December 2020
To all industries

METEORA SYSTEM Co., Ltd

# Quantum-resistant blockchain

## Potential of industrial innovation

Looking back, Japan had many world-class inventions such as the Walkman and iMode. Unfortunately, however, it is now a country behind iPhone, Android and Huawei. Please take advantage of the fact that I, as a Japanese, have secured a number of patents and copyrights that support the quantum-resistant blockchains and its mathematical basis.

## [Developer biography]

Eiji Watanabe
After graduating from the Department of Electronic Engineering, Tokyo Denki University in 1964, he joined JEOL Ltd. After that, he was enrolled in Fujimic Inc.(Think Tank) until 1972. Established Meteora-System Co., Ltd. in 1979, and formed a capital tie-up with Amada Co., Ltd. in July 1982 (the capital tie-up was dissolved in March 2005). Established Post Quantum Bit Co., Ltd. in 2018 with a patent in-kind investment. As an inventor, I have established 1) A technology that interrupts the establishment of a connection at the subnet TCP / IP layer when any unknown backdoor (setup is past tense) is activated. 2) Boundary defense line created by the non-commutative algorithm.

## [Post-quantum cryptography and commutative algorithms]

On October 24, 2020, NIST entered Round 3 of the post-quantum cryptography standardization process and announced the finalists. ☞ https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions. The current public key scheme is commutative between encryption process and decryption process (commutative algorithm). Techniques for making this commutative relationship stable quantum-resistant are usually difficult to achieve (with one exception). Therefore, NIST decided to divide the public key scheme into three schemes: (1) Public-key encryption scheme, (2) Key establishment scheme, (3) Digital signature scheme, and proceed with the standardization process for each of the three schemes (let it referred to as NIST standard scheme). This means that the quantum-resistant of the commutative algorithm is difficult to achieve.

## [Expectations for non-commutative algorithms]

On the other hand, the title is a new blockchain that integrates the feature of key management

based on a non-commutative algorithm and the feature of the NIST standard scheme. The non-commutative algorithm-based key management is a technology (Mathematical defense) that specializes in information-theoretic defense rather than the current computational difficulty. There is no need for standardization because the only attack that breaks the information-theoretic defense is to roll the dice. This is a feature of non-commutative algorithms.

[The title = Key management by the non-commutative algorithm + NIST standard scheme]

For example, when we assume digital financial assets, I think we should seek perfect consumer protection. The title solved this challenge by "Integrating Key Management with Non-Commutative Algorithms and NIST Standard Schemes". This has made it possible to *protect user privacy*, *neutralize cyberattacks*, and *implement protocols to stop money laundering* (illegal remittances). I posted this logic in "Multivariable Digital Currency" on the same site.

[Image from the consumer's perspective]

A wallet is also required for digital financial assets. Your smartphone becomes a hard wallet. In the quantum resistant blockchain, while smartphones become wallets, their "deposit accounts" can also be managed. The management method is a device different from the wallet. For now, we are assuming a "wristband".

Your smartphone is your wallet. Meanwhile, the "wristband" opens / closes the "deposit account": In an emergency such as when you lose your smartphone, your wristband closes your "deposit account", i.e., no password.

”Euro watch”, ”Apple watch”, ”Libra watch”, and …

Blockchain (guaranteeing anonymity) does not allow you to temporarily close your "deposit account". This is why consumers cannot be protected. This is also the reason why money laundering cannot be stopped. On the other hand, the private key can be erased by the non-commutative algorithm. This establishes *a line of defense* that protects the private key from the unspecified. This made it possible to remotely close the "deposit account". In fact, let's move on to the non-commutative algorithm.

[In fact, when moving to the non-commutative algorithm ... even if confidential information is leaked ...]

It is impossible to stop the information leakage itself. When the leaked information B is used,

the system does not distinguish it from the original information A. Whichever is used first gives the same result: the original information A and the leaked information B are *commutative, i.e., AB = BA.* Now let's move on to non-commutative algorithms. It is assumed that the key information A is leaked and the cyberattack obtains the information B. An attacker wants to use information B on the net as a user of key information A. When it is the commutative algorithm, AB = BA, so the attacker can also be a user (the attack succeeds). However, *in non-commutative algorithm, since AB ≠ BA, so the leaked information B is useless.* For this reason, the non-commutative algorithms provide *a line of defense* that protects consumers from various crimes. That is, it protects our privacy and financial assets. Similarly, it makes currency forgery difficult and protects the trust of currency issuance. And you will have a protocol to stop money laundering, that is, you will be able to close your "deposit account".

## [Don't ask for password registration: because the user side manages the account]

Let's think about your account. We have long believed that a user's account is managed by the service provider: here we ask for a password and so the service provider manages the account.

When moving to the non-commutative algorithm, password registration is not required. The user side manages the account. The user side is the user, the exchange, and the third party. When the collision function $Y^{-1}()$ verifies the consent of these three people, the user can log in to the signing task. Thus,

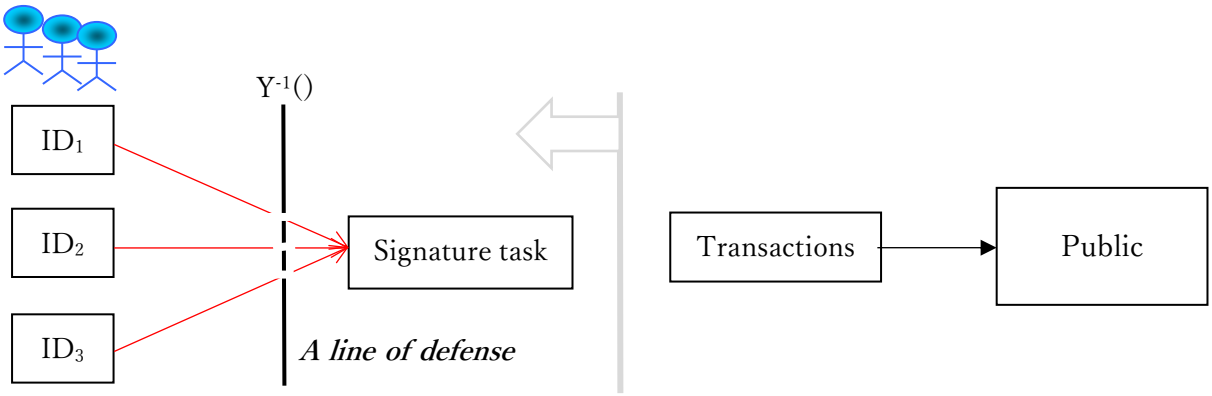


Fig.1: Three login IDs will appear.

The login ID ($ID_1$ $ID_2$ $ID_3$), the collision function $Y^{-1}()$, and a communication protocol correspond to a current account. The collision function $Y^{-1}()$ is quantum resistant, and not only that, no attack can successfully deceive the collision function $Y^{-1}()$ in real time: in short, any cyberattacks are neutralized.

## [Potential of industrial innovation]

Quantum-resistant blockchain updates existing industries. It can also be applied to the financial

field as "multivariable digital currencies". There is no day when we do not see wallets and banknotes (fiat money). Banknotes have the characteristics of being "visible," "not having a user ID," "payable by hand," and "not limiting the freedom of people."

Digital currencies can be given the same characteristics as banknotes above. That is, multivariable digital currencies are compatible with banknotes. Central banks should have no objection to "compatibility with banknotes" (see Table 1).

| Character | visible | not having a user ID | payable by hand | not limiting the freedom | A chest of deposit |
|---|---|---|---|---|---|
| Fiat money | ○ | ○ | ○ | ○ | ○ |
| Gold | ○ | ○ | Stop double payment | ○ | ○ |
| Multivariable DC | × | ○ | Stop double payment | ○ Note 3 | ○ |
| Bitcoin Use password | × | ○ | Stop double payment | ○ | ○ |
| デジタル人民元 Use password | × | × | ○ | × Note 2 | × |
| CBDC Use password | × | × | ○ | × | × Note 1 |

Table 1: The non-commutative algorithms can close "deposit accounts".

Note 1: Japanese people trust cash because banknotes guarantee anonymity. Since there is anonymity, it is possible to make deposit in a chest of drawers. This is one of the reasons why cashless payments are not widespread in Japan. The ongoing CBDC could also be a means of collecting deposit in a chest of drawers, with interest rates. The possible CBDC, which guarantees anonymity, will be widely loved for a long time. we would like to expect such CBDC from the central bank.

Note 2: In general, it tends to be designed based on the logic of the issuer, but multivariable digital currencies are in the position of consumer protection, to protect privacy and financial assets, as well as to have protocols to block money laundering. The logic of the issuer is "mere IT", but the logic of multivariable digital currencies is "Money". It is possible to operate that "mere IT" can be used for daily shopping, but not for purchasing airline tickets.

Note 3: Gold, banknotes, and multivariable digital currencies do not limit human freedom. Also,

no password is required. This is the reason why "money" becomes current.

[Global innovation caused by Japan]

Looking back, Japan had many world-class inventions such as the Walkman and iMode. Unfortunately, however, it is now a country behind iPhone, Android and Huawei. Please take advantage of the fact that I, as a Japanese, have secured a number of patents and copyrights that support the quantum-resistant blockchains. I am convinced that Japan has a chance to take the lead again. If Japan does not take the leadership, "Euro watch", "Apple watch" and "Libra watch" will be loved by people all over the world, and Japan will become Galapagos again. Because of these concerns, we welcome not only license candidates, but also *those who are willing to take part in the overall innovation that this non-commutative algorithm causes*. This message can be used both domestically and internationally.

In relation to the above, we are also ready to license a technology (PoC completed) that automatically disconnects the connection at the subnet TCP / IP layer when an unknown backdoor starts its activity. This will be a distinguishing factor between 5G and 6G.

Updated January 28, 2021