# 1

## Advantages of blockchain technology (Budhi, 2022)

### Advantages

* Immutability – once block if added to blockchain, it cannot be changed. Data recorded on blockchain will be distributed to all nodes on blockchain and it will be not possible to change it.
* Transparency – blockchains support transparency to the great degree. It is very easy to trace transactions recorded on blockchain all the way to the very block.
* Non-existent censorship - blockchain is a distributed technology that is managed by peers and all interactions happen peer-to-peer. There is no centralised control over the blockchain. It supports free-market concepts, and reciprocal validation by peers on blockchain network.

Advantages of blockchain, in context of CabChain, guarantee that peers requirements are clearly stated, and cannot be influenced by other factors. Passengers and Drivers will not be constrained by 3rd party which promotes free-market leverage, and ultimately, benefits users of application.

### Disadvantages

* Speed – Due to the computational processing overhead (hashing), on different blockchain networks, it can take from 15 – 30 seconds to consent. It is significantly slower than traditional web 2.0 server-side services such as card payment, which usually take under a second to process.
* Lack of data modification ability – If we consider a case in which some company wishes to develop application of high complexity. We could assume that there will be a certain number of mistakes, or changes in requirements, that were not accounted for at the time of developing application. Blockchains make it incredibly difficult to update requirements after technology was deployed.

In context of CabChain, speed and lack of ability to change login begins application contract means that peers will experience longer time to process their interaction with blockchain than expected by most of the users. We are used to that most of our application are almost instant. Unfortunately, in blockchain, this will not be the case. It will take certain amount of time to process every transaction. The fact that some requirement might change, or new ones might arise, will force starting a new blockchain at every iteration of the application. This will force data to be erased, or stored in external data storge, which poses big question over transparency and security.

## Cryptographic methods used in blockchain technology

Cryptography is a core part of the blockchain technology, in fact, blockchain could not exists without it. Asymmetric cryptography (public-private key pair) and hashing are the two methods that blockchain utilises the most. In blockchain realm, public key is an address of the user and private key is a secret that allows to access addresses data and authorise transactions. (Sahu, 2022)

Most common hashing algorithm used in blockchain technology is SHA-256 algorithm. SHA stands for Secure Hash Algorithm, which was developed by NAS (National Security Agency of USA) and published in 2001. SHA-256 produces 256 bit output of a given file.   
In blockchain SHA-256 is used to hash transaction, among other detail, such as proceeding block in blockchain, to the value that suffices value of a nonce below certain threshold. Then, it is signed by private key of a sender, we call this a signature. After all processing block is added to blockchain. This computational process guarantees integrity and immutability of each block and overall blockchain.

# 2

# 3