Table 1

Multivariable digital currencies

Invention to prevent digital currency from becoming money laundering and terrorist financing

Table 1: Currency convenience comparison

Exchange means (money)	Convenience	No need to trust government: no need to trust a single will.	Privacy integrity*	Ability to issue currencies to meet economic demand
Gold, platinum, silver	✕	◎	◎	✕
Bitcoin	✕	◎	△ *	✕
Fiat money ¥, $	◎	✕	✕ **	◎
Central bank DC	◎	✕	✕	◎
Multivariable digital currency	◎	◎	◎	◎
	Compare with La valeur d'être (cells of ◎) of Gold The result of social implementation of multivariable blockchain.			

* Since the design of Bitcoin lacks key management, I made privacy integrity △.

** Fiat money is marked ✕ because its account could be monitored by authorities with "My ID".

Social implementation of multivariable blockchain n=3

In multivariable digital currencies, the key for signing (a private key) is "burned" and there is no key data: the key exists only as a function. The ash that remains after burning is called the multivariable digital IDs n = 3: The equation n = 3 means three variables.

Each of the three variables is implemented in society (user, exchange, third party), but any key data is not implemented.

Table 1

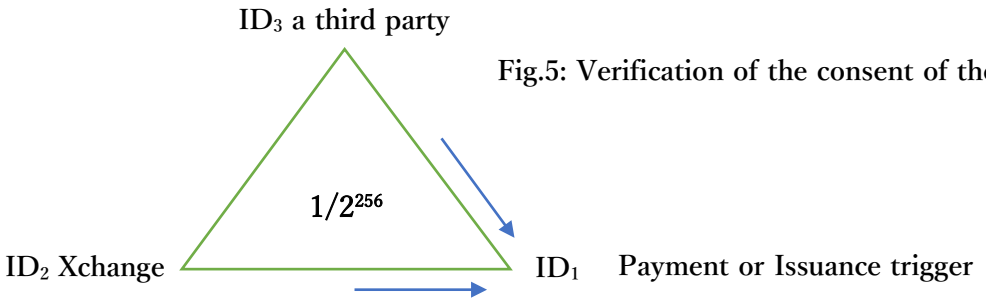

Fig.5: Verification of the consent of the three parties

1) No remittances will be made without the consent of the three parties: No remittances will fail-safe against accidents and crimes.
2) Having a collision function that verifies the consent of the three parties is more reliable than a settlement made by a single will.

Fiat money ¥, $ and central bank DC have a single will to issue. However, in multivariable digital currencies, three variables verify the consent of the three parties. It is not a single will, but the consent / disagreement of the three parties. In general, it is more reliable to verify the consent of three parties than to verify a single will. I have something to remember about this: the separation of the three powers democracy is more credible than the single will of one-party dictatorship: Democracy is not the best, but not the worst.

Currency issuance system to replace mining

Each of the three variables is implemented in society (user, Xchange, third party), and the three variables perform the signing procedure. These three parties do not always agree to the signature. In fact, the output of the collision function (☞ text PDF) is divided into either consent or disagreement. In case of disagreement, after several steps,

1) Separate only money laundering from remittance procedures. Money laundering assets are frozen.
2) No key data is implemented. Cyberattacks have lost sight of their targets, and consumer crypto assets are in a logically protected state. (don't say your assets are gone!). further,
3) The verification of the consent of the three parties becomes the entity responsible for issuing money. The three-party consent verification is a currency issuing system that replaces Bitcoin mining.

© Author
Eiji Watanabe
METEORA SYSTEM
October 25, 2020