



HAL
open science

Proof of Behavior

Paul-Marie Grollemund, Pascal Lafourcade, Kevin Thiry-Atighehchi, Ariane Tichit

► **To cite this version:**

Paul-Marie Grollemund, Pascal Lafourcade, Kevin Thiry-Atighehchi, Ariane Tichit. Proof of Behavior. The 2nd Tokenomics Conference on Blockchain Economics, Security and Protocols, Oct 2020, Toulouse, France. hal-02559573

HAL Id: hal-02559573

<https://hal.science/hal-02559573v1>

Submitted on 30 Apr 2020

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.




Distributed under a Creative Commons Attribution 4.0 International License

1 Proof of Behavior

2 Paul-Marie Grollemund

3 Université Clermont Auvergne, LMBP UMR 6620, Aubière, France
4 paul_marie.grollemund@uca.fr

5 Pascal Lafourcade¹ 

6 Université Clermont Auvergne, LIMOS UMR 6158, Aubière, France
7 pascal.lafourcade@uca.fr

8 Kevin Thiry-Atighehchi

9 Université Clermont Auvergne, LIMOS UMR 6158, Aubière, France
10 kevin.atighehchi@uca.fr

11 Ariane Tichit

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

14 Abstract

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

21 **2012 ACM Subject Classification** Security and privacy

22 **Keywords and phrases** Proof of behavior, Blockchain, Security

23 **Digital Object Identifier** 10.4230/LIPIcs.CVIT.2016.23

24 1 Introduction

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

34 **Contributions:** We present the notion of PoB, the idea is to incentivize citizens to have
35 responsible behaviors instead of doing useless computations as in PoW. Our aim is to replace
36 PoW by PoB. We propose a first application to design a new cryptocurrency for the mobility,
37 called *EcoMobiCoin* for Ecological and Collaborative Mobility Coin. If you can prove that
38 you are biking or walking or using public transportation to go somewhere instead of using
39 your car, or if you can prove that you are using your car with some passengers to go to
40 somewhere, you are generating a Proof of Behavior for eco-responsible mobility and then
41 creating new *EcoMobiCoins*. This approach aims at facilitating the energy transition that is
42 a key point of the next years.

¹ Corresponding author



43 **Related Work:** Many works aim at improving existing blockchains or cryptocurrencies
 44 as for instance [2, 8, 9, 11, 5]. There are many works that use blockchain to develop new
 45 applications as for instance online secure e-voting [7] or online secure e-auction [4] or even
 46 proof of identity [10].

47 Moreover many cryptocurrencies have been designed after Bitcoin, as for example Eth-
 48 ereum, PeerCoin, PrimeCoin etc. In [1], the authors proposed a classification in 4 categories
 49 of the existing cryptocurrencies:

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

64 Our concept of Proof of Behavior is clearly at the intersection of the two last categories.
 65 We are proposing a new goal and at the same time a new paradigm. The closest existing
 66 cryptocurrency to a PoB is SolarCoin². The goal of SolarCoin is to “*incentivize solar electricity*
 67 *by rewarding the generators of solar electricity*”. They reward solar energy producers with
 68 blockchain-based digital tokens at the rate of 1 SolarCoin (SLR) per 1 MWh of solar energy
 69 produced. More precisely, users produce solar energy and provide a proof of this production
 70 to the SolarCoin Foundation that approves its behavior. Then users receive SolarCoins
 71 and can use them. The experience of SolarCoin started in 2014 clearly shows that it is an
 72 economic model that works.

73 Concerning our application to mobility, the closed project is MobiCoin presented in 2018
 74 at the Mobile World Congress in Barcelona, Spain by Mercedes-Benz to reward conductors
 75 that have an ecological drive³. They aim at collecting users data and rewarding some of them
 76 with Mobicoin. Unfortunately in 2020, this project is not yet used and it is difficult to obtain
 77 any information on its status. However our aim is different, since we reward collaborative
 78 mobility and zero emission mobility like walking and biking.

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

81 **2 Proof of Behavior**

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

² <https://solarcoin.org/>

³ Visited the 18 January 2019,

<https://www.ellulschranz.com/mercedes-benz-invested-blockchain-technology>

84 **The idea of Proof of Behavior**

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

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

91 **Comparison**

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

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

106 **Conditions**

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

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

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

117 **ProofMaker:** Person who realizes a PoB.

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

120 To summarize, everyone can be a ProofMaker and generate PoB. Everyone can verify
121 the validity of some PoB and then uses these valid PoB to register on the blockchain some
122 valid transactions. To compare with Bitcoin where the miners perform the verification of the
123 validity of the transactions and also the proof of work, we have the verifiers that only verify
124 the validity of the transactions and of the PoB. Moreover, the proof of work are done by the
125 ProofMaker by having positive behaviors.

126 Moreover we add the fact that a PoB has a validity period. We use the fact that a
127 behavior is something that is done at some precise time, then a PoB has a validity period of

23:4 Proof of Behavior

128 few hours (for instance 24h) to be used by a verifier to generate new coins. We can also add
129 such constraints on the transactions, if a transaction is not written in the blockchain after
130 few hours (it can also be for instance 24h) then the transaction is removed from the pool of
131 transactions. Indeed this is implicitly done in Bitcoin.

132 In this setting, in order to validate a transaction, a verifier needs to have verified:

- 133 ■ a proof of behavior
- 134 ■ the validity of some transactions.

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

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

138 **Public:** Every verifier can write in the blockchain, the longest chain having the highest
139 behavior score⁴ is the main chain. We also add the fact that all blocks written after 24h
140 in the main chain cannot be changed. This point limits the possibilities of fork.

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

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

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

148 **3 Application: EcoMobiCoin**

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

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

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

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

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

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. URL: <http://arxiv.org/abs/1803.05069>, 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, Nov 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. URL: <http://arxiv.org/abs/1607.01341>, 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. Bitcoin mining and its energy footprint. *IET Conference Proceedings*, pages 280–285(5). 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.