consensus protocols with regards to the contextual constraints in developing countries
- suggestions of a roadmap for the sustainable adoption of the blockchain technology across Africa

The remainder of this paper is organized as follows. Section 2 quickly overviews the fundamentals of blockchain working. Section 3 describes a few use cases that are relevant to the developing world. Section 4 describes the consensus protocols and develops their strengths and weaknesses. Section 5 discusses the insights as well as related work. Finally Sect. 6 concludes this paper.

2 Understanding the Blockchain Technology

Similarly to how the concept of "world wide web" has been long assimilated to the internet, blockchain is currently mostly reduced to its cryptocurrency application. Blockchain can however be used to build a broader range of applications involving transactions.

At the core of the blockchain technology is a distributed ledger or decentralized database which keeps records of digital transactions. Instead of implementing a central administrator as in traditional databases (e.g., a bank, the government, an accountant), a distributed ledger has a network of replicated databases, synchronized via the internet and visible to anyone within the network.

[1] cf. Preface of Joël de Rosney in the book "La blockchain décryptée - les clefs d'une révolution" by Blockchain France.

Whether they are private with restricted membership (similar to an Intranet) or public and accessible to every one (similar to the Internet), blockchain networks work in the same way as depicted[2] in Fig. 1. When a digital transaction is carried out, it is sent to the network and validated cryptographically by a node, then grouped together in a cryptographically protected block with other transactions that have occurred in the last time frame (generally about 10 min) and sent out to the entire network. When a block is created, all participants in the network evaluate the transactions and, through mathematical calculations, determine whether they are valid, based on agreed-upon rules. When "consensus" has been achieved, typically among more than 50% of participating computers, the transactions are considered verified.

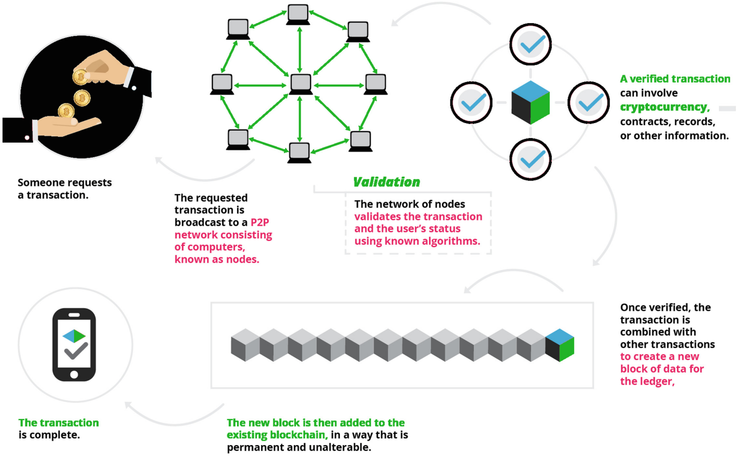
Someone requests a transaction.
The requested transaction is broadcast to a P2P network consisting of computers, known as nodes.
Validation
The network of nodes validates the transaction and the user's status using known algorithms.
A verified transaction can involve cryptocurrency, contracts, records, or other information.
Once verified, the transaction is combined with other transactions to create a new block of data for the ledger,
The new block is then added to the existing blockchain, in a way that is permanent and unalterable.
The transaction is complete.

Fig. 1. Typical blockchain working process - Schema courtesy of ©BlockGeeks

By design, blockchains are inherently resistant to modification of the data. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks and a collusion of the network majority.

3 Blockchain Use-Cases

As largely hinted in previous section, a blockchain mainly solves the pervasive problem of manipulation in transactions and data. Vitalik Buterin, inventor of the Ethereum, was reported to having said the following about manipulation: "when I speak about it in the West, people say they trust Google, Facebook, or

[2] Figure elements borrowed from https://blockgeeks.com/guides/what-is-blockchain-technology/.

their banks. But the rest of the world doesn't trust organizations and corporations that much – I mean Africa, India, the Eastern Europe, or Russia. It's not about the places where people are really rich. Blockchain's opportunities are the highest in the countries that haven't reached that level yet" [4].

In the following, we introduce concrete use-cases where blockchain technology can contribute to solving most pressing citizens and governments concerns. We present three families of use-cases, where the first focuses on leveraging the historical objective of blockchain infrastructure, the second considers the features of distribution and transparency of the database, and the third explores advanced automation services.

3.1 Cryptocurrencies and Payments

Historically, blockchain technology is associated with currency. Indeed, after Bitcoin, the main applications of blockchain were the creation of new cryptocurrencies, including Litecoin, Dogecoin, Namecoin.

Generally, fragile economies in developing countries may not be ready for currencies that are "mined" (almost out of thin air) based on computing power. Nevertheless, cryptocurrency systems have desirable properties for solving important issues in developing countries, especially for tracking money flows. Thus, blockchain can be leveraged to develop *digital fiat currency* systems which will be systematically pegged to the national currency (i.e., one would give 1 token from fiat currency in exchange of one crypted digital token). Such digital currencies can be used to properly implement transparent crowdfunding, follow and assess the use of development aid. Finally, cryptocurrencies, because, if needed, they can be traced back in all its exchange paths, can be leveraged to ensure tax contributions by all merchants. This last possibility could be instrumental in more rapidly transforming the informal economy of developing countries into a formal one.

The main advantages that can be gained with this application of blockchain are the reduction of cost for handling cash, collecting taxes, as well as the speed for transactions and reporting.

3.2 Identification/Authentication

Current development of blockchain applications beyond cryptocurrencies, focus on the immutability of its database. In developing countries, this property can be leveraged to solve rooted problems related to identification and authentication based on immutable registries. For example, a common concern lies in tracking land ownership. Another concern for promoting democracy is the count of citizen's vote, ensuring that it is protected and non-temperable.

The main advantage that such applications bring is their openness and flexibility properties, with possibilities to empower users and deliver new business models.

3.3 Smart Contracts

Recently, a new term, *Blockchain 2.0* [6], has been coined to refer to new kinds of applications of the distributed blockchain database. Smart contracts are one possible implementation of this second-generation programmable blockchain which come with "a programming language that allows users to write more sophisticated smart contracts, thus creating invoices that pay themselves when a shipment arrives or share certificates which automatically send their owners dividends if profits reach a certain level" [7].

In developing countries, smart contracts can be heavily relied upon to avoid the dictatorship of intermediates in handling insurance claims or dealing with notary needs. For example, they could serve to manage family trusts and reduce the number of issues that are increasingly seen around inheritance sharing.

The main advantages that this type of applications provide are the autonomy of execution as well as the irrefutability of the transactions. Speed and cost are also incidentally improved.

4 Consensus Models

The consensus mechanism is the most critical feature of a blockchain. It ensures that all participants involved in maintaining a distributed ledger are on the same page, and further enables the distributed network of peers to remain reliable for circulating information even if some of the peers keep failing.

4.1 Recap: Byzantine Generals Problem

To better summarize the challenge to reach consensus, we recall the Byzantine generals problem detailed by Lamport et al. [5]. The following is an excerpt from the seminal 1982 paper on byzantine fault tolerance:

"Several divisions of the Byzantine army are camped outside an enemy city, each division commanded by its own general. The generals can communicate with one another only by messenger. They must decide upon a common plan of action. However, some of the generals may be traitors, trying to prevent the loyal generals from reaching agreement. The generals must have an algorithm to guarantee that:

C_1: All loyal generals decide upon the same plan of action.

The loyal generals will all do what the algorithm says they should, but the traitors may do anything they wish. The algorithm must guarantee condition C_1 regardless of what the traitors do. The loyal generals need to reach agreement and agree on a reasonable plan that also ensures that

C_2: A small number of traitors cannot cause the loyal generals to adopt a bad plan"

Such an algorithm is known as the *consensus protocol.* The goal of this protocol in a public blockchain network is indeed to let many different computing nodes to agree on the current state of the blockchain even though they don't trust each other or any central authority. Therefore, the protocol serves two roles: (a) to ensures that the added block in a blockchain is the one and only version of the truth (i.e., the actual, un-tampered, transaction that was requested), and (b) to prevent adversarial nodes, even when they are computationally powerful, from derailing the system and successfully forking the chain (i.e., creating another chain of transactions). In the remainder of this section, we present a few common protocols implemented in existing blockchain infrastructure initiatives.

4.2 State-of-the-Art Consensus Protocols

Proof-of-Work (PoW) – In this pioneer protocol [8,9], participating nodes "work" to solve difficult mathematical problems, and then broadcast the results in the network. PoW use the number and difficulty of solutions being found to measure what percentage of the network agrees on the state of the blockchain.

To prevent legitimate nodes from coming to agreement about the state of the blockchain, an adversary must control a large portion of the involved computing power in order to seed his/her opinion as the real consensus, or work for perpetual disagreement in the network.

Bitcoin was the first to implement this consensus protocol in a real-world case for cryptocurrencies [10]. Although the requirement for actual resources (computing power, electricity, time) is a strong point for PoW protocols to guarantee efficacy in deterring adversaries, it is also the weak point for efficiency since it involves a constant expenditure and resources to work normally (i.e., even when no one is actually trying to interfere with the blockchain).

Proof-of-Stake (PoS) – The energy inefficiency of PoW protocols have motivated a new consensus protocol [11,12] where agreement within the blockchain network is not measured on the basis of the computing power that is spent to validate a blockchain state, but rather on the basis of the amount of cryptocurrencies that are in agreement with the current state. Thus, a block in the blockchain is now created by a node selected in a deterministic, i.e., pseudo-random, way with a probability that is correlated with its wealth (i.e., its stake). Therefore, mining is done by stakeholders in the ecosystem who have the strongest incentives to be good stewards of the system [13]. PoS has been implemented for the Ethereum blockchain.

PoS-based currencies have been shown to be up to several times more cost-effective than PoW currencies. Unfortunately, simulations have already proven theoretically that simultaneous forging of several chains is possible [14] and can be abused to attempt to double-spend "for free".

Byzantine Fault Tolerant (BFT) – Since blockchain are distributed systems, they can leverage the state-of-the-art practical byzantine fault tolerance (PBFT) [15] for the consensus mechanism. Each blockchain node publishes its public key, and messages coming through the node is signed by the node to verify its format. If a majority of responses are identical, then the blockchain network consensually agrees that the message is a valid transaction.

PBFT was originally designed for low-latency storage systems, and its properties have been argued to be valuable in blockchain use-cases where digital asset-based platforms do not require a large amount of throughput, but instead see a large number of transactions [16]. Hyperledger[3] is an example of blockchain system that relies on PBFT.

Federated Byzantine Agreement (FBA) – Implemented in the Stellar Consensus protocol [17] the FBA model relies on a small sets of trusted parties to achieve quorum: the assumption is that a given node "knows" a subset of nodes in the network. Thus, nodes in the blockchain network agree to accept information from a group of nodes (a.k.a, quorums or slices which are believed will not collude among themselves). Consensus is then formed as these quorums form collective agreement on the information.

Proof of Elapsed Time (PoET) – Introduced by Intel focusing on efficiency, PoET uses secure CPU instructions in processor chips to ensure the safety and randomness of a leader election without requiring costly investment on power and/or hardware. Concretely, every node in the blockchain network requests a wait time from an trusted function. The node with the shortest wait time for a given transaction block is then elected validation leader. The algorithm is said to meet the criteria of a good lottery algorithm where leader role can be bestowed randomly to any of the node with a distribution similar to lottery algorithms where the probability to be selected is proportional to the resources contributed (i.e., how many chips with the trusted functions you have).

The main limitation of the PoET algorithm is that it implicitly moves the trust problem to a single authority, the chip maker, which implements the trusted functions. Nevertheless, PoET can be effective in a private enterprise blockchain setup.

Many other consensus protocols have been directly derived from Proof-of-Work and Proof-of-Stake to address some of their limitations (mainly security guarantees). Among them we can quickly cite Proof-of-Activity (PoA) [18], Proof-of-Burn (PoB) [19] and Proof-of-Capacity (PoC) [20]. We encourage the reader to find more details on these protocols in the literature. We will focus our comparison on the mainstream protocols presented above.

4.3 Comparative Assessment

In this section we discuss a high-level comparison of consensus protocols based on several essential blockchain properties that can be related to the context of developing countries. We first enumerate features regrouped in families following the assessment of Vukolic [16].

[3] https://www.hyperledger.org/.

- *Identity management*: This feature relates to how blockchain node identities are managed by the consensus protocols. For example, while PoW implements an entirely *decentralized control* allowing anyone to participate in the blockchain, BFT protocols typically requires every node to know the entire set of its peer nodes participating in the blockchain. The first type of protocols are useful for creating "public" **permissionless** blockchains, while the latter allow to create **permissioned** blockchain.
- *Scalability*: This feature relates to the numbers of nodes that can participate in the blockchain and of clients that can simultaneously send transactions to the system.
- *Performance*: This regroups features related to the latency (how fast are transactions), throughput (how many transactions per unit of time can be submitted) and the amount of power consumed. As an example, Bitcoin shows very limited performance: up to 7 transactions per second, 1-h latency with 6 block confirmation. Furthermore, according to a bitcoin mining-farm operator, energy consumption totaled 240 kWh per bitcoin in 2014 (i.e., approximately the equivalent of 16 gallons of gasoline) [23].

4.4 Property-Based Comparison

Although the properties listed above are not exhaustive for characterizing Blockchain consensus protocols, they allow to differentiate clearly most state-of-the-art algorithms, and are assessment dimensions that are representative for the context of developing countries.

Table 1 provides a comparative listing of the protocols. Positive markings +++, ++ and + indicates that the protocol more or less takes this property into account. Negative markings ---, -- and -, on the other hand, indicate that the design of the consensus protocol was more or less detrimental to this aspect. For example *energy performance* of PoW will be marked as --- while BFT protocol, which shows a very low latency, will be marked as +++ for this aspect.

Table 1. Blockchain consensus protocols

Feature		Consensus protocols				
		PoW	PoS	BFT	FBA	PoET
Decentralized control		+++	+++	---	+++	-
Scalability	Nodes	+++	+++	--	+	+
	Clients	+++	+++	+++	+++	+++
Performance	Latency	---	+	+++	+	++
	Throughput	--	+	+++	+++	++
	Energy	---	++	+++	+++	+++

4.5 Constraints of Developing Countries

Developing countries, including those in sub-Saharan, have specific constraints related to network latency, to the trustworthiness of governments (and their infrastructures), to energy scarcity, and to increasing demographics.

Decentralized control is an essential feature for any blockchain that must truly offer trust to citizens and stakeholders. Unfortunately, PoW, wwich is the most adapted for public, permissionless, fully decentralized blockchain, has numerous caveats with regards to computing power and energy consumption, as well as with regards to latency and throughput. Similarly, although BFT presents desirable properties for latency, its low throughput makes it less interesting for many use cases.

Roadmap: As can be viewed in the comparison table of previous section, all consensus protocols present different strengths and weaknesses. Some consensus protocols are further token-based (e.g., cryptocurrency-oriented blockchains) while some may not be (e.g., general purpose blockchains). It is thus necessary when contemplating the implementation of a blockchain application to consider the expected scenarios and the contextual constraints. This requires a very good understanding of blockchain fundamentals, as well as practical hands-on experience into the inner working of consensus protocols. This work is a stepping stone towards eliciting all parameters to take into account when selecting a blockchain system: e.g., for an online voting system in developing countries, given the instability and corruption risks, it may be suitable to consider only fully decentralized control. For implementing payment systems on the other hand, it may be interesting to focus on permissioned, low-latency, high-throughput blockchains.

5 Insights and Related Work

In January 2017, in response to Sarah Underwood's article 'Blockchain Beyond Bitcoin' [21], Ingo Mueller pointed that many blockchain proponents fail to raise the right questions. He then went on to protest that "Instead of focusing on *what block-chain could do*, one should address *what blockchain can do better than other technologies*. As described above, the underlying consensus algorithms even predate the blockchain phenomenon. For example, Proof-of-work-alike protocol was proposed 15 years before the Bitcoin, while the recent Hyperledger system is developed on top of PBFT which was developed for operating system storage management.

Our work is a step towards asking the right questions about blockchain for developing countries. This article is a first of a series where we aim to explore the applicability of blockchain with regards to developing countries contents. We have so far focused on technical constraints. However, as Mueller pointed out, although blockchain is often credited with the ability to solve tough longstanding problems (e.g., digital identity), one should keep in mind that various attempts to solve such challenges, including state-of-the-art approaches (e.g., Public Key infrastructure for digital identity) “have often failed due to non-technical aspects of human relationships, including trust, social, cognitive, economic, and even physical”.

With regards to related work, although there is currently a number of blog and websites providing details on the blockchain technology, very few academic work provide a comprehensive view of the current state-of-the-art on blockchain consensus protocols. Jesse et al. [22] have recently presented a systematic literature review of research on blockchain technology. However, the particular of consensus protocols has not been addressed.

6 Conclusion and Future Work

Development of blockchain across various industries is an opportunity for developing countries research and practice around ICT for development. Nevertheless, there is a huge gap between the promise of blockchain and its eventual real impact on our processes. We have contributed in this work with a first look at what options present themselves today with regards to the consensus protocols, the core element of blockchain.

In this article we have focused on the theory of how the protocols are designed. In future work, we plan to experiment with the available software for a better view of the technological readiness level of the different systems. We further plan to enumerate the various non-technical aspects in our societies which can challenge the use of blockchain, and for which there may be a need to develop ad-hoc consensus protocol that is culturally-aligned [24] with developing countries context.

References

1. Latour, B.: Technology is society made durable. Sociol. Rev. **38**(1–suppl), 103–131 (1990)
2. Bell, D.: The coming of the post-industrial society. Educ. Forum. **40**(4), 574–579 (1976)
3. Brito, J., Castillo, C.: Bitcoin: A Primer for Policymakers. Mercatus Center at George Mason University, Arlington (2013)
4. Vitalik buterin about ethereum, smart contracts, and himself, May 2016. https://goo.gl/C58nJZ
5. Lamport, L.: The byzantine generals problem. ACM Trans. Program. Lang. Syst. **4**(3), 382–401 (1982). http://dl.acm.org/citation.cfm?id=357176
6. Bheemaiah, K.: Block chain 2.0: the renaissance of money. Wired, January 2015
7. Economist Staff: Blockchains: the great chain of being sure about things. The Economist, 31 October 2015. https://goo.gl/PwLDsw
8. Dwork, C., Naor, M.: Pricing via processing or combatting junk mail. In: Brickell, E.F. (ed.) CRYPTO 1992. LNCS, vol. 740, pp. 139–147. Springer, Heidelberg (1993). https://doi.org/10.1007/3-540-48071-4_10
9. Jakobsson, M., Juels, A.: Proofs of work and bread pudding protocols. In: Communications and Multimedia Security, pp. 258–272. Kluwer Academic Publishers (1999)

10. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system, October 2008. https://bitcoin.org/bitcoin.pdf
11. Popov, S.: A probabilistic analysis of the Nxt forging algorithm. Ledger **1**, 69–83 (2016). https://doi.org/10.5195/LEDGER.2016.46. ISSN 2379–5980
12. Vitalik, B.: What proof of stake is and why it matters. Bitcoin Mag
13. Narayanan, B.: Bitcoin and Cryptocurrency Technologies. Princeton University Press, Princeton (2016)
14. Chepurnoy, A.: PoS forging algorithms: formal approach and multibranch forging. https://www.scribd.com/doc/248208963/Multibranch-forging
15. Castro, M., Liskov, B.: Practical byzantine fault tolerance. In: OSDI, vol. 99 (1999)
16. Vukolić, M.: The quest for scalable blockchain fabric: proof-of-work vs. BFT replication. In: Camenisch, J., Kesdoğan, D. (eds.) iNetSec 2015. LNCS, vol. 9591, pp. 112–125. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-39028-4_9
17. Mazieres, D.: The stellar consensus protocol: federated model for internet level consensus. Stellar Development Foundation (2015)
18. Bentov, I.: Proof of activity: extending Bitcoin's proof of work via proof of stake. ACM SIGMETRICS Perform. Eval. Rev. **42**(3), 34–37 (2014)
19. P4Titan: Slimcoin: a peer-to-peer crypto-currency with proof-of-burn, May 2014. http://www.slimcoin.club/whitepaper.pdf
20. BURST's proof of capacity mining. Bitcoin Talk. https://bitcointalk.org/index.php?topic=731923.0
21. Underwood, S.: Blockchain beyond bitcoin. Commun. ACM **59**(11), 15–17 (2016)
22. Yli-Huumo, J., et al.: Where is current research on blockchain technology? A systematic review. PLoS one **11**(10) (2016)
23. CoinDesk: Carbon footprint of bitcoin. http://www.coindesk.com/carbon-footprint-bitcoin/
24. Ouoba, J., Bissyandé, T.F.: Leveraging the cultural model for opportunistic networking in sub-saharan Africa. In: Jonas, K., Rai, I.A., Tchuente, M. (eds.) AFRICOMM 2012. LNICST, vol. 119, pp. 163–173. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-41178-6_17