CRYPTO-BOOM

15 NOVEMBER 2021

NAQIZ & PARTNERS

CLIENT ALERT: CRYPTO-BOOM

Author: Lo Khai Yi
(khaiyi@naqiz.com)

News relating to cryptocurrencies, non-fungible tokens (NFT), blockchain, blockchain assets, distributed ledger technology, etc. have pretty much dominated the social media news feed of most internet users these days – Ethereum surging to a new all-time high, Squid Game's creators (no, we are not referring to the hyped Korean series on Netflix, but the cryptocurrency which was obviously "inspired" by it) did a "rug pull" and absconded with millions of investors' money, creators of SushiSwap did something similar as well, Bitcoin having just gone through its first major upgrade in 4 years, numerous alt coins that have folded their values 10 times or 100 times. With all these headlines, it is no wonder that "crypto" is the buzzword right now.

What does "crypto" actually mean? What does it stand for? We are going to discuss the technology behind "crypto" in this article for the geeks out there.

Cryptography

"Crypto" is short for "cryptography", which is defined by Oxford Languages as the art of writing or solving codes, a.k.a. encrypting and decrypting. It is the fundamental enabler of the underlying technology behind blockchain, a distributed ledger technology, or more commonly known as DLT.

Believe it or not, cryptography is not new. Its first use case can be traced back more than 2,000 years ago to Julius Caesar. At a time where written correspondences were very much prone to interceptions and leaks, Julius Caesar invented an encryption mechanism for his written correspondences such that the order of alphabets are rotated 3 positions to the back (for example). This way, alphabet "A" would be replaced by "D", "H" replaced by "K", "Z" replaced by "C". This type of cryptography is now known as the "Caesar Cipher" and is one of the many forms of rotational cipher.

Essentially, a "cipher", is an algorithm to obscure (encipher) or reveal (decipher) information. A cipher transforms plaintext (the original information) into cipher text (coded information).

Modern day cryptography is really just an extended version of cipher that is made possible with advancement in computational power, and is generally referred to as "hash". While both hash and cipher have similar concept, cipher is generally reversible (meaning a cipher text can be reversed into plaintext), hash is generally irreversible. When a plaintext is hashed with a cryptographic hash function (or commonly known as a "key"), it is transformed into a series of numbers or strings known as "hash code" or "digest".

It is important to note that a strong cryptographic hash function needs to have these 3 criteria: (1) the same plaintext should (almost) always hashed into the same hash code; (2) minute changes to a given set of plaintexts should (almost) always create very distinct hash code; and (3) hashing the hash code will not reveal the plaintext. Due to these characteristics of cryptographic hash function, it is often used by online services to store users' passwords.

Since what are essentially stored on the online services' database are the hash codes (instead of the users' passwords in plaintext), a compromise of the database will not directly result in compromise of users' credentials.

Public-Key Cryptography / Asymmetric Encryption

So how does cryptography relate to blockchain? We will get there soon enough. Spoiler? It has something to do with this variant of cryptography called the Public-Key Cryptography, also known as Asymmetric Encryption. For those of you who have been following Naqiz & Partners' publication, you would have come across a similar sounding term in our article on digital signatures.

Public-key cryptography, also known as asymmetric encryption, is a cryptography that utilises 2 sets of cryptographic hash functions – which are typically referred to as the "public key" and the "private key", forming the "public-private key pair". Public key, as its name suggests, would be the key that is accessible by the public; on the other hand, private key is the key that is possessed only by the owner of the public-private key pair. Each of the public-private key pair is unique, and the pair reverses the effect of one another. Supposedly, hashing a plaintext with a public key will generate a hash code, when the generated hash code is hashed with the private key, the output will be the plaintext that was earlier hashed / encrypted with the public key. Neither hashing the hash code again with the same public key, nor hashing the hash code with a private key from a different key pair, will reveal the plaintext.

This mechanism forms the backbone of end-to-end encryption technology that is used by many online services (think WhatsApp). As WhatsApp users, we each have our own unique public-private key pair. Assuming end-to-end encryption is enabled, when I am sending a text read "Hello, World" to you on WhatsApp, the message will be encrypted using your public key (which is blasted and made known to your contacts), and be sent to you in a series of randomised strings or numbers (the hash code). Upon receiving the message in the hash code, you will then decrypt it using your private key that is only known and possessed by you, and reveal the text "Hello, World". Of course, all these encrypting and decrypting are happening at the backend level of WhatsApp without us having to perform any task on our own.

Digital Signature – Inverse Asymmetric Encryption

A digital signature adopts the inverse of asymmetric encryption. When you are signing a document digitally, several processes would take place:

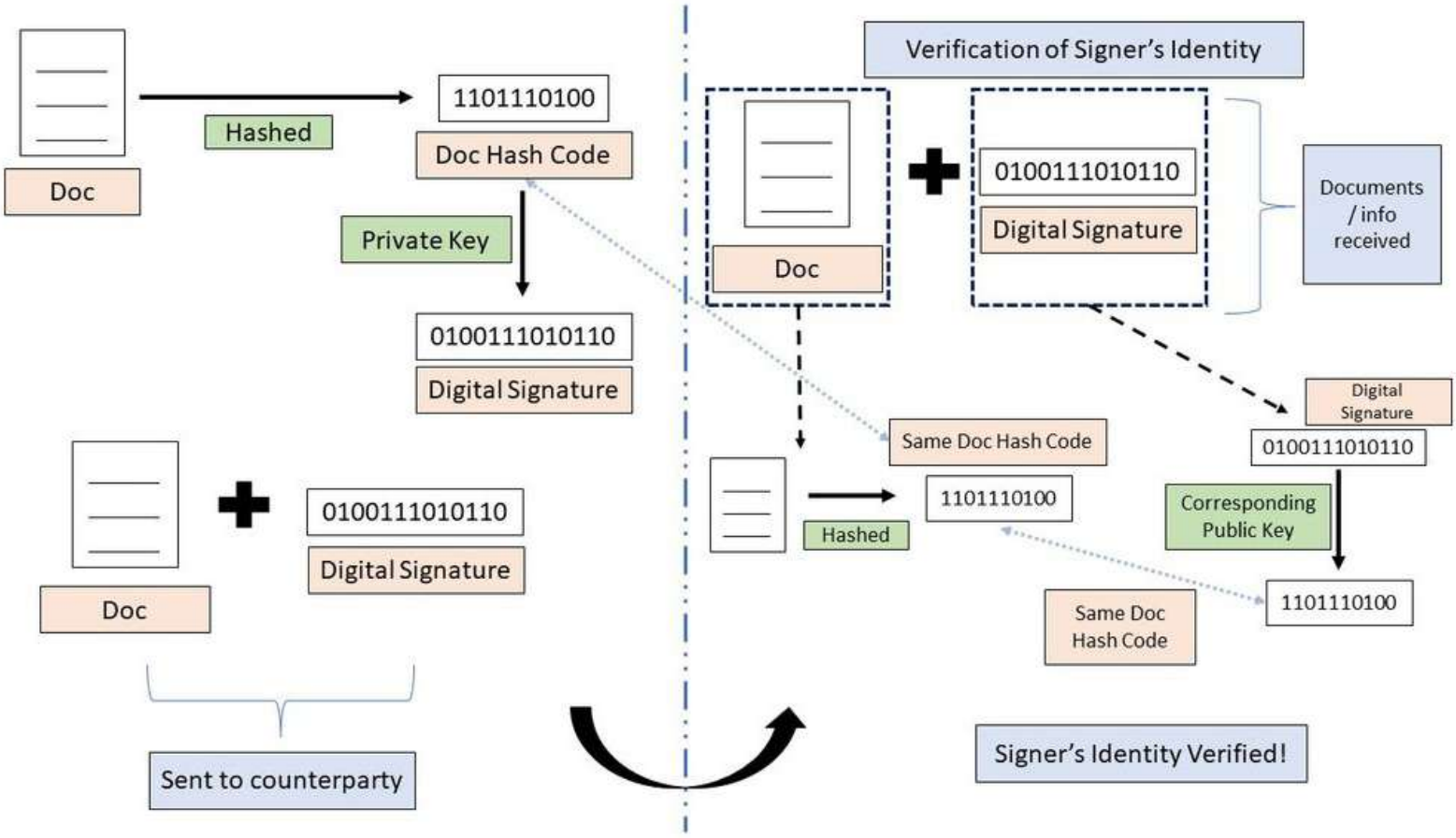
(1) The document to be signed is hashed with a specific hash function (usually widely adopted cryptographic hash function such as SHA-1, MD-5, MD-6, etc.) into a unique hash code **("Doc Hash Code")**;

(2) The Doc Hash Code is then encrypted with your private key, forming your digital signature, which is also in the form of hash code **("Digital Signature")**;

(3) To verify whether the document is indeed signed by you, we simply have to perform 2 tasks:

a) hashing the original document with the specified hash function, which should then generate the same Doc Hash Code from step (1); and

b) decrypt your Digital Signature using your public key, revealing the plaintext, which ideally should be the same hash code that we got in step 3(a) (the Doc Hash Code).
If the hash codes generated in step 3(a) and 3(b) are identical, we can then be sure that the document was indeed signed by you, and vice versa.

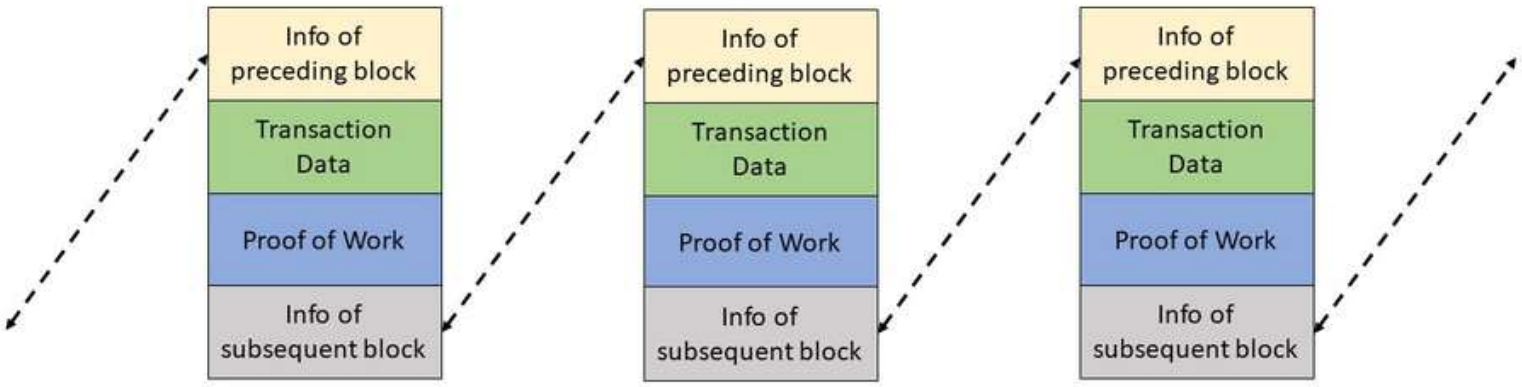


Blockchain

Now that we have understood the different types of cryptographies, we can better appreciate the mechanism of blockchain.

Blockchain, as its name suggests, is really a chain made up of blocks of information, each block connected to the one before it and the one after. Computer scientists sometimes refer to this sort of data structure as a "linked list". Cryptocurrencies in general are based on blockchain technology. They are decentralised, which means there is no one single authority that governs the system, unlike fiat money. Instead, the blockchains are self-regulated by their users such that copies of the blockchains are distributed to all its users and are all updated concurrently. For ease of discussion, we are going to talk about blockchain with particular reference to Bitcoin, considering that it is the most commonly known cryptocurrency at this point in our opinion.

A single block on a blockchain can be dissected into 4 sections: (a) a section that stores information of its preceding block; (b) a section that stores information of its subsequent block; (c) a section that stores data for which the blockchain protocol is built for – in the case of Bitcoin, the data stored are the transactions made with Bitcoin, all of which are digitally signed by the persons initiating the transactions (the **"Transaction Data"**); and (d) a section that stores the "Proof of Work", or POW for short.



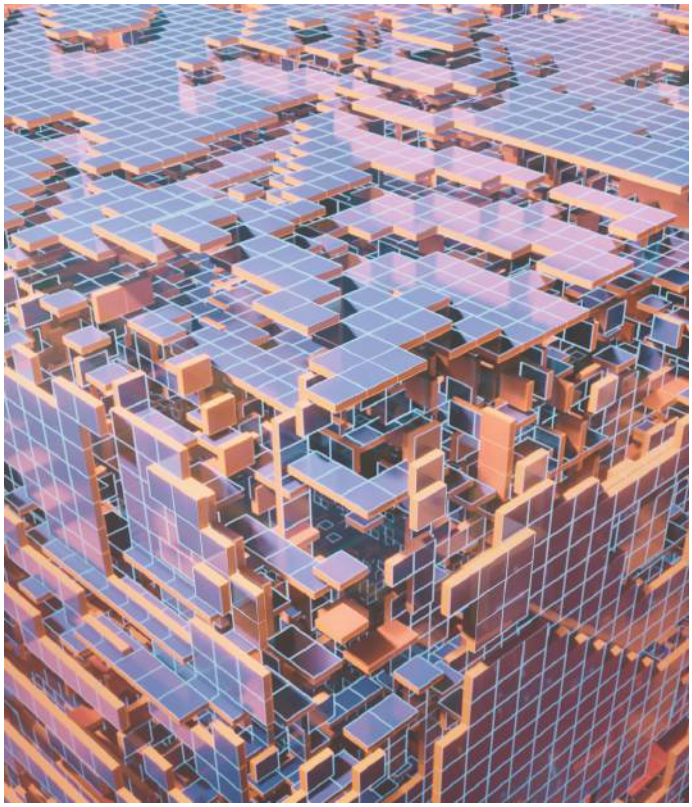
The POW is what essentially validates a block and allows it to be added to the blockchain.

Due to the lack of a central regulating body, each block to be added to the blockchain is required to be verified, and that verification process will generate the so-called "Proof of Work". Miners – who are actually just a group of people hashing the Transaction Data with cryptographic hash function over and over in combination with some random numbers, looking for an output cryptographic hash code that is "unique" (for example, a series of ones and zeroes that starts with 30 ones – just for context, the probability of finding such a unique hash code is $1/2^{30}$).

When such a unique hash code is finally found through the hashing of the Transaction Data in combination with a particular number (say "15112021"), the block comprises the Transaction Data will then be added to the blockchain along with the number identified. Due to the extremely small probability of a miner being able to find a set of specific numbers that when hashed with the Transaction Data will generate such a unique hash code, such feat is only possible with the help of large computational power and energy to pretty much brute force the equation by trial-and-error. At the end of the day, miners who successfully identify the set of numbers will be rewarded with Bitcoin for the labour.

To verify the work that has been done by the miners, one will simply have to hash the Transaction Data recorded on a block with the set of numbers identified by the miners to see if the hash code generated is indeed the unique hash code identified.

From the illustration above, we can see that cryptography technologies are abundantly used in a blockchain protocol, and in fact the technology is what makes a blockchain protocol more secure than others.



Without going too much into the specifics, tampering with a blockchain is infeasible because of how each block is linked end-to-end – tampering the Transaction Data on a block will result in a mismatch in terms of the hash codes recorded on the blocks before and after it; because of a blockchain's distributed mechanism, altering one copy of the blockchain means nothing if the rest of the copies are not altered (and it is impractical and close to impossible to alter every single copies of the blockchain considering:

(1) the number of users who own a copy of the blockchain; and
(2) the domino effect that will be created by tampering with a block as explained.

By now, we hope you will have a better understanding of cryptography, and how it is being utilised in cryptocurrency protocols. Of course, you do not have to have full grasped of how the technology works before you can own cryptocurrency or adopt the technology. Considering the attention the technology has garnered over the years and the huge potentials for future adoptions and use cases, we strongly believe the technology will bring forth a wave of change that is unprecedented in the cyberspace, and possibly even blurring the line that has long been segregating physical and the cyber realms.

As the forward looking firm that we are, Naqiz & Partners will publish more articles relating to cryptocurrency, cryptography and their various forms of adoptions such as NFTs, smart contracts, metaverse, etc. in our future articles. Do stay tuned.

NAQIZ & PARTNERS

Suite 9B.02, Level 10,
Wisma E&C,
Lorong Dungun Kiri,
50490 Damansara Heights,
Kuala Lumpur

+603 2095 1188
www.naqiz.com