

Proof of Behavior

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

Tokenomics
Toulouse, France, October 26-27 2020



Outline

Introduction

Related Works

Proof of Behavior

EcoMobiCoin

Conclusion

Introduction

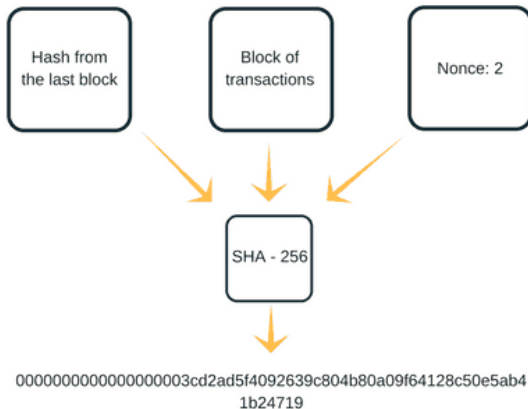
Bitcoin relies on the concept of Proof of Work



Introduction

Proof of Work in Bitcoin

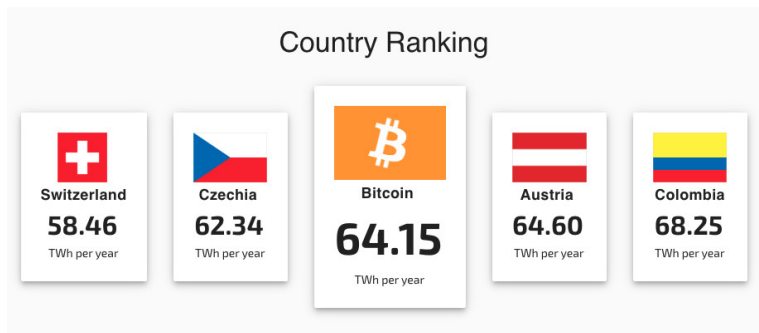
- ▶ Find a number satisfying an objective hash



Introduction

Proof of Work in Bitcoin

- ▶ And highly energy consuming



Introduction

Proof of Work

- ▶ Useless computations



Introduction

Examples of Blockchain-based applications

- ▶ Online secure e-voting
- ▶ Online secure e-auction
- ▶ Identity management
- ▶ Document certification and tracking

Introduction

Post-Bitcoin cryptocurrencies (Ethereum, PeerCoin, etc)



Introduction

Classification in 4 categories

- ▶ Scam
- ▶ Clone
 - Special purposes, e.g. PokerCoin
- ▶ New goal
 - Solving useful puzzles, e.g. PrimeCoin, CureCoin, FoldingCoin
- ▶ New consensus
 - *Proof of Stake, Proof of Space, Proof of Retrievability, Proof of Elapsed Time*

Introduction

Our aim: Concretize an alternative paradigm serving other purposes than the consensus

- ▶ A new cryptocurrency : **EcoMobiCoin**
- ▶ A new consensus
- ▶ A new goal : **Incentivization of green behaviors**

Related Work

Closest projects

▶ SolarCoin



*"incentivize solar electricity
by rewarding the generators
of solar electricity"*

▶ MobiCoin

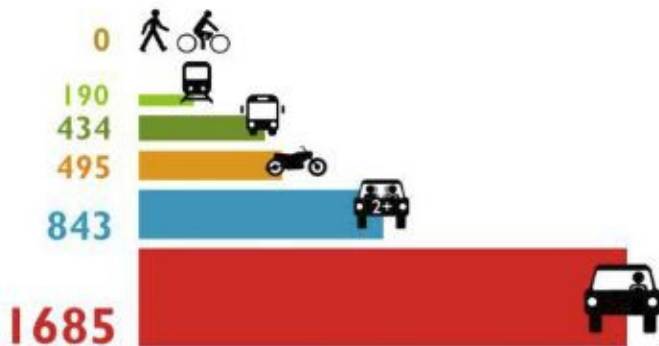
- Project by Mercedes-Benz
- Goal: collecting users data and rewarding car drivers having an ecological drive
- Lack of available information



EcoMobiCoin rewards

- ▶ Collaborative mobility
- ▶ Zero emission mobility

Greenhouse Gas Emissions Due to Personal Transportation



Comparison of greenhouse gas emissions in kg (CO² equivalent) by mode of travel for a 13 km commute to work
(source: ADEME, Calculette eco-déplacements, 2015)

Proof of Behavior (PoB)

Idea behind PoB: Proving positive actions in the real world enables the generation of coins

PoB in replacement of PoW

- ▶ No specialized hardware required for mining
- ▶ Anyone can select a green behavior she wants to conform to generate new coins
- ▶ No waste of computational power

Proof of Behavior (PoB)

Shared properties with Bitcoin

- ▶ Decentralization
- ▶ Everything is written and publicly available

With PoB, the right to write in the blockchain shared between

- ▶ **User**
- ▶ **Prover**
- ▶ **Verifier**

Proof of Behavior (PoB)

User who performs transactions



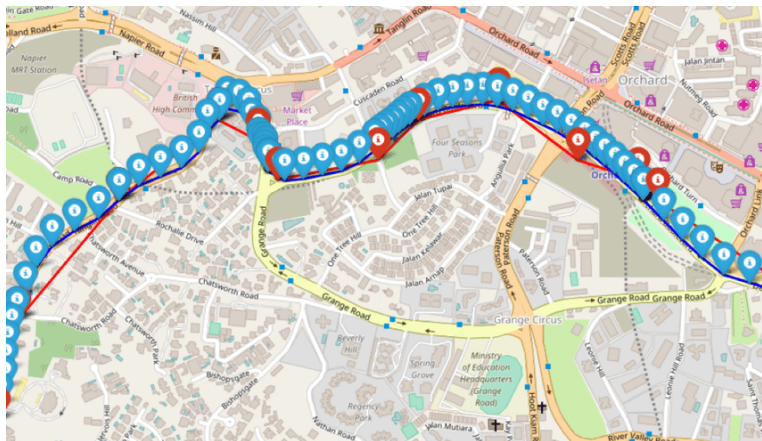
Proof of Behavior (PoB)

Prover who realizes a PoB



Proof of Behavior (PoB)

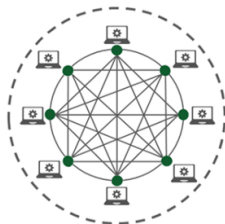
Verifier who verifies PoBs and transactions



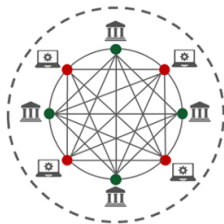
Proof of Behavior (PoB)

3 types of blockchain can be considered for using PoB

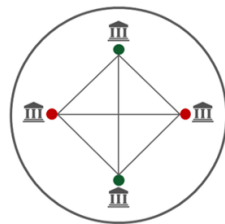
Public



Hybrid



Private



Application: EcoMobiCoin for sustainable mobility

- ▶ Incentivize less emission in the transportation



- ▶ A real GPS trace collected by a smartphone
 - Requires a signature of the device
- ▶ Proof of Behavior in EcoMobiCoin = Proof of Transport Mode
 - Walking
 - Biking
 - Using public transportation (2 GPS traces)
 - Carpooling (several GPS traces)



Conclusion

- ▶ PoW paradigm replaced by PoB
- ▶ Incentivization of the behaviors of users
- ▶ Many PoB-based applications can be considered
- ▶ Important requirements
 - Call for efficient pattern recognition algorithms
 - Call for well-suited cryptographic primitives
 - Compliance with the GDPR

Thanks for your attention...

Questions?