Proof of Behavior

Paul-Marie Grollemund
Université Clermont Auvergne, LMBP UMR 6620, Aubière, France
paul_marie.grollemund@uca.fr

Pascal Lafourcade[1]
Université Clermont Auvergne, LIMOS UMR 6158, Aubière, France
pascal.lafourcade@uca.fr

Kevin Thiry-Atighehchi
Université Clermont Auvergne, LIMOS UMR 6158, Aubière, France
kevin.atighehchi@uca.fr

Ariane Tichit
Université Clermont Auvergne, Cerdi UMR 6587, Clermont-Ferrand, France
ariane.tichit@uca.fr

Abstract

Our aim is to change the *Proof of Work* paradigm. Instead of wasting energy in dummy computations with hash computations, we propose a new approach based on the behavior of the users. Our idea is to design a mechanism that replaces the Proof of Work and that has a positive impact on the world and a social impact on the behaviors of the citizens. For this, we introduce the notion of *Proof of Behavior*. Based on this notion, we present a new cryptocurrency, called *EcoMobiCoin*, that encourages the ecological behavior in the mobility of the citizens.

2012 ACM Subject Classification Security and privacy

Keywords and phrases Proof of behavior, Blockchain, Security

Digital Object Identifier 10.4230/OASIcs.Tokenomics.2020.11

Category Short Paper

1 Introduction

Bitcoin [12] was the beginning of a digital revolution and it is also the birth of the blockchain technology (see [3] for an overview). The security of this technology relies on the concept of Proof of Work (PoW). In order to validate a transaction, a miner needs to produce a PoW. In Bitcoin, a PoW is the computation of an objective of hash, which is finding a number that satisfies an inequation. Finding this number requires to compute thousands of hash functions. PoW is one of the main negative aspect of this technology since it is highly energy consuming [13]. Moreover in the case of Bitcoin, the performed hash computations are really useless. Our goal is to design an alternative to PoW, for this purpose we introduce the notion of *Proof of Behavior* (PoB).

Contributions. We present the notion of PoB, the idea is to incentivize citizens to have responsible behaviors instead of doing useless computations as in PoW. Our aim is to replace PoW by PoB. We propose a first application to design a new cryptocurrency for the mobility, called *EcoMobiCoin* for Ecological and Collaborative Mobility Coin. If you can prove that you are biking or walking or using public transportation to go somewhere instead of using your car, or if you can prove that you are using your car with some passengers to go to

[1] Corresponding author

somewhere, you are generating a Proof of Behavior for eco-responsible mobility and then creating new *EcoMobiCoins*. This approach aims at facilitating the energy transition that is a key point of the next years.

Related Work. Many works aim at improving existing blockchains or cryptocurrencies as for instance [2, 8, 9, 11, 5]. There are many works that use blockchain to develop new applications as for instance online secure e-voting [7] or online secure e-auction [4] or even proof of identity [10]. Moreover many cryptocurrencies have been designed after Bitcoin, as for example Ethereum, PeerCoin, PrimeCoin etc. In [1], the authors proposed a classification in 4 categories of the existing cryptocurrencies:

1. Scam: These are cryptocurrencies that are designed quickly, not secure and their only goal is to convince people to invest money in these coins in order that the designers earn some money. They are usual quickly identified by the community as *scams* and they disappear.
2. Clone: These cryptocurrencies are just some clones of Bitcoin to particular purpose as for instance PokerCoin for poker players.
3. New goal: Here the aim is to change the goal of the cryptocurrencies, for instance PrimeCoin aims at discovering new Cunningham chains that are mathematical advances in prime numbers. Two other examples are CureCoin or FoldingCoin that aim at using the computation to solve medicine problems.
4. New consensus: The goals of such cryptocurrencies is to propose different consensus. The first initiative was PeerCoin that introduces the notion of *Proof of Stake*. Some other initiatives exist like SpaceMint [14] that introduces the Proof of Space or PermaCoin that introduces the notion of *Proof of retrievability*.

Our concept of Proof of Behavior is clearly at the intersection of the two last categories. We are proposing a new goal and at the same time a new paradigm. The closest existing cryptocurrency to a PoB is SolarCoin[2]. The goal of SolarCoin is to "*incentivize solar electricity by rewarding the generators of solar electricity*". They reward solar energy producers with blockchain-based digital tokens at the rate of 1 SolarCoin (SLR) per 1 MWh of solar energy produced. More precisely, users produce solar energy and provide a proof of this production to the SolarCoin Foundation that approves its behavior. Then users receive SolarCoins and can use them. The experience of SolarCoin started in 2014 clearly shows that it is an economic model that works.

Concerning our application to mobility, the closed project is MobiCoin presented in 2018 at the Mobile World Congress in Barcelona, Spain by Mercedes-Benz to reward conductors that have an ecological drive[3]. They aim at collecting users data and rewarding some of them with Mobicoins. Unfortunately in 2020, this project is not yet used and it is difficult to obtain any information on its status. However our aim is different, since we reward collaborative mobility and zero emission mobility like walking and biking.

Outline. We first explain the concept of Proof of Behavior in the next section. Then we apply PoB to design EcoMobiCoin, before concluding.

---

[2] `https://solarcoin.org/`

[3] Visited the 18 January 2019,
`https://www.ellulschranz.com/mercedes-benz-invested-blockchain-technology`

2 Proof of Behavior

We first present the idea of PoB, then the differences with PoW and finally the necessary conditions for such system to work.

The idea of Proof of Behavior

The main idea behind PoB is that if users are doing some concrete actions in the real world and they can provide a proof of their actions then these PoB are used to generate new coin.

This is clearly a comeback to the essence of the revolution launched by Bitcoin: a system based on a decentralized, collaborative, distributed consensus to validate transactions and create new coins. Moreover, the main innovation in PoB is that it is not consuming time and energy to useless things.

Comparison

Comparing to the PoW the actions of the users in the real world allow everyone to participate to the coin generation. It is not necessary to spend money in specialized material for mining, as in Bitcoin, since it is user's behavior that gives the power to mine coins. With this change of paradigm everyone can decide to select which behavior he wants to have in order to contribute to a global improvement of the society.

The main difference is that valid proofs of behavior are used to generate new coins. It means that nothing is wasted, because PoB are positive actions for the society, so it does not matter if they are realized but not used to generate coins. It is not necessary that the behavior is more and more difficult according to the number of persons, as in Bitcoin where the system adapts itself in order that only few transactions are validated every ten minutes. This implies in Bitcoin that the cost of the transactions is more and more expensive, because everyone wants to win the race to find the nonce to solve the objective of hash and because the difficulty is increasing. In a proof of behavior any action can contribute to the generation of new coins.

Conditions

In Bitcoin, the revolution comes with a main innovation: decentralization. It means that central entities are not needed anymore to create currencies. It implies that everyone can mine and not only the financial institutions can generate money. A necessary condition in this system is that everyone can also verify the results of the computations of the miners since everything is publicly distributed. The same mechanism is present in PoB: everything is publicly verifiable and written in the blockchain.

The key point is to determine who has the right to write in the blockchain and how? In PoB, this right is not given to miners that have a lot of computational resources as in Bitcoin but it is, in some sense, shared between the three following actors:

User: Person who does some transactions by sending coins to someone.

ProofMaker: Person who realizes a PoB.

Verifier: Person who verifies the validity of PoB and the validity of transactions. Then he writes in the blockchain the verified PoB and transactions.

To summarize, everyone can be a ProofMaker and generate PoB. Everyone can verify the validity of some PoB and then uses these valid PoB to register on the blockchain some valid transactions. To compare with Bitcoin where the miners perform the verification of the

validity of the transactions and also the proof of work, we have the verifiers that only verify the validity of the transactions and of the PoB. Moreover, the proof of work are done by the ProofMaker by having positive behaviors.

Moreover we add the fact that a PoB has a validity period. We use the fact that a behavior is something that is done at some precise time, then a PoB has a validity period of few hours (for instance 24h) to be used by a verifier to generate new coins. We can also add such constraints on the transactions, if a transaction is not written in the blockchain after few hours (it can also be for instance 24h) then the transaction is removed from the pool of transactions. Indeed this is implicitly done in Bitcoin. In this setting, in order to validate a transaction, a verifier needs to have verified a proof of behavior and the validity of some transactions.

Concerning the blockchain, we can imagine at least three possibilities:

Private: A consortium of partners like public transportation, cities, government or industrial can just vote or validate the verified associations PoB and transactions.

Public: Every verifier can write in the blockchain, the longest chain having the highest behavior score[4] is the main chain. We also add the fact that all blocks written after 24h in the main chain cannot be changed. This point limits the possibilities of fork.

Hybrid: A mix between public and private blockchain is also possible.

Each time a verifier writes a block, he creates one coin. It is important that this reward remains a constant and depends neither on the transactions nor on the PoB. At the same time, the owners of the PoB used by the verifier also receive one coin that is fairly split between all PoB owners used by the verifier.

The concept of Proof of Behavior is clearly an important innovation toward a new economical system where everyone is responsible of its acts.

3 Application: EcoMobiCoin

One of the first application of PoW is the design of a cryptocurrency to incentivize less emission in the transportation. For this, the first task is to define what are the behaviors that we want to promote. We identify four main behaviors: walking, biking, using public transportation and carpooling.

For each situation a proof of behavior is a real GPS trace that can be collected using a simple smartphone. For this we need a signature of the device that is unique. This is necessary in order that a device can be identified and not be used in several traces at the same time. The trace should also prove that the user was walking or biking or driving. For this some statistical algorithms [6] are used to determine if a user's GPS trace is a valid trace of the following behaviors: walking, biking or driving. These algorithms are public and used by verifiers to determine the trace validity. The verification is part of the work of the verifier and then he can write to the blockchain.

Concerning the public transportation, the proof contains two GPS traces: one for the user and for instance one for the tram line. Here other algorithms are used to prove that the two traces are similar. Finally for the carpooling, a PoB also include several GPS traces. Of course each proof of behavior is awarded by some EcoMobiCoins, so a PKI infrastructure is used to ensure all the cryptographic mechanisms as in any blockchain.

[4] This score depends of which behaviors the cryptocurrency wants to emphasize.

In comparison to other economic systems based on a cryptocurrency, PoB allows to define a range of ways to generate coins. Cryptocurrencies as SolarCoin are focusing on only one behavior or only one small subset of the society. On the opposite, a PoB-based cryptocurrency is affordable to a large part of the population. As a consequence, an economic system based on EcoMobiCoin is more robust and is likely to include a wider public embracing.

4 Conclusion

We change the paradigm of Proof of Work and we introduce the concept of Proof of Behavior. This allows us to incentivize behaviors of users. We propose one first application for transportation with the design of EcoMobiCoin. Many applications can be envisaged based on the notion of Proof of Behavior. We can imagine several other applications in order to reward good usages as soon as it is possible to construct a verifiable proof of behavior. In each application it is important to design adapted cryptographic primitives in order to have a sufficient security level in how the proofs of behavior are produced.

References

1. A. Tichit, P. Lafourcade, and V. Mazenod. Les monnaies virtuelles décentralisées sont-elles des dispositifs d'avenir ? *revue Interventions Economiques*, 2017.
2. E. Anceaume, R. Ludinard, M. Potop-Butucaru, and F. Tronel. Bitcoin a Distributed Shared Register. In *19th Intl. Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS)*, 2017.
3. J-G. Dumas, P. Lafourcade, A. Tichit, and S. Varette. *Les blockchains en 50 Questions, comprendre le fonctionnement et les enjeux de cette technologie innovante*. Dunod, 2018.
4. P. Lafourcade, M. Nopere, J. Picot, D. Pizzuti, and E. Roudeix. Security analysis of auctionity: a blockchain based e-auction. In *12th International Symposium on Foundations and Practice of Security - Revised Selected Papers*, FPS, 2019.
5. I. Abraham, G. G. Gueta, D. Malkhi, M. K. Reiter, and M. Yin. Hot-stuff the linear, optimal-resilience, one-message BFT devil. *CoRR*, abs/1803.05069, 2018. `arXiv:1803.05069`.
6. P. C. Besse, B. Guillouet, J. Loubes, and F. Royer. Review and perspective for distance-based clustering of vehicle trajectories. *IEEE Transactions on Intelligent Transportation Systems*, 17(11):3306–3317, November 2016. `doi:10.1109/TITS.2016.2547641`.
7. Marwa Chaieb, Mirko Koscina, Souheib Yousfi, P. Lafourcade, and Riadh Robbana. Dabsters: a privacy preserving e-voting protocol for permissioned blockchain. In *16th International Colloquium on Theoretical Aspects of Computing*, ICTAC, 2019.
8. A. Durand, E. Anceaume, and R. Ludinard. STAKECUBE: Combining Sharding and Proof-of-Stake to build Fork-free Secure Permissionless Distributed Ledgers. In *7th International Conference, (NETYS)*, 2019. URL: `https://hal.archives-ouvertes.fr/hal-02078072`.
9. A. Kiayias, A. Russell, B. David, and R. Oliynykov. Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol. In *37th Annual International Cryptology Conference*, CRYPTO, 2017.
10. Marius Lombard-Platet and P. Lafourcade. Get-your-id: Decentralized proof of identity. In *12th International Symposium on Foundations and Practice of Security - Revised Selected Papers*, FPS, 2019.
11. S. Micali. ALGORAND: the efficient and democratic ledger. *CoRR*, abs/1607.01341, 2016. `arXiv:1607.01341`.
12. S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2009. URL: `http://www.bitcoin.org/bitcoin.pdf`.

13 K.J. O'Dwyer and D. Malone. Bitcoin mining and its energy footprint. *IET Conference Proceedings*, pages 280–285(5), 2014. URL: `https://digital-library.theiet.org/content/conferences/10.1049/cp.2014.0699`.

14 Sunoo Park, Albert Kwon, Georg Fuchsbauer, Peter Gazi, Joël Alwen, and Krzysztof Pietrzak. Spacemint: A cryptocurrency based on proofs of space. In *Financial Cryptography and Data Security - 22nd International Conference, FC 2018*, volume 10957, pages 480–499. Springer, 2018.