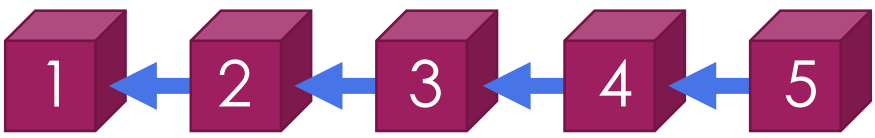
Blockchain

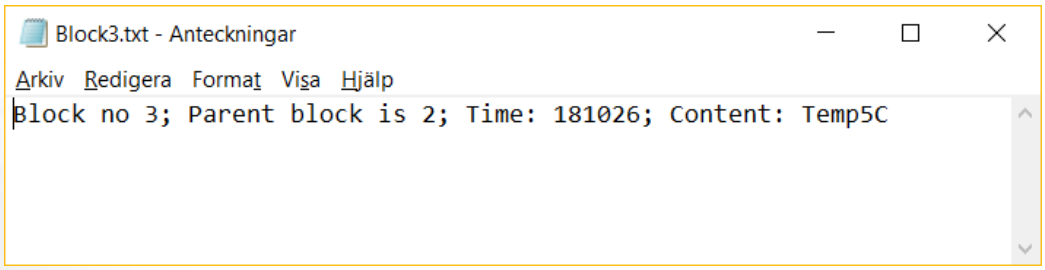
This might be the first summary where blockchain is explained without referring to a well-known cyber currency starting with "B". Blockchains are a combination of blocks, chains, members, cryptography and distributed databases.

Blockchain is a concept of how to securely store and share data.

Blocks and chains
Data is stored in blocks. Each block (except the first block – known as the genesis block) refer to a parent block. When visualizing the blocks reference structure, it looks like a chain:

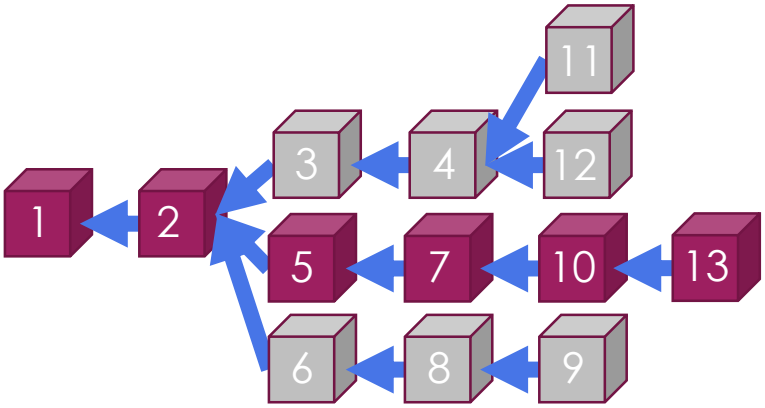


The data of a block could be seen as a simple text line:
Block no 3; Parent block is 2; Time: 181026; Content: Temp5C

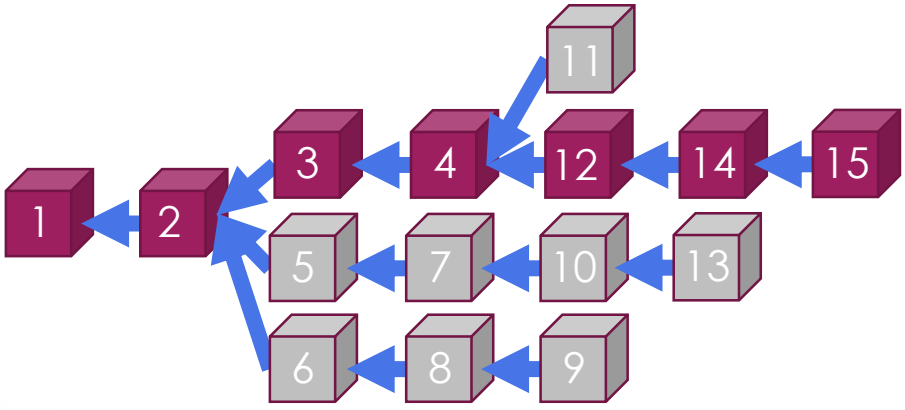


Summary

Several blocks can refer to the same parent. The longest chain is called the main chain, marked red below:

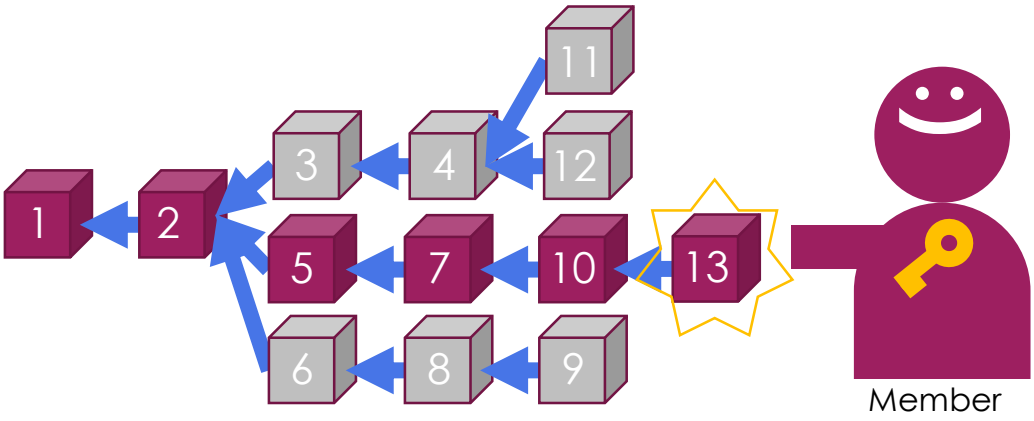


The main chain can be changed if more blocks are added to another branch:



Summary

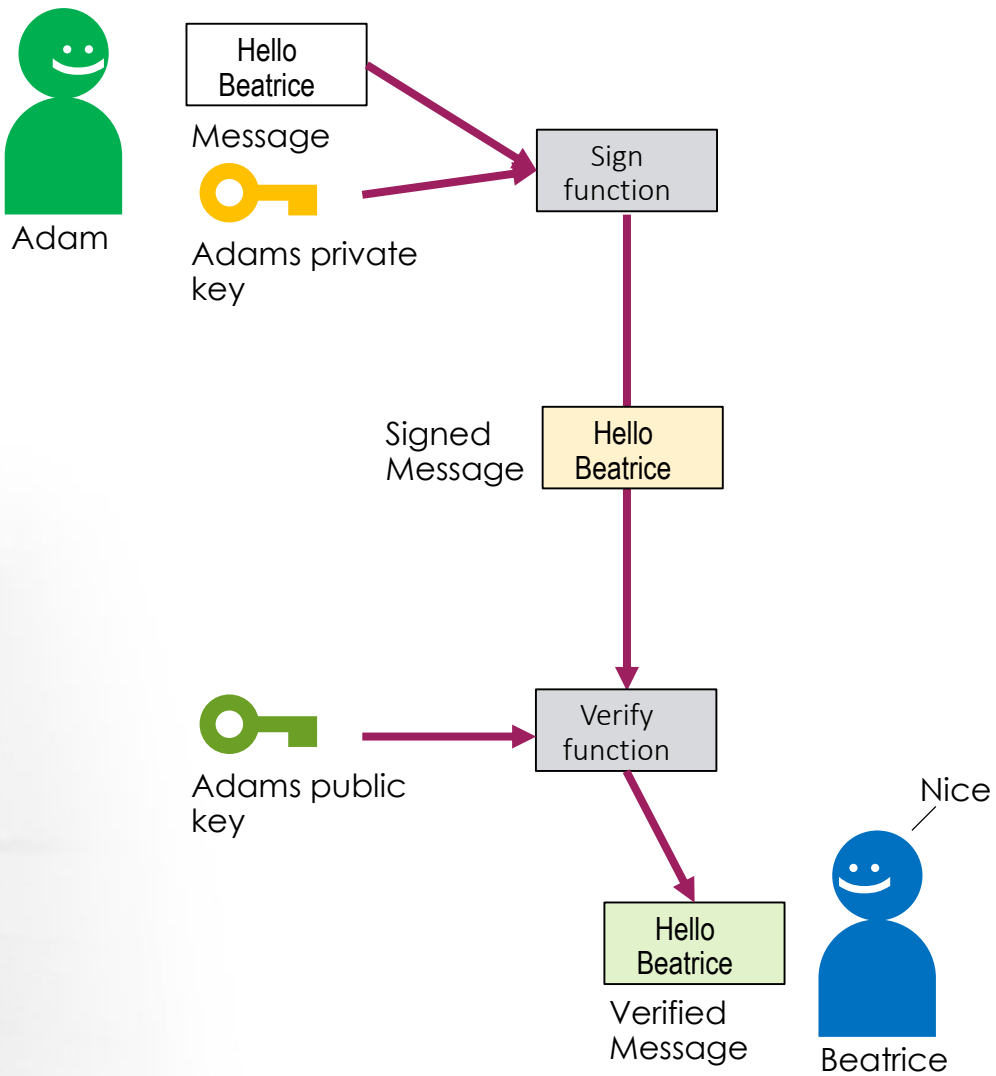
Members
In order to add blocks, one have to be a member of that blockchain. This requires that they register to receive a unique key, which they use to validate themselves being a member.



Anonymous members
There are blockchains where the member doesn't have to share their personal information - they can register to receive a unique key anonymously.

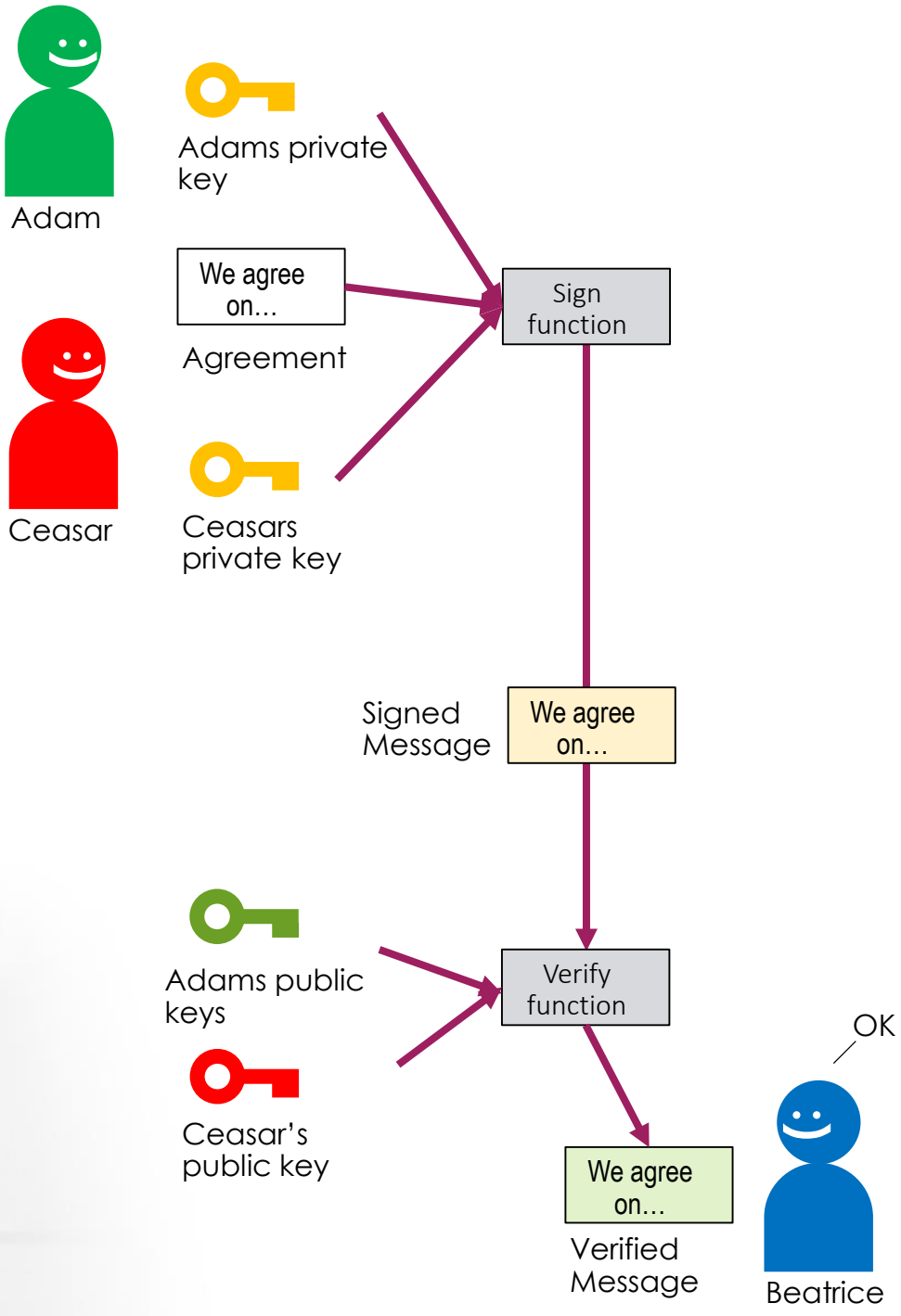
Summary

Public-key cryptography
A member of a blockchain must be able to "confirm" themselves for the other members. This is done by a method called public-key cryptography. The method can be compared with how people in the past signed documents:
All persons signing documents had an unique sign (a family crest).
There was a book, that all had access to, containing all signs.
When a person signed a document, the person pushed his unique signet ring into melted wax on the document forming his sign (that no one could copy).
The receiver of the document could easily verify the sender by looking at the sign in wax comparing it to the public book.
The "book" in blockchain is called public-key and the unique signet rings are called private-keys. They are both long series of numbers. To use the keys, there are sign and verify functions (programs on a computer).



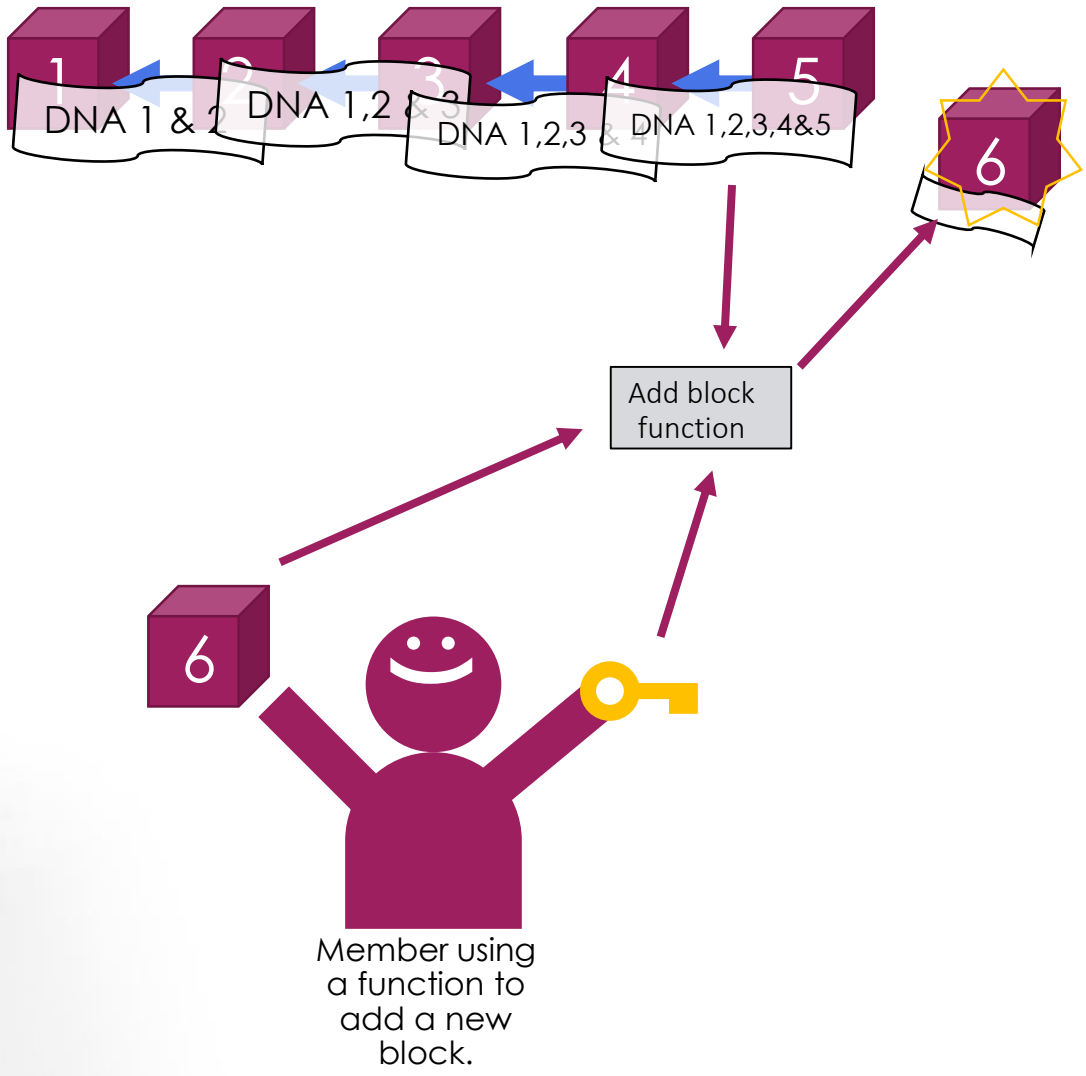
Summary

Multiple signing
There are also ways of signing things together, e.g. an agreement.



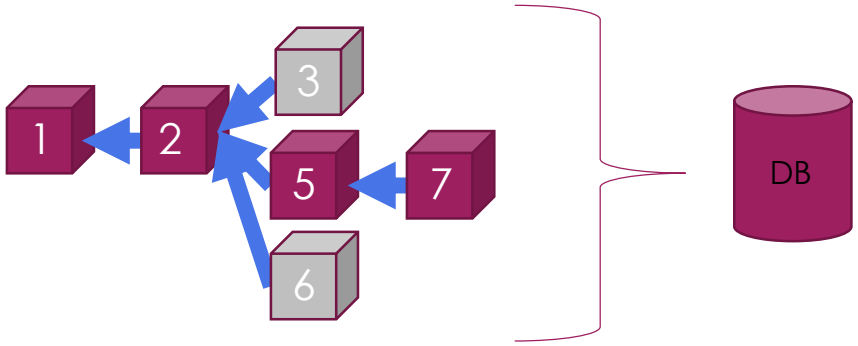
Summary

Cryptography hash
When adding a block to a chain, the member adding the block uses cryptography to assure that the block refer to the correct parent block (and can't be altered by someone else).
This can be compared to an unremovable tape of with the clue consist of DNA from both the new block and the parent blocks. The DNA tape is placed to hold the two blocks together.

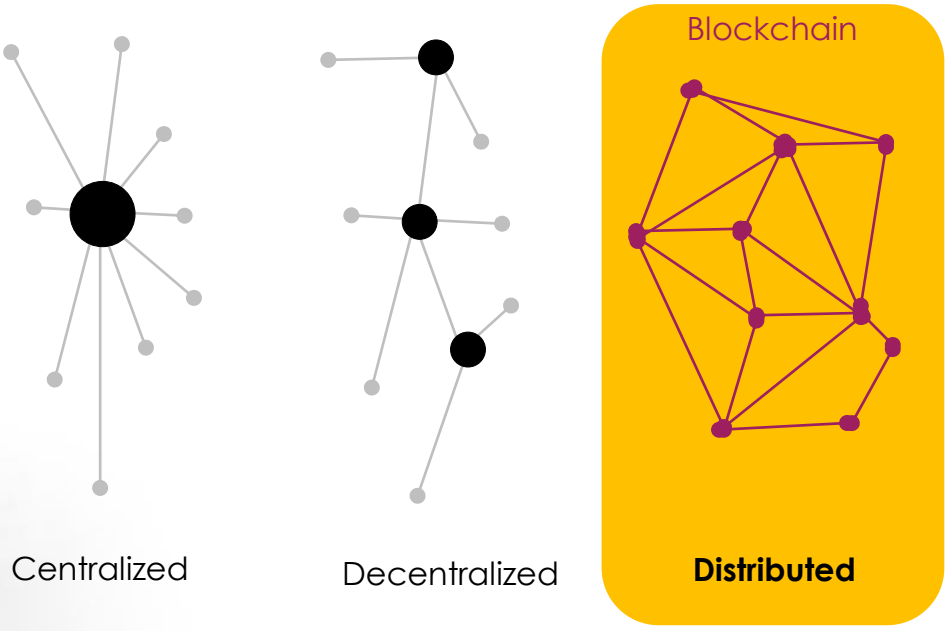


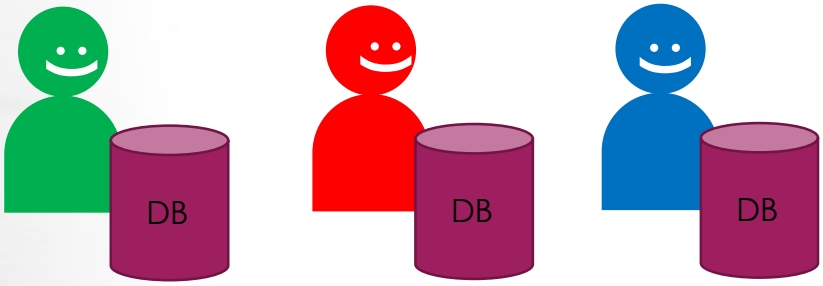
Summary

Distributed database
Blockchains are not stored at one (or several) central place(s), the blockchain is distributed to all parties involved, as a database.



Different database models:

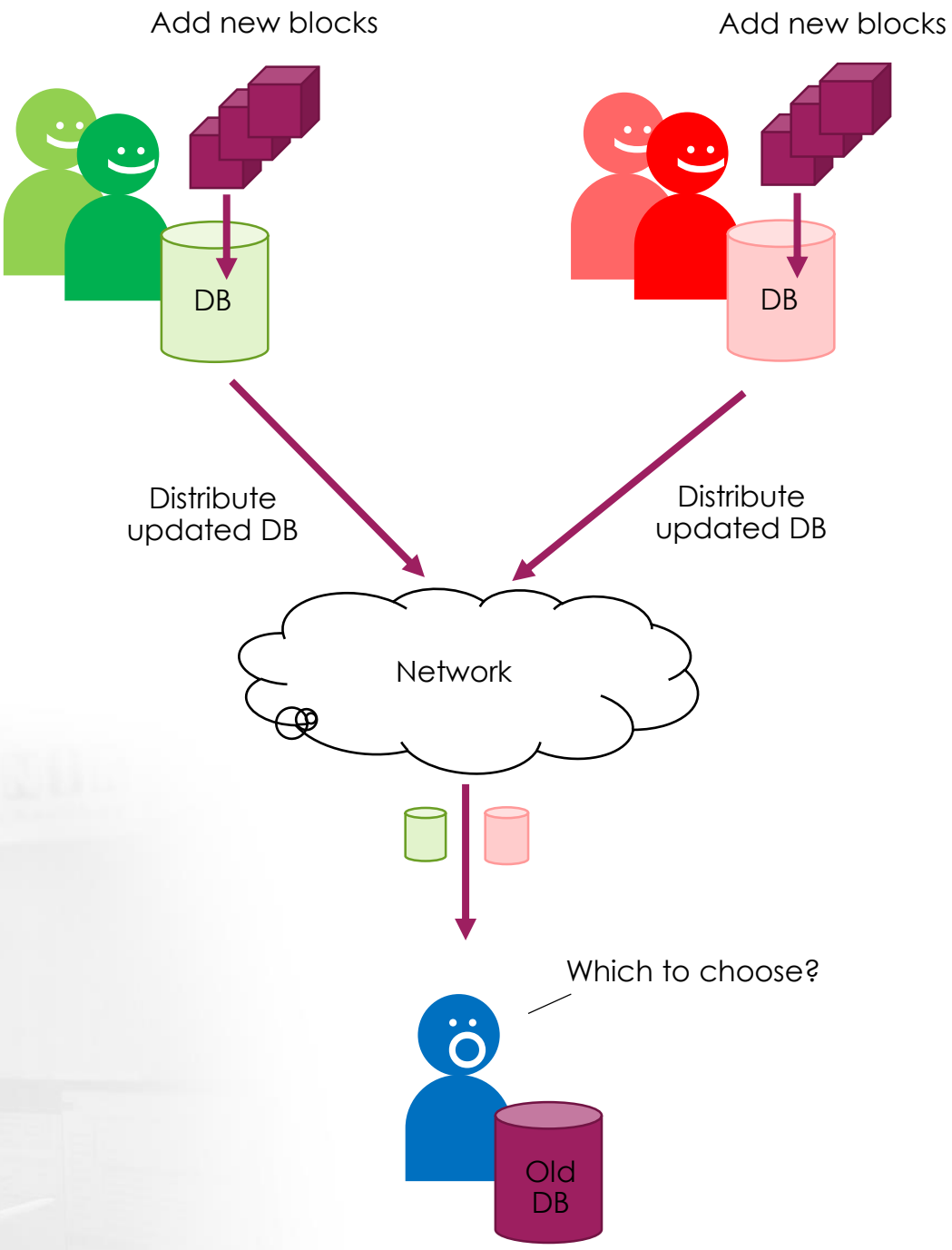




Members all having the distributed database at hand

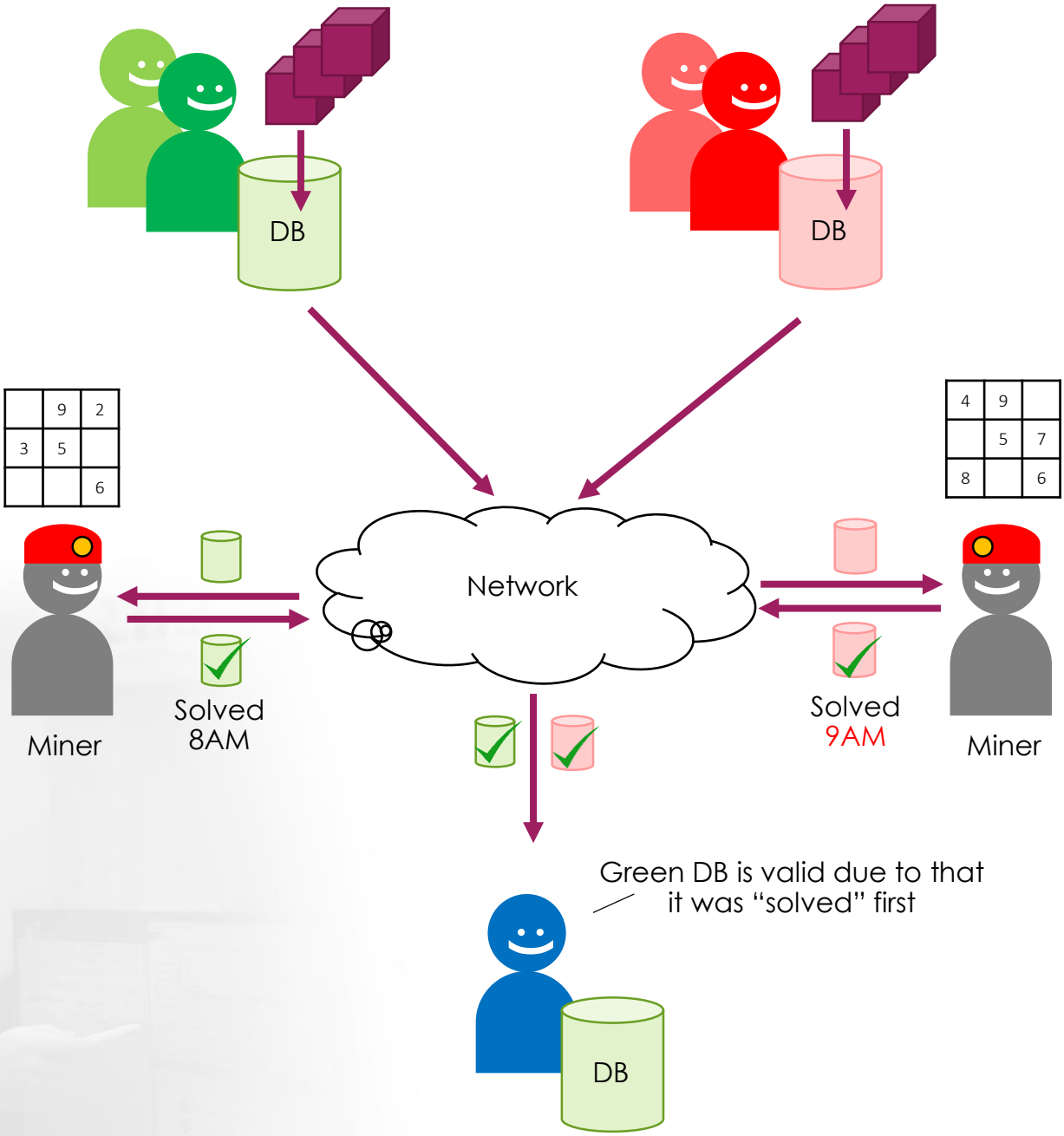
Summary

Distributed database dilemma
The problem with distributed database is to know which one is valid. If members are updating the database faster than it's distributed there will be different versions. The dilemma is which to choose.



Summary

Proof-of-work
One way to choose the right database is to use proof-of-work. They idea is to have members (usually called "miners") to solve a difficult computerized problem for each new updated database. The problem can be compared to a sudoku; it's hard to solve but easy to verify when done. The miner that solves the sudoku first timestamp the solution and database. The database with the earliest timestamp is the valid one. Keep in mind that there can be several "solved" databases around, so a member might have to replace the "solved" database when receiving another having an earlier timestamp.



Summary

Conclusion

Blockchain is a concept of how to securely store and share data. Blockchains are a combination of blocks, chains, members, cryptography and distributed databases:

- Blocks are containers of data.
- Chains are linked lists of blocks.
- There can be several chains in a blockchain; the main chain is the longest one.
- Only members of the block chain can add blocks. Security is handled by public-key and hash cryptography.
- All members have the database. Change management to the distributed database can be handled by proof-of-work.