CLIMATE | LEDGER INITIATIVE

Factsheet

April 2018| CLI_Factsheet_Immutability of Blockchained explained_ITMO example.docx

Sven Braden, CLI

Why is data stored in Blockchains considered immutable?

Image source: www.unsplash.com

Data stored on blockchains or similar approaches within the area of distributed ledger technology (DLT)[1] is considered to be immutably stored. The immutability claim is one of the core features of the blockchain technology and may also serve the tasks of the climate community in the near future, for example when implementing the instruments of the Paris Agreement. This factsheet provides a non-technical explanation with regard to the bases that form the ground of the immutability claim of blockchains. In order to understand the way blockchains operate, it is crucial to take a look at its fundamental pillars: decentralization and cryptography.

[1] As a simplification, however, we are using the very common term «blockchain» in this text as a placeholder for the much broader concept that includes all distributed ledger technologies, even though blockchain is only one implementation of DLT.

Decentralization

Unlike within common data management systems, where a dataset is stored on centralized servers, blockchains and their underlying networks ensure that the data is duplicated and stored on the servers of every network participant. Every participant of such a decentralized network uses the same software that runs on numerous computers at the same time (so called clients).
These clients ensure that:

- All Data transactions of the network are constantly monitored and validated by **every network participant**;
- All network participants **propose** their "own" individual records to be added to the network's joint database,
- A **consensus** mechanism enables all network participants to agree on one next data set proposed by a "fellow" participant and to be added to the **universal history of data transactions of the network**.

The client ensures that all network participants can rely on one universal set of data history which is identical in its content on all participating network computers. This is how decentralization of one database is achieved. The result is the establishment of a very safe and immutable data management system which comes with much lower costs than current systems.

Cryptography

Immutability, lower costs and security are directly related to the way blockchain technology applies cryptography, more precisely hash algorithms. The heart of every blockchain network is powered by hash algorithms. A hash is something like the unique digital fingerprint of any imaginable set of data, regardless of its size. Technically a hash is comparable to a cross sum.[2] A hash formula, however, is much more complex than just adding numbers for a cross sum – a hash can be seen as a cross sum mixer which factors, summands and multiplies every single digit (including letters) of a data set and calculates a certain result from it: **the hash**. Like with the cross sum, a hash can be much shorter than the original hashed text (data).[3] It is also impossible to conclude from the hash back to the initial data set – and that is a feature!

[2] A cross some is the sum of a number's individual digits - repeatedly applied. The cross sum of 8'2141 is 7. 8 + 2 + 1 + 4 + 1 = 16 which leads to 1 + 6 = 7

[3] The hash formula used by the Bitcoin network is the SHA256 algorithm which consists of 32 bits and hashes numbers as well as minuscule and capital letters: the number of hash possibilities is literally endless – one hundred quattuorvigintillion possible variations (a number with 77 zeros)

For example, the **hash** of the phrase

“Nothing is decided until everything is decided” always has the hash:

9f62f85d500c8d4682c2aa9f8a00d89658be956b3a680dfd370eb1c9bb94e445.

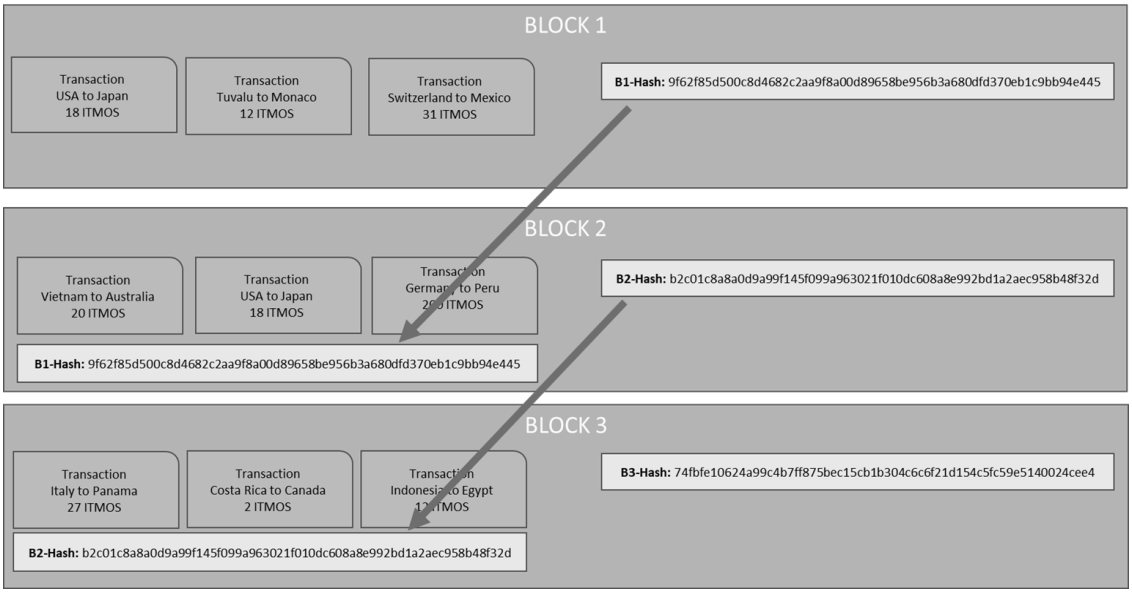
A change of just one minor part of the data set causes the so-called avalanche effect in the “hash mixer” and leads to a complete different hash. For example, the slightly altered phrase:

“Nothing is decided until everything´s decided” has the hash:

3f9801bc00d0a466b42c006dbbbf312ce38d1cf515a999bb09f9b556feeb5624[4]

As already stated, the hashing of datasets is the fundament of the blockchain technology. The following example illustrates the central role of hashes in a blockchain network.

For the sake of the example[5] we assume the existence of a blockchain network for corporative approaches, run and maintained by participating Designated National Authorities (DNAs) of Parties to the Paris Agreement – **the PA Network**. Here, the USA and Japan agree on a transaction of 18 ITMOS[6]. Tuvalu, Monaco, Switzerland and Mexico also do add their transaction of ITMOs to this block (BLOCK 1). The information is basically nothing but a set of data that will be automatically hashed, once the block is “full”. This Hash, described as Block Hash (B1-Hash) in the graph below, will be added to the following Block as previous Hash (which again will be hashed etc., see graphic below).



[4] Hash generators may be found online, e.g. http://passwordsgenerator.net/sha256-hash-generator/
[5] The taken example would also work with a distribute inventory of GHG.
[6] ITMO_ Internationally Transferable Mitigation Outcome, Art. 6.2 PA

The respective block hashes are central for the immutability, the safety and the low costs of the overall network. Here is why:

The last block hash of the PA-Network would always contain the whole history of all ITMO transactions in the PA-Network until back to the first ever made transaction – within the so-called Genesis Block. Altering just one little digit in an earlier block would immediately lead to a distortion of the chain of blocks – and would consequently lead to the "kick-out" of the participant whose record is not in sync with the other participants records anymore. It is still the greatest challenge of current databases to synchronize data around the globe in a way that they can be sure that every participant looks at the same set of data. Being able to only focus on a series of 32 digits (the most recent block hash) is much easier, cheaper and at the end even safer than being forced to check the content of all participating data storage centres around the globe. In the assumed PA-Network all Parties would continuously check and verify all transaction within the network and then "only" compare their last block hashes with the last block hashes of the other participants (e.g. Parties/countries).

The Climate Ledger Initiative (CLI, www.climateledger.org) aims at providing objective and technology neutral information with regard to current and future climate-relevant applications which are based on distributed ledger technology. The work of the CLI is financially supported by the Governments of Liechtenstein and Switzerland as well as by the EU's Innovation Program Climate-KIC.

GOVERNMENT
PRINCIPALITY OF LIECHTENSTEIN

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Agency for Development and Cooperation SDC

eit Climate-KIC