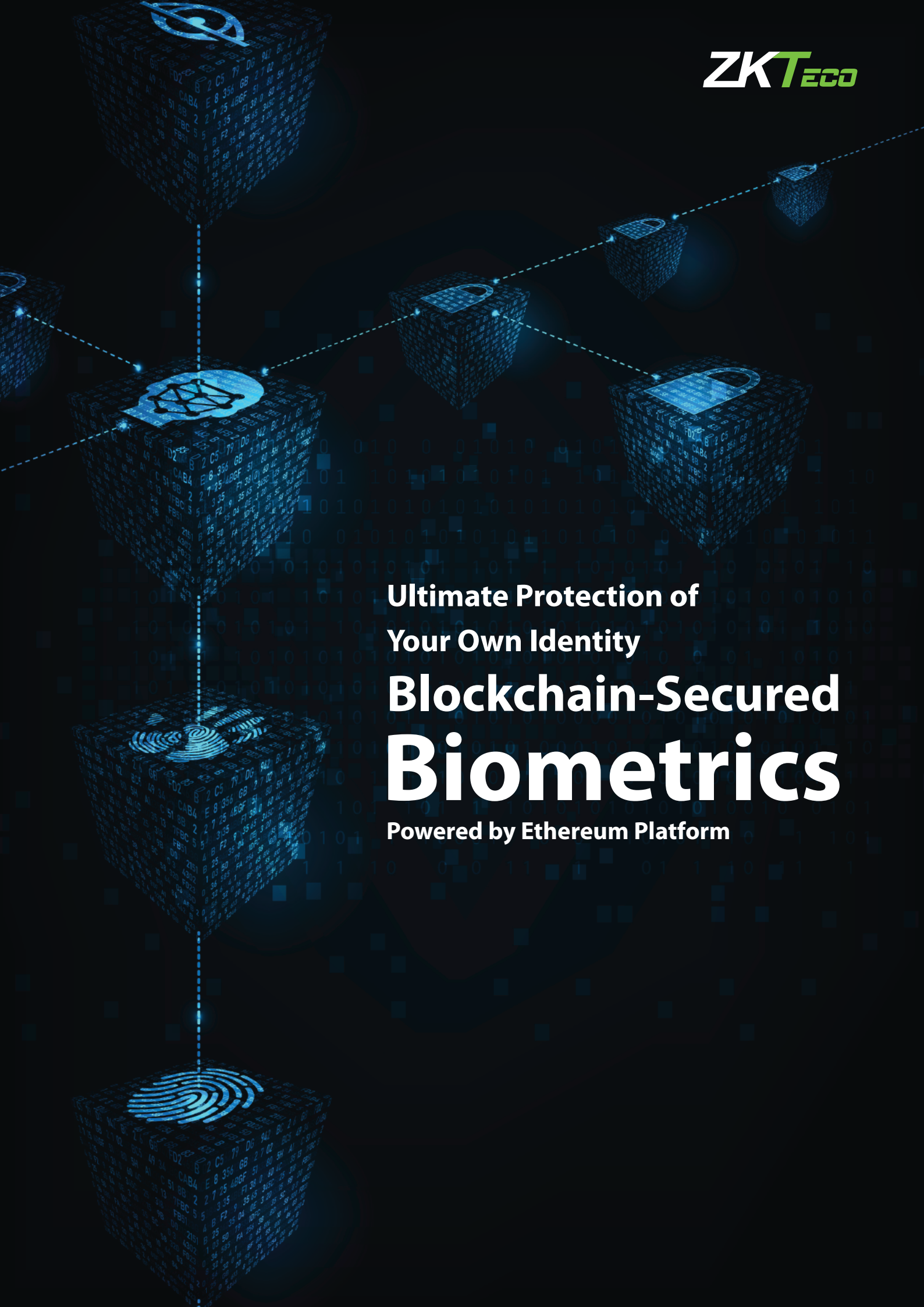


ZKTeco

Ultimate Protection of
Your Own Identity

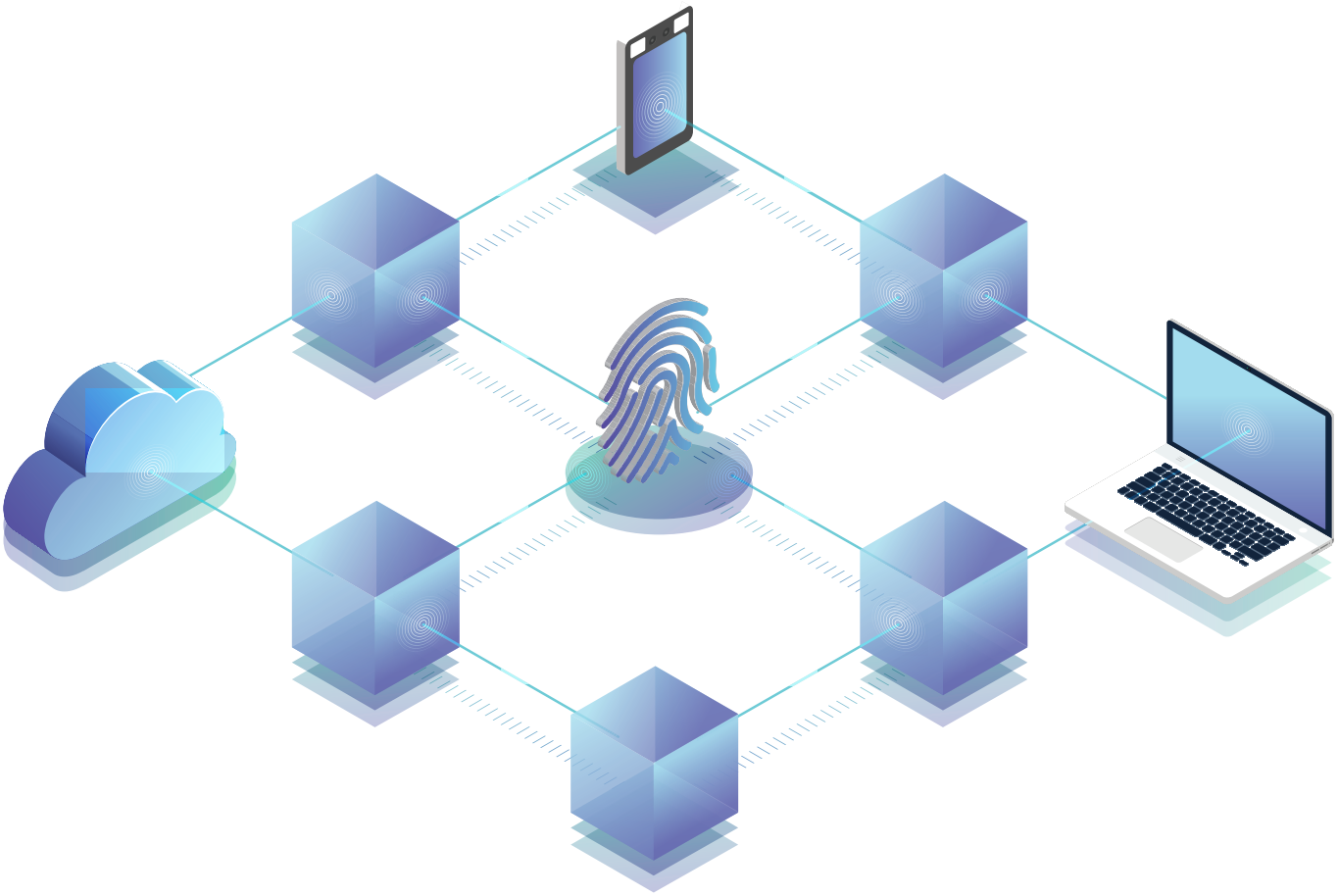
Blockchain-Secured Biometrics

Powered by Ethereum Platform

Background

Blockchain has been one of the hottest technology topics in recent years as people have started paying a lot attention to it. Since Bitcoin (the very first cryptocurrency in the world) first applied this technology in 2009, with unique P2P communication method, time stamp feature and immutable record of data characteristic, it has become a **supreme security transaction method**. Literally, Blockchain cannot be hacked in any sense. Of course every technology has its limitation, especially to the older ones. In Blockchain, the information format of blocks was standardized, no extra information was allowed to be added in the block, which limited the interaction between biometrics and Blockchain.

Moore's law indicates that, the processing power for computers will double every two years, so does the Blockchain development. **Ethereum** is the key concept of blockchain2.0, which greatly extends the concept of decentralization by extending Blockchain technology from cryptocurrency to all kinds of services by initialing a new concept of adding "attachment" in blocks. In Blockchain1.0, taking Bitcoin as an example, the information stored in the blocks is so standardized that except bitcoin itself, no other information can be added in the blocks. In **Blockchain2.0**, user may add more information in blocks to form a new concept of blocks, which are named as "Token". And the "Token" will be the key of the interaction between biometrics and Blockchain.



What is Blockchain?

Blockchain is a distributed ledger that is completely open to anyone in the chain. Once data is recorded in a block, it becomes **very hard to change.**

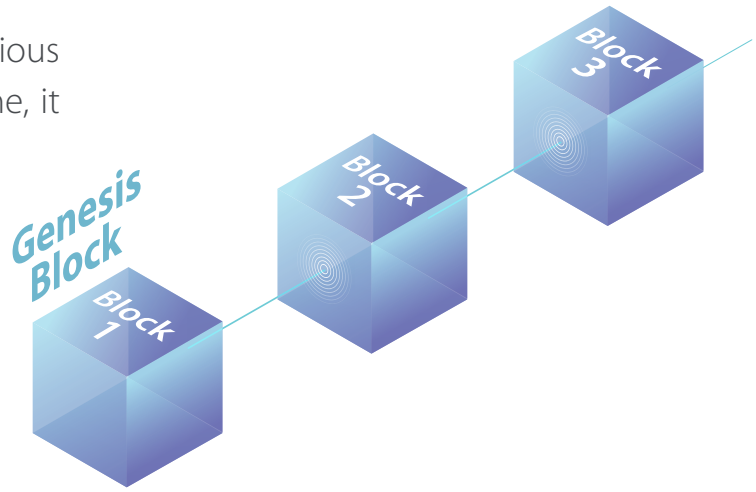
Each block contains **"Data"**, **"Hash"**, and the **"Hash of the previous block"**, the data stored inside the block is subject to the type of Blockchain. For example, a biometrics Blockchain stores details of biometrics templates such as template type, registration date, user name, registration terminal SN etc.

Each block has a unique hash, users may identify blocks and contents by their hashes. Once a block is created, if there is any changes inside the block, the hash will also change. In another words, the **hash will indicate changes of the block**, if the hash of the block changes, it no longer is the same block.

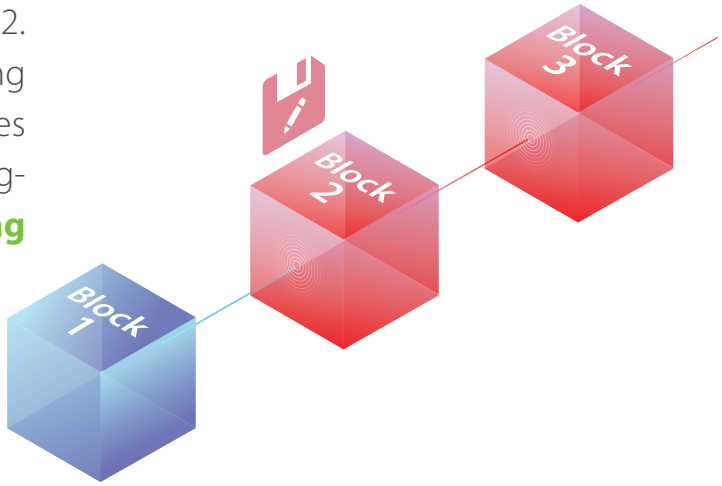
The third element of the block is the "hash of the previous block", it effectively creates a chain of block, and this element makes the Blockchain so secure.

For example, here we have a chain of 3 blocks, each block has a hash and a hash of the previous block, so block 3 is linked to block 2, and block 2 is linked to block 1.

Block 1 cannot be linked to any previous block because it is already the first one, it will be called the **"Genesis Block"**.

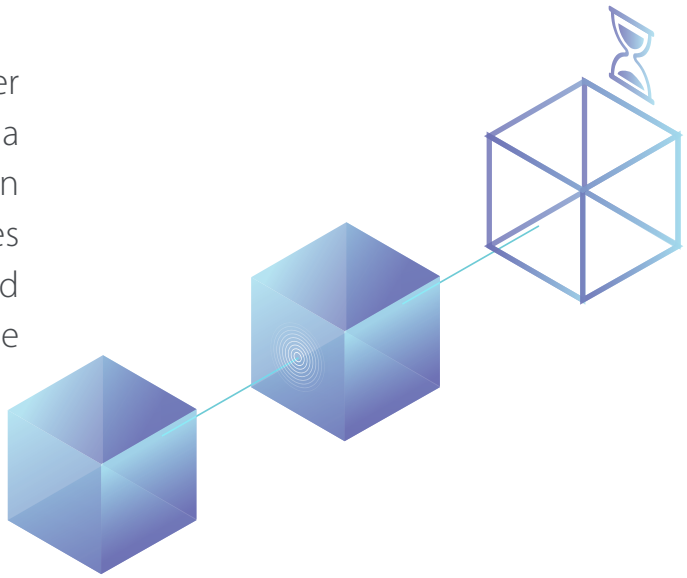


If any user attempts to tamper block 2, it will also **change the hash** of the block 2. Therefore, block 3 and all the following blocks will be invalid, as it no longer stores a valid hash of the previous block. Changing a single block will make **all following blocks invalid**.



However, because the processing power of the latest computers are very fast, only relying on **hash is no longer enough** to prevent tampering. Hackers' computer can easily calculate hundreds of thousands of hashes per second, thus hackers can effectively tamper blocks and recalculate all hashes of the other blocks to make the Blockchain valid again.

For this problem Blockchain has another mechanism called **"Proof of work",** it is a mechanism that slows down the creation of new blocks. For example, Bit才oin takes about 10 minutes to calculate a required proof of work and add a new block to the chain.



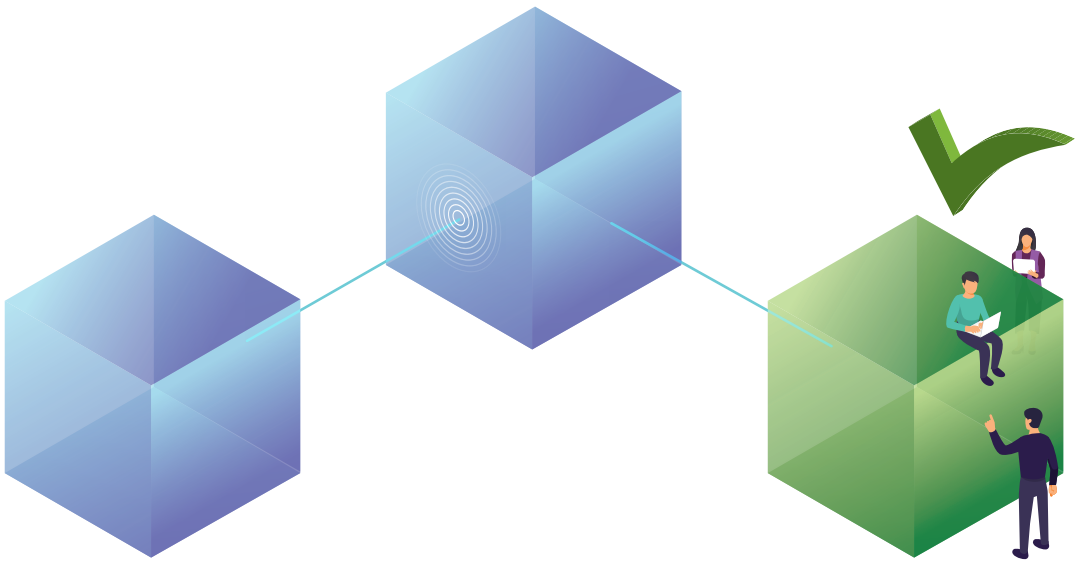
This mechanism make it **very hard to tamper** blocks, because if a hacker tampers a block, he needs to recalculate "proof of work" for all the following blocks. If there are 10,000 blocks available in a Blockchain, it will take the hacker 100,000 minutes to finish all the proof of work process, which is almost 7 days.

Therefore, the security of the Blockchain is very solid with the above measures, but there is **one more way** that Blockchain secures itself by being distributed instead of using a central entity to manage chain.

Blockchain uses **P2P network** and everyone is allowed to join. When someone joins a network, he gets the full copy of the Blockchain, which is called **"node"** to verify that everything is properly in order.

If someone creates a new block, the block will be sent to everyone within the network, **each node will verify** the block to make sure it has not been tampered.

If everything is checked, each node adds this block to their own Blockchain. All nodes in this network reach to a consensus, they agree about what blocks are valid and which are not.



Blocks that are tampered will be rejected by other nodes in the network. Thus, to successfully tamper a Blockchain, you will need to tamper all blocks in the chain, re-do the "proof of work" for each block and take control of more than 50% of the peer to peer network, only until then will your tampered block become accepted by everyone else, which is almost **impossible** to do so.

How Blockchain associates or interacts with Biometrics?

Without any doubt, Biometrics is the best way for identity recognition, especially with the help of the recent technology boom, the speed, and accuracy of biometrics have reached a new height. However, in most advanced regions, the application of biometrics technology is slower than it has been expected, and the reasons are pointing to the **privacy concern**, even most of the biometrics terminal does not actually capture the bio-features, but it cannot stop the panic form public. Finally, **Blockchain** seems to be **the end of this problem**.

In the soon future, all the biometric compliances will **not save any biometrics templates**, all the template will be stored in the Blockchain, which is supposed to store in cloud servers.

User will have a delegated **"Token"** to access to its own biometric block, without the "Token", no one can access or edit or delete or overwrite any information in the block.

When a user needs to use their biometrics templates, they will need to **activate** the token to access the block to open their biometrics template, and then grant a **one-time usage right** to the biometric terminal for recognition. After the recognition process, the biometrics template will be **eliminated** from the terminal.