Dealing with mutable data in blockchain-based applications

LPS CHAIN

Dr. Piergiovanni La SETA
Gökhan ÖNAL

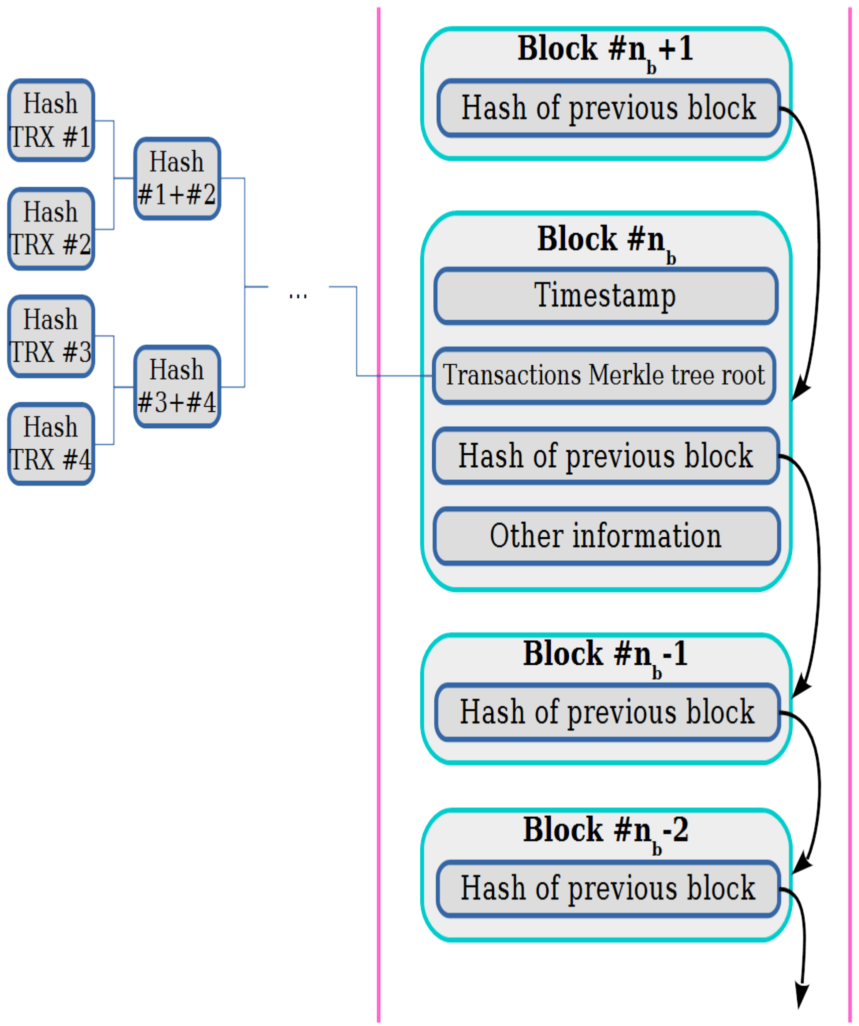
Motivation

- The blockchain technology is a young technology with high potential for data management.
- Several possible applications besides cryptocurrencies have been proposed in the specialized literature
- One of the main characteristics of the blockchain technology is the inherent security, what makes the recorded transactions to be resistant to modifications
- The blockchain's immutability may be however in contrast with certain requirements, first of all the user's privacy
- In this work, some approaches to deal with mutable data are discussed

LPS CHAIN

Blockchain Structure

- A blockchain is referred to a continuously growing list of blocks
- The blocks of a blockchain are linked and secured using cryptography
- Recorded transactions can be efficiently and quickly validated but with very high effort modified afterwards.
- A timestamp is included in the block header. By implementing a timestamp server, a timely order in the block generation is introduced.



LPS CHAIN

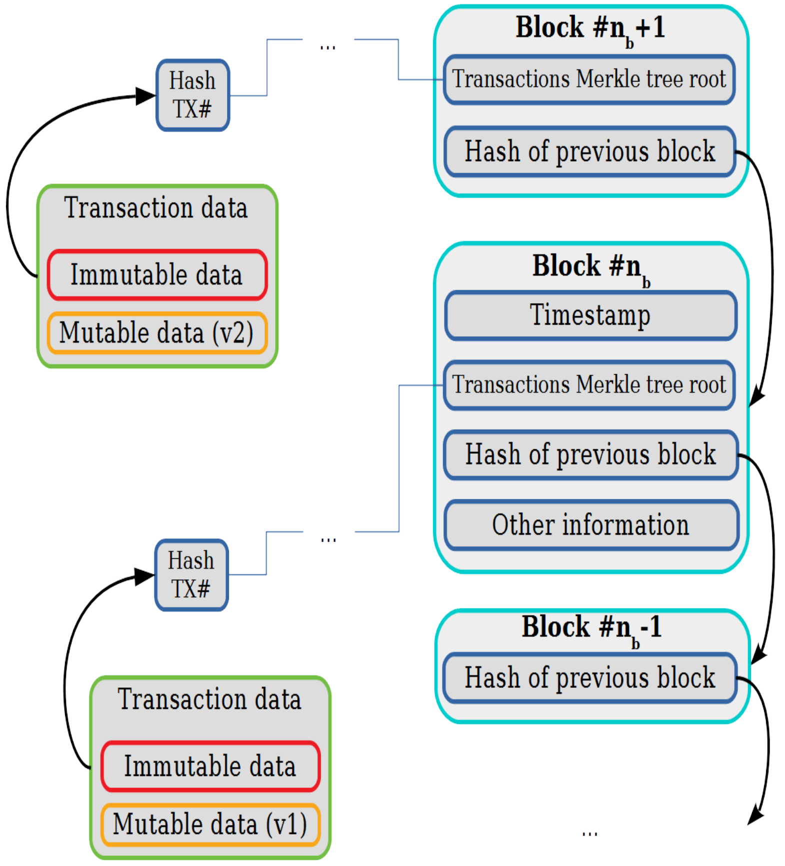
Challenges

- The purpose of blockchain is to make the data stored in it immutable. This is an advantage in many applications (money and stock transactions, supply chain management, etc.)
- Due to its characteristics, the blockchain technology generates trust in consumers even without a central authority
- It could be a preferred solution even in cases when some of the data to be managed can be legitimately mutable
- An important category of data that can be legitimately mutable are identity data
- Blockchain applications for identity management could be problematic due to data protection regulatory aspects

LPS CHAIN

Options to deal with mutable data (1/3)

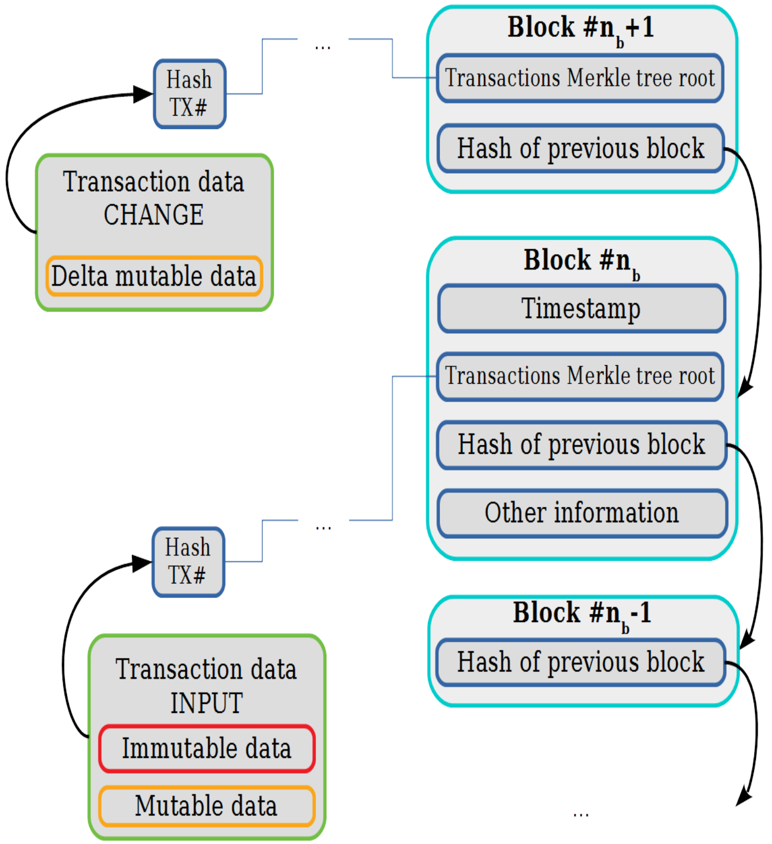
- A first option could be to store all data, immutable and mutable, into a transaction
- As the user's data is input for the first time, a new transaction is created, validated and included in a block. After the block is mined, the transaction data are secured.
- As the data related to the same user is input for the second time with some different values, the new data "overwrites" the original one.
- Provided that the transaction signature is valid, this is perfectly legitimate



LPS CHAIN

Options to deal with mutable data (2/3)

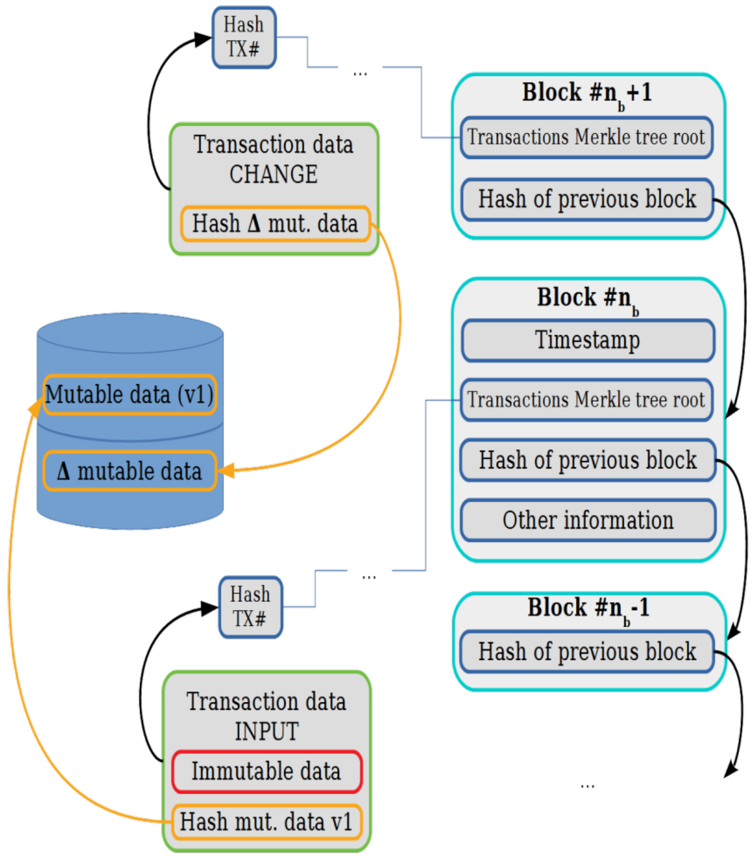
- A second option is similar to option 1 but without redundancy of unchanged data
- A second transaction (marked as a change transaction) only stores the values that have changed for a specific user
- This solution still ensures traceability but it requires less storage space as option 1.
- In both solutions mentioned above, no data is stored off-chain, and the hash codes of all transactions are calculated by using the whole data, both immutable and mutable.



LPS CHAIN

Options to deal with mutable data (3/3)

- When the data to be stored is large, a possible solution is to store some data (e.g. the mutable part) off-chain
- As the transactions contain the hash code of the stored data and their position in the off-chain storage, the block validity is kept
- The off-chain approach has advantages with regard to the storage space but adds complexity



LPS CHAIN

Conclusions

- The potential use of the blockchain technology in some fields (such as digital identity management) implies dealing with data mutability
- This paper does not focus on removing immutability. Instead, some approaches to overcome immutability have been discussed.
- Three approaches have been shown, each with its own limitations, though among others off-chain techniques seem to be the most promising
- In our opinion, the management of digital data requires dedicated blockchain solutions providing additional functionalities besides the typical blockchain features

Thank you!

LPS CHAIN **www.lpschain.com**

piergiovanni.laseta@gmail.com

twitter @PiergiovanniLaS

goekhan@leanpowersolutions.com

twitter @onal_gokhan