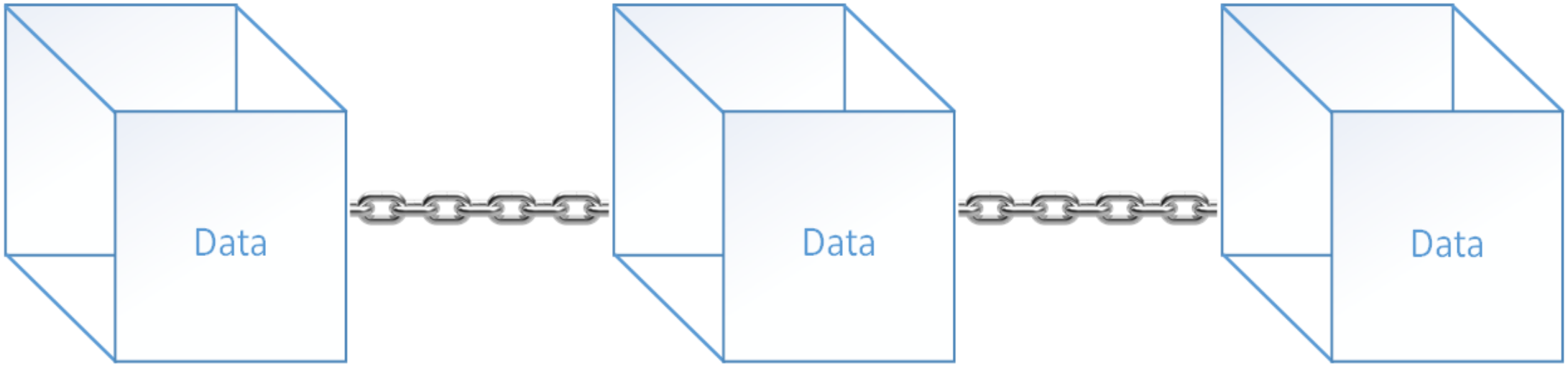
Blockchain

A Blockchain is a method of storing data. Data is stored in blocks which are linked to the previous block.

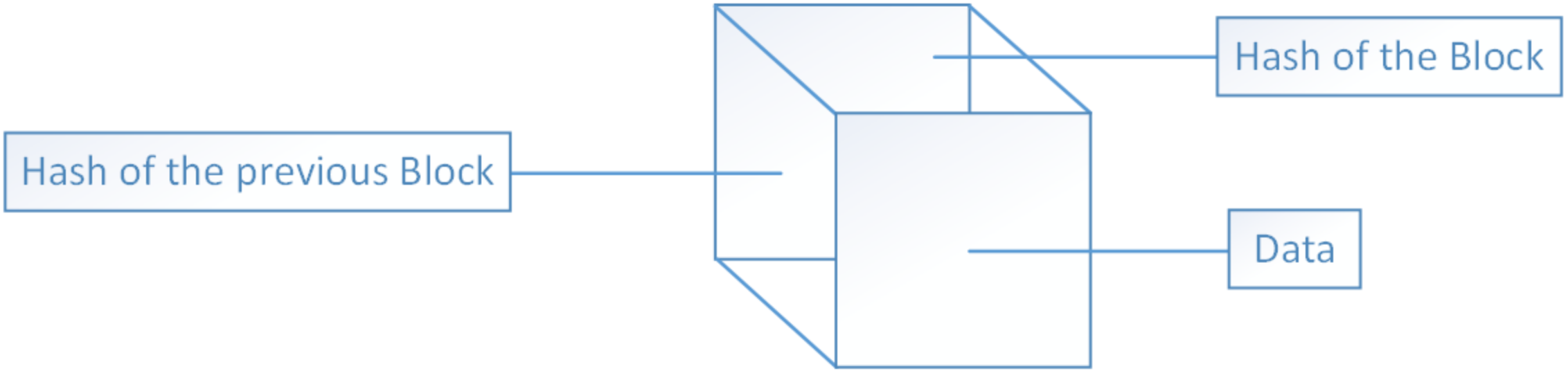


https://hackernoon.com/blockchain-a-short-and-simple-explanation-with-pictures-d60d652f207f

But what does a “Block” look like?

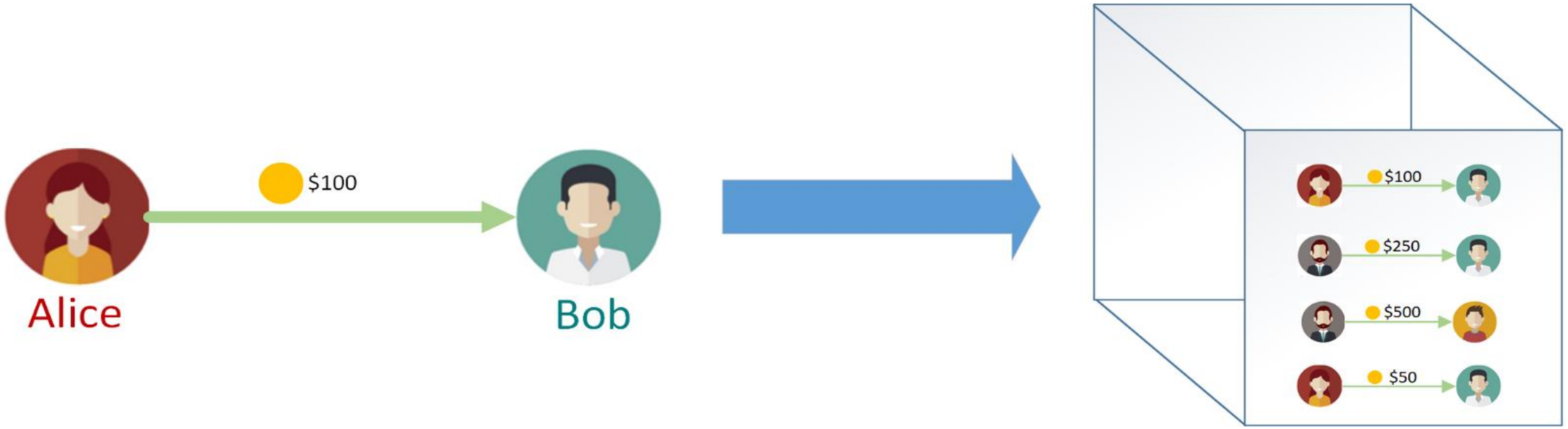
Each “block” contains

1. Data of transactions
2. A unique fingerprint for all the data in the block called a hash
3. A hash of the previous block’s data

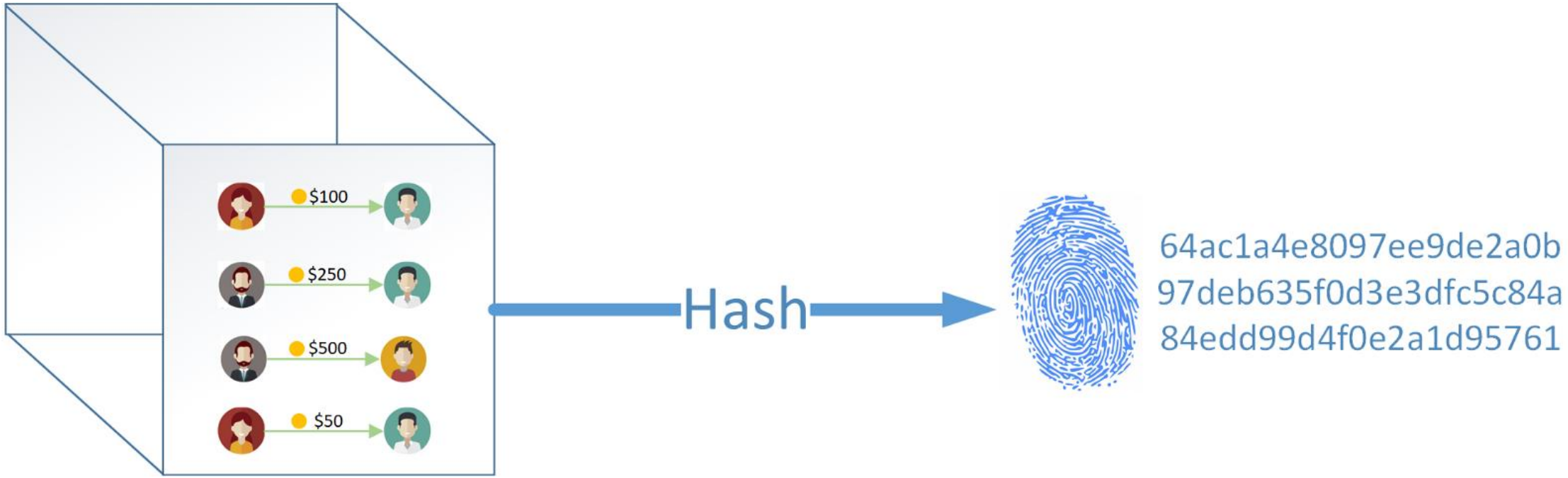


What do each of these items mean?

Data in the block usually consists of transactions. A block can contain hundreds of transactions. Alice sending Bob $100 is an example of a transaction in a block

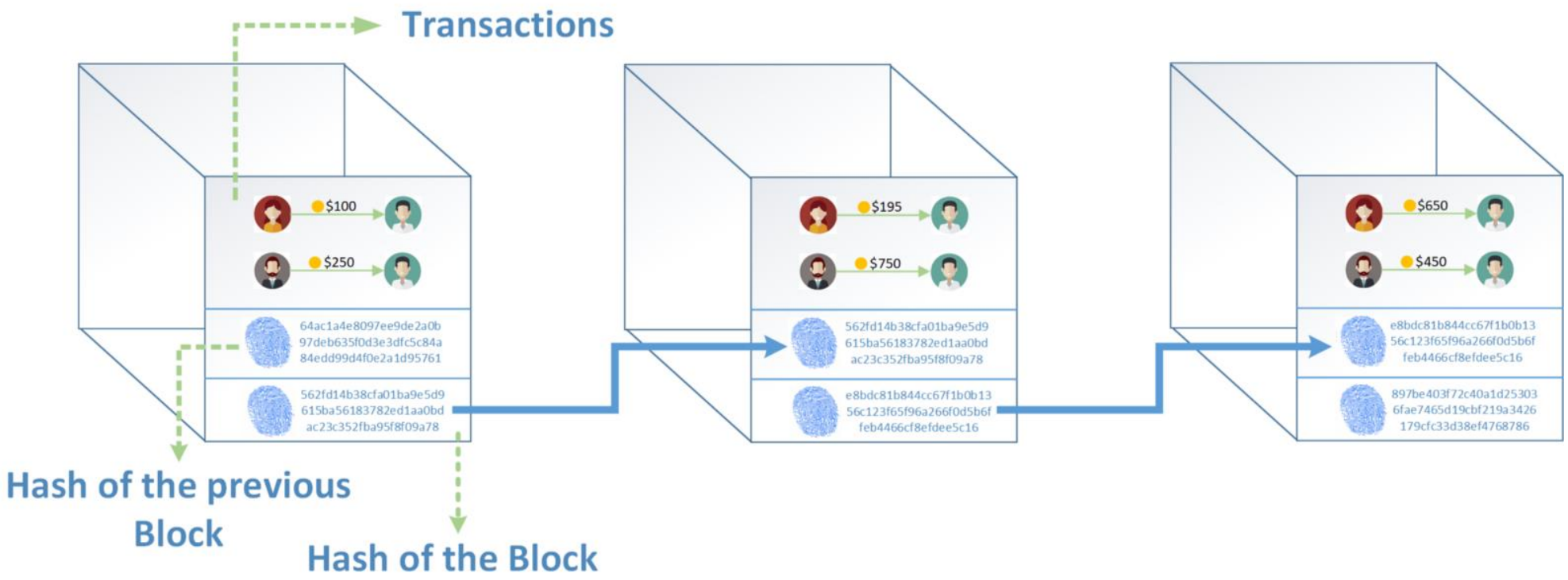


A hash is a unique combination of letters and numbers. It is like a fingerprint for the data in a block and it is always unique to every block in the Blockchain. When the data in a block changes, the hash will also change.



Hence in a transaction, if the amount being sent Alice to Bob changes from $50 to $100, the hash of the block will completely change.

A block also contains the hash of the previous block. Hence forming a chain structure. Combining the above three together, this is what a Blockchain will look like

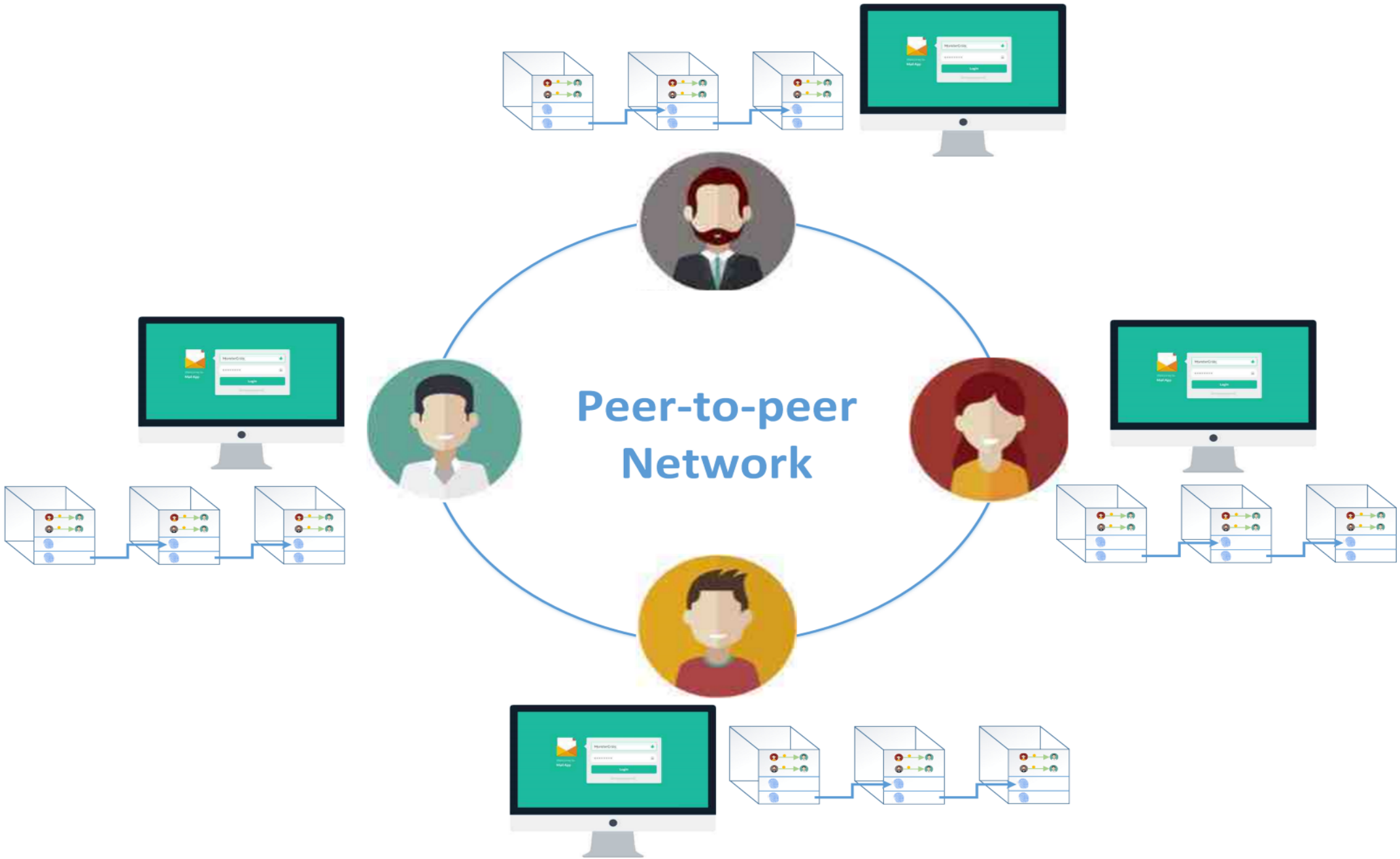


Now if a transaction in any block changes, the hash of the block will change. When the hash of the block changes, the next block will show a mismatch with the previous hash that was recorded by it.

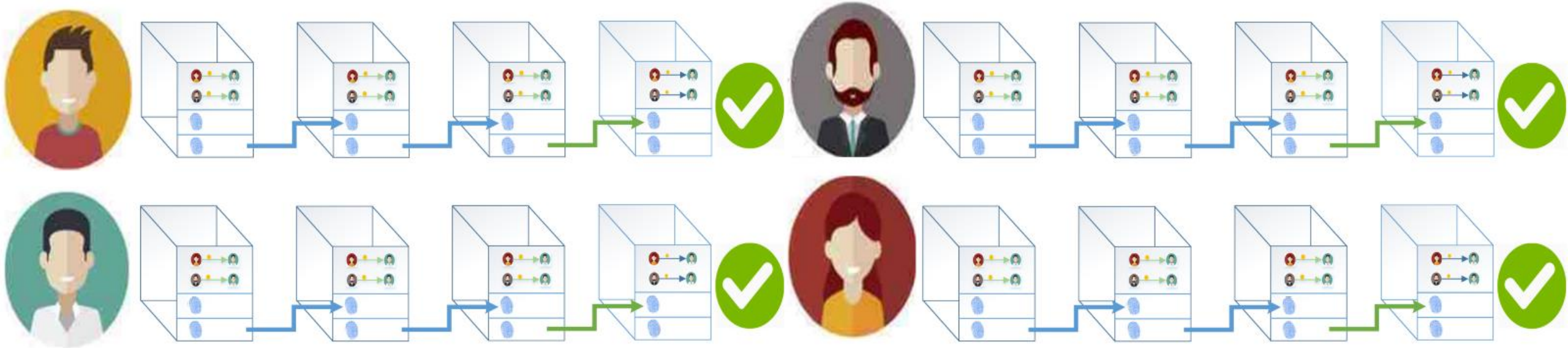
This gives Blockchain the property of being tamper-resistance as it becomes very easy to identify when data in a Block has changed.

Hashes can be seen in action here. Try entering “Orange”, and then “orange”. See how a simple change in one alphabet completely changes the hash. Additionally, this link can be used to see how hashes secure the entire Blockchain.

Blockchain has one more property which makes them secure. A Blockchain is not stored on one person’s computer. Instead, it is stored in a large network of computers called a peer-to-peer network. A computer on this network is called a node, and every node will have a copy of the Blockchain.


Peer-to-peer
Network

Every a time a new block of transactions has to be added to this network, all members (nodes) of the network must check and verify if all transactions in the block are valid. If all nodes in the network are in agreement that the transactions in a block are correct, then the new block will get added to every node’s Blockchain. This process is called consensus.



Hence any attacker who tries to tamper with the data on a Blockchain must tamper with the data in the majority of the computers in the peer-to-peer network. This is how Blockchains proves to be a secure method of storing data.

Now, what if I wish to create a transaction in a Blockchain. How will I go about doing it?

Every computer software that uses a Blockchain, will give its users a public key and a private key. These are again just like hashes; they are a random sequence of alphabets and numbers that are generated by the software itself. Every user has to keep their private key securely and not reveal it to anyone. The public key, on the other hand, can be revealed to everyone.

PRIVATE KEY

68317289906367255519345137905528179295707647578558684440512287097919467220420

PUBLIC KEY

044e554e13e016a83a958197cf3b8622b9afc5b9ea04bdf37e1ef20a2dabcfa7d180ba760ec74408abadd2468bc5415d67305dd679d4bd1610c72f0aff57dc1ab3

Consider the example of a mailbox. The public key is like your mailbox which everyone knows about, and can drop you messages. The private key, on the other hand, is like the key to that mailbox. Only you own it, and only you can read the messages inside.

Both public and private keys have a unique property. The **private key** can be used to **sign** any message to create a **digital signature.** A digital signature is yet another sequence of characters and numbers. But there's a catch!

All digital signatures can be verified using the corresponding **public key**. This means anyone who has a digital signature can verify whether a person truly signed the message, using the signer's public key.

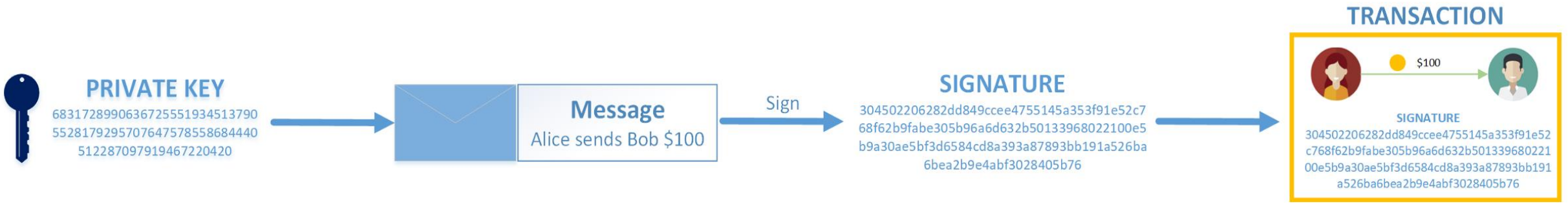
Both these keys, combined with message signing to create digital signatures can be called the **cryptography** in Blockchains.

Too complex?

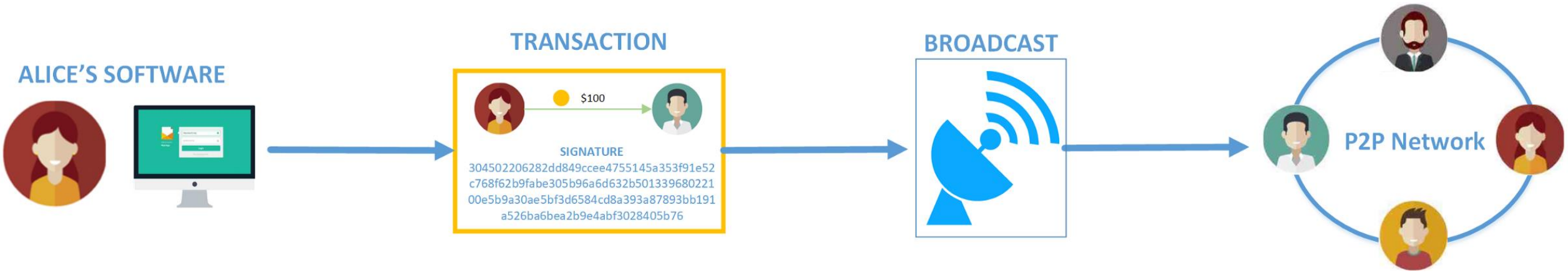
Let's break it down step-by-step with an example.

Alice wishes to record the message that she sent $100 to Bob on a Blockchain.

1. She writes the message and signs it using her private key to create a digital signature. Her message combined with the signature is a **transaction.**

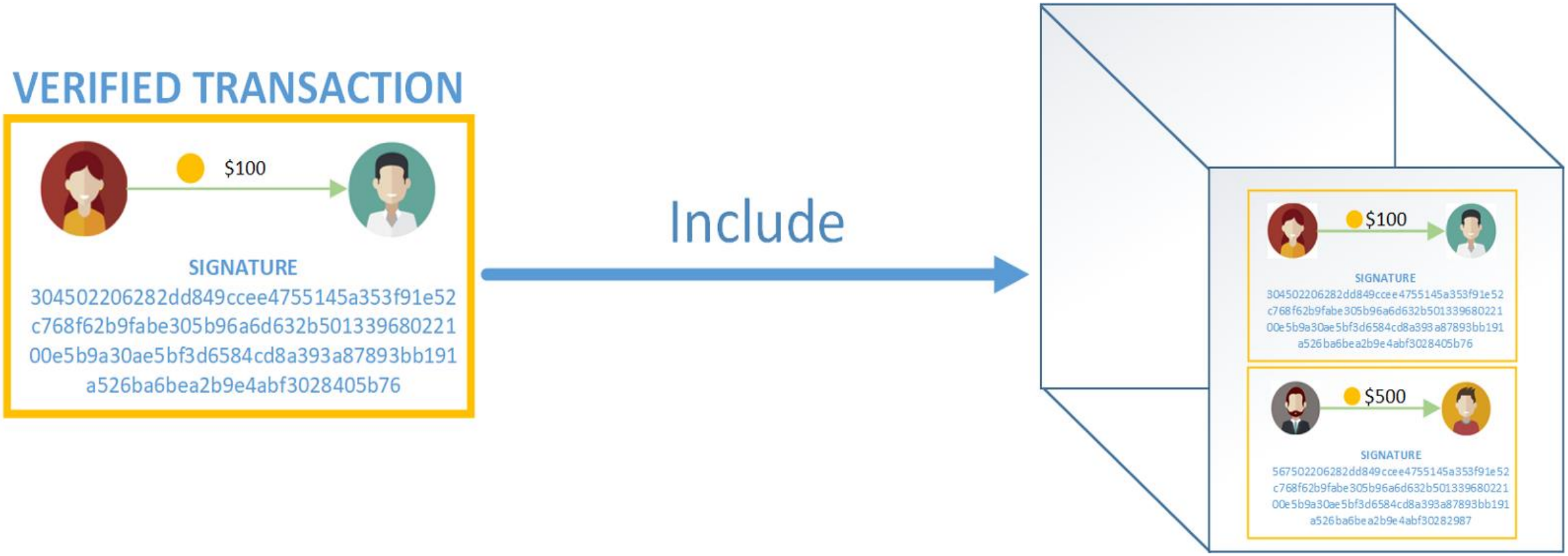


2. The software Alice uses broadcast her transaction to everyone in the peer-to-peer network

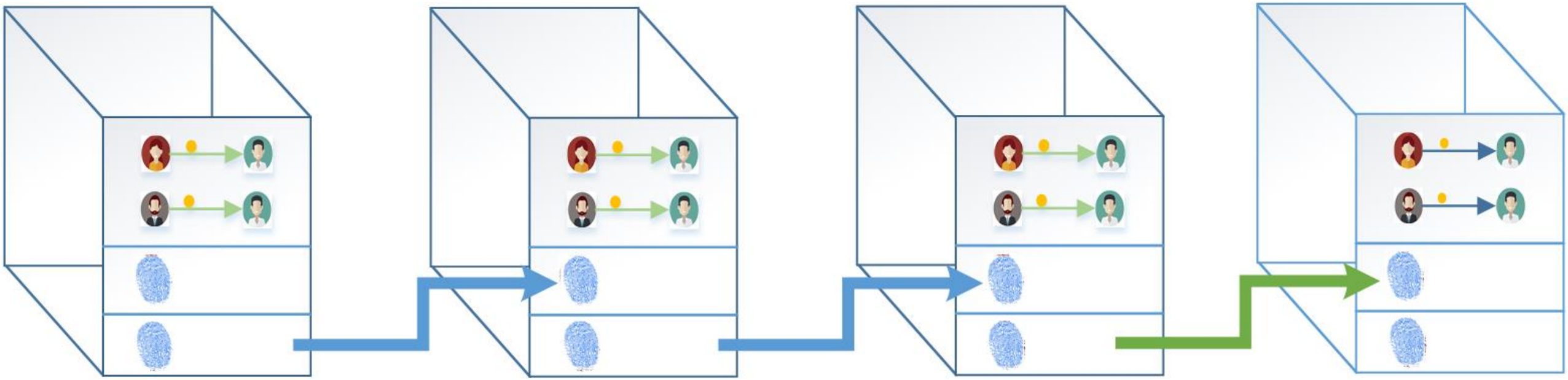


3. Everyone in the P2P network first verifies her transaction signature, to see if Alice is the one who really signed that message. They do so using Alice's public key which everyone knows.

4. Once verified, the P2P network includes Alice's transaction on a block in a Blockchain.



5. When the P2P network reaches **consensus**, after verifying all transactions, the block with Alice's transaction gets included in the Blockchain!



Once included, Alice’s transaction cannot be changed by anyone so easily!

And there you have it. That is a near complete explanation of how data is stored on a Blockchain

To summarize,

1. A Blockchain is a method of storing data in blocks which are linked together in the form of a chain.
2. It relies on hashes and cryptography to secure the data inside a block.
3. This chain of blocks resides on all computers in a peer-to-peer network.
4. This network of computers use consensus methods to verify transactions in a block and include a block on the Blockchain.

Hope you learned something new.

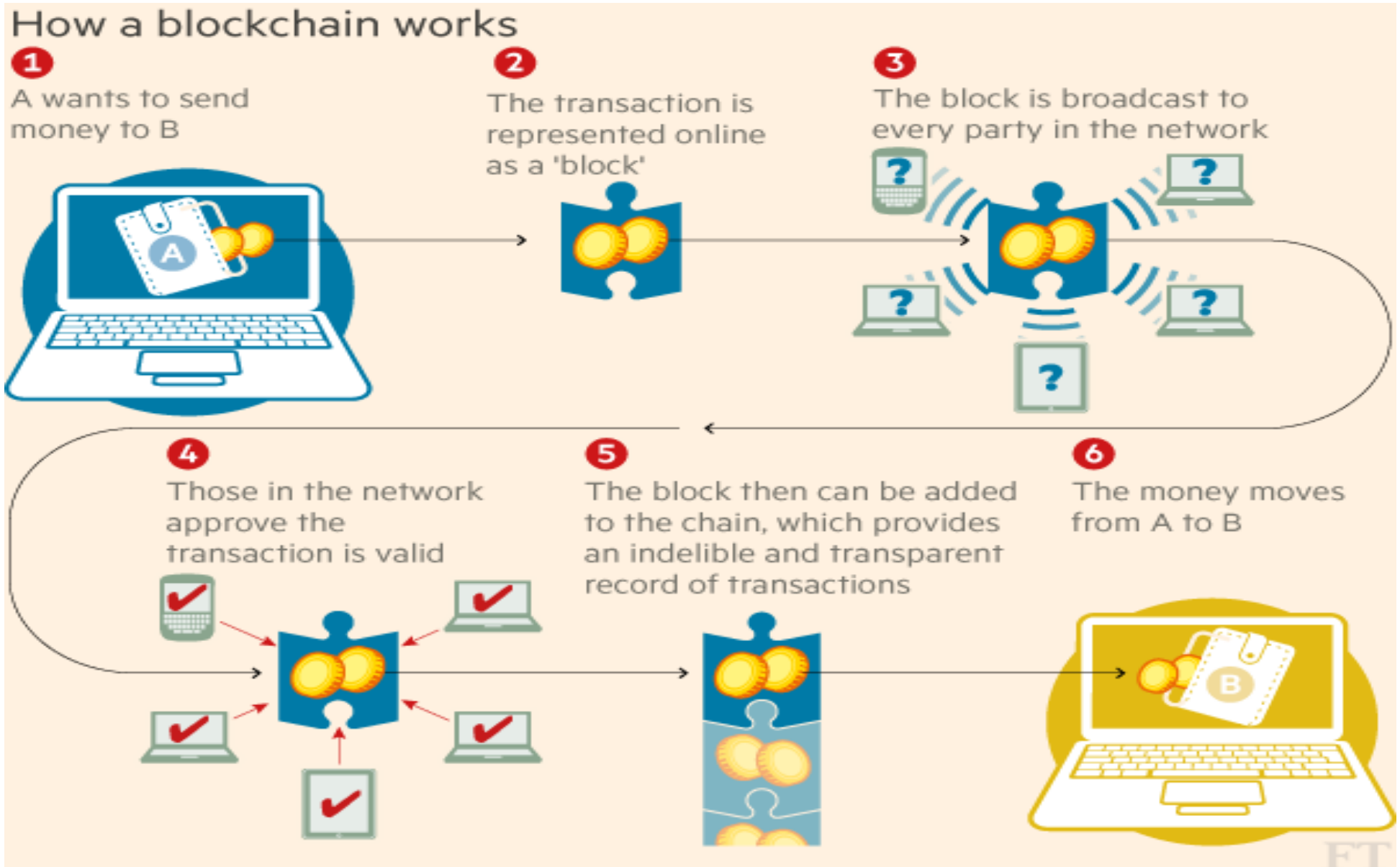
From another site

A block chain is a blockchain that contains batches of valid transactions. Each block includes the hash of the previous block of the blockchain, joining the two. Joined blocks form a string, allowing only that block (successor) to chain to that other block (predecessor), giving this database its name."

Thus, we can say that a blockchain is a blockchain of data that contains transactions. Well, it doesn't look promising at all, does it?

Let's highlight a small detail: a blockchain is a history of transactions that cannot be manipulated or forged. Can you think of what can be done with this?

Blockchain y Ciberseguridad I - Security Art Work


How a blockchain works
1
A wants to send money to B
2
The transaction is represented online as a 'block'
3
The block is broadcast to every party in the network
4
Those in the network approve the transaction is valid
5
The block then can be added to the chain, which provides an indelible and transparent record of transactions
6
The money moves from A to B
A
B
FT

This first definition speaks of the basic stone of this technology, however, blocks are just the beginning. In this "transaction history" that is a blockchain, these blocks containing transaction information are distributed over the Internet to all nodes that make up the network. These nodes process the information and reach a consensus, approve the transaction, and add the block to the string, leaving an indelible, public record of it.

In the following image we have a more graphical explanation of how blockchain works using the most common case so far: monetary transactions.

The first question that arises, very valid, is: *and who are these nodes?*
A node can be any node. All the code on a blockchain is Open Source and can be run on any computer. The trick of success is in the motivation to be a node. The anonymous blockchain creator, **Satoshi Nakamoto,**very intelligently integrated a reward system for nodes into the transaction validation process.

For validation, this network of nodes must reach consensus using a known mechanism. The most used and well-known is "proof of work", although there are others. This mechanism is based on the properties of certain algorithms, such as finding a hash, for which it is difficult (in time and computational resources) to solve a certain arbitrarily defined problem but it is very easy to check if the solution is correct.

To add a block to the chain, nodes must select a certain number of transactions from the queue, verify that they are valid, retransmit them, and calculate the "work test" especially the transaction block, whose solution requires that certain requirements be met. Finding the proof of work is a random process with a probability directly proportional to the computation capacity used, so that a lot of trial and error is required on average until the solution is found.

The first node that finds the solution is rewarded. In a way, nodes "compete" to find the solution. In the case of Bitcoin, the reward consists of a fixed amount of Bitcoins, plus a fee that the creators of the transactions can include to motivate the nodes to include their transaction in the block as soon as possible.

When a node manufactures a valid block, it relays it to the rest of the network, which checks the validity of the block and the transactions it contains, based on the blocks (past transactions) that are already enrolled in the blockchain.

Since transactions are validated for each block, the only way to perform a "double expense" attack, spending the same currency at two different sites, requires rewriting all blocks from the transaction that you want to be manipulated to the current block.

This is why a transaction is considered more secure the more blocks that have been written later. For important Bitcoin transactions, for example, a depth of 6 blocks (about an hour's wait) is considered absolutely impossible to manipulate.

Although at first glance it may seem like a toy process, the complexity of the inherent security mechanism of this technology is impressive, attracting an incredible community of developers and cryptography experts who have been working since Satoshi Nakamoto, back in 2009, published his great Whitepaper.

Do you think it's revolutionary?

Well, the truth is, yes. This consensus mechanism has great implications. In the absence of an "official" copy and no particular node is more trusted than another, we are talking about a decentralized trust system.

And this is where we have the main course.

The first blockchain application is much better known than the technology itself: Bitcoin. And for years it's been the only one in place. However, as of 2014, what are known as blockchain 2.0 technologies began to emerge. These are a new wave of blockchain-based applications, since the chain can record data that is not necessarily transactions.

This data can be anything. From legal birth certificates, weddings, cadastre registrations or digital identities, to copyright (with proof of first creation) or patents to contracts or votes.

Traditionally, a trusted central authority has been needed to certify that certain information (a document) is valid and truthful. This is the workspace of many entities: notary, banks, many public administrations and records, dispute resolution systems,... And indeed, the world's leading economic institutions are already investigating their usefulness and use, as well as starting the first pilots.

However, in a decentralized trust system, these central entities are not required.

The initial community of Bitcoin and blockchain has proclaimed from the beginning that this technology will be disruptive, changing many aspects of society. These changes will come from the new ways of offering commercial (and non-commercial services as well) that blockchain will enable, just as the Internet did in its day, and which are butter enough to write several posts

https://www.blockchainresearchinstitute.org/an-intro-to-blockchain-and-nfts/#:~:text=A%20blockchain%20is%20a%20distributed,of%20assets%20without%20an%20intermediary.&text=Anything%20from%20currencies%20to%20land,exchanged%20on%20a%20blockchain%20network.

https://www.youtube.com/playlist?list=PLYgkm0MK8DQGa5_-kK-836SoaOXqjD4rW

Blockchain 101
13 videos1,638 viewsLast updated on May 10, 2019