THE CORPORATE INVESTMENT TIME...
corporateinvestmenttimes.com
CORPORATE INVESTMENT TIMES
Time to think about the future of money
An Impactful Milestone Ahead: AI-based Quantum Money evolution
Amnon Samid
The user decides, the user is in control
BitMint
Trans-Vernam
Vernam
RANDOMNESS
JUNE 2023

The user should be the stakeholder of the data, the money and the level of privacy. This new user approach shifts control from the remote designer to the engaged user, who is the rightful claimant

- We need Harassment-Resistant people's digital currency that will gain public trust, by avoiding surveillance and censorship, by preserving cash-like privacy when two parties (human or devices) trade with digital money, by everyone, everywhere, anytime, and that offers disruptive use cases that does not exist today with prevailing payments protocols.

Time to think about the future of money

An Impactful Milestone Ahead: AI-based Quantum Money evolution

Amnon Samid *
Cyber-security and digital currencies expert
amnon@BitMint.com

Originally published at the Corporate Investment Times Magazine, June 2023 edition

https://corporateinvestmenttimes.com/downloads.php?edition=June-2023-AmnonSamid

Freedom and dignity begin with privacy

Innovation and personal-reorientation emerge from an unviolated personal space. The more integrated we are on this earth, the more our privacy, freedom and dignity are at risk, and the more difficult it is to uphold this societal foundation.

Money is the life blood of society. It is how society manages its resources to satisfy its need for progress. From a societal point of view - money is a means to:
- move people in a civilized way towards societal goals,
- means for the more fortunate to help the less fortunate,
- means to provide the talented members of society with the resources required for them to help society with their imagination and abilities.

Money is written today as a number representing value, associated with meta-data embodying a pointer to its owner and expressing various attributes, such as US$, €, INR or Yuan, debit, credit. This is about to change with the vision of Quantum-Resistant, User-Centric, Dynamic-Response Smart Money, that is briefly presented in this article.

The user decides, the user is in control
BitMint
NO CLOUD
LeVeL
THE CIPHER WHO CAME IN FROM THE COLD
GIDEON SAMID
21st Century Bit-Wise Coin
Trans-Vernam
BitMint
Quantum Randomness Money
Two Quantum Security Strategies
RANDOMNESS
BitMint
NIST
COMPLEXITY
Vernam
InnovationSP.net
RANDOMNESS
Replacing Rigidity and Complexity with Randomness

The user should be the stakeholder of the data, the money and the level of privacy. This new user-centric approach shifts control from the remote designer to the engaged user, who is the rightful claimant thereto.

Users should be the stakeholder of the data, the money and the level of privacy

When you pay cash, you control how much money you pay, to whom you pay, who knows about the transaction etc. The same, when you talk face to face, you are in control. But when you wire money, or using a mobile app, or even a cryptocurrency, you do not know how the money goes from you to the payee, who knows about it, how much money will be deducted and how long will it take. Similarly, when you send a message over the Internet – assuming it is a private message, you do not really control how much security is projected from the transmitted data. It's Microsoft or another cryptographic vendor who chooses one cipher or another. In the best case, you can switch a cipher, but you sure cannot tweak the algorithm.

Quantum Money versus Crypto Money

Technology always serves as a major catalyst in changing the paradigm of monetary and payment systems, and the way we communicate with each other. Technology is expected to fulfil the big issues of today, security, privacy, freedom and democracy, as less and less people trust their political leaders in preserving their privacy and freedom of speech. In the past, the only way to purchase something anonymously was to walk into a storefront and pay with cash. Today, we have reached a milestone: a belated adaptation of the first patent for a cash-like digital currency per se (Samid, 2007), that covers a broad range of transactions, person-to-person, person-to-merchant, person-to-machine, machine-to-machine, continuous payments per time or per service. It is inclusive, does not require a bank account, can be used by all and accepted by all, it does not discriminate against age, gender, wealth or ethnicity. It is a secure payment instrument, online and offline, up to being quantum-safe, resilient, with extremely low levels of counterfeiting possibilities.

It is in sharp contrast to the electronic payment systems from the 90th, like the Avant card, backed by the bank of Finland, that was a kind of preamble to central bank digital currency (CBDC), or the similar stored-value payment platform, Mondex, that was tested by the National Westminster Bank (NatWest), in which a monetary value was recorded (not the money per se) on a computer chip. Both never gained wide acceptance. Credit and debit cards replaced them, and went also through an evolution from magnetic strip to EMV.

Sixteen years ago, two technologies emerged with the mission of conceptualizing into building a peer to-peer transaction network and creating a distinct form of cryptographically encrypted currencies. Both are decentralized distributed, however the first, is an AI-based, centralized minted user-centric quantum-currency (BitMint, 2007), and the second is a decentralized-minted crypto-currency (Bitcoin, 2009). The bitcoin is a currency that does not exist outside the protocol that defines it. Its decentralization is groundbreaking, but it gives too much aid and comfort to wrong doers. Although bitcoin and other blockchain-based cryptocurrencies operate in an unregulated space for a long time, they lack the necessary characteristics to become alternative currencies, an efficient medium of exchange, because of their volatility, speculative nature and high mining costs (energy-wise). On top of that, bitcoin and its variants rely on a fixed public/private key algorithm. Being 'fixed' turns it into a resting target for advanced cryptanalysis. Contrary to **Crypto-Currencies** and to most CBDCs that use one algorithm (usually ECC), assuming, but not proven, to be strong enough to withstand a smarter attacker, the **Quantum-Currency** does not rely on single algorithm and keeps changing the algorithms. Quantum-resiliency achieved through algorithmic mutation, the same way a Covid-19 virus mutates against the vaccine.

The following characters were demonstrated:

1. Payor-payee privacy with strong anti-money laundering weapon;
2. Payor-payee fast, frictionless, cross-border, instant settlement in online as well as in offline modes;
3. Payor-payee resilience: no need for peers’ approval;
4. Payment continuity when Internet is down;
5. User’s device - Hard Wallet in offline mode, or mobile phone in online mode, can split each coin with no network connection, while each split will have new value and new unique identity;
6. Continuous payment per time or service is enabled, relevant also for automated M2M and Internet-of Things payments;
7. Terms of use (‘Tethered-Money’, purpose-of-use) can be written on the coins themselves;
8. Serves unbanked and underbanked consumers, as well as non-technology-savvy users, all from top to bottom of pyramid;
9. Accommodating the potential for high transaction volumes;
10. It is not legacy bank accounts and it is not peer-dependent, nor a self-organizing network.

The Quantum-Currency coins are being issued by the Mint, generated from an analogue source of non-algorithmic quantum-resistant bits, while each digital coin has a unique alpha-numeric id, like a serial number on banknotes, that is separated from the coin value. The coin id sequence of bits is fully randomized, inseparable from the value function. Coins will retain unique id even after they split by the traders, with no need for network connection, which enables also continuous payments per time or service.

How to deal with the growing public sentiment against CBDC?

It’s the duty and obligation of central banks and governments to convince their citizens that they can trust CBDC, and convince citizens that it can provide added value over current payments rails, without robbing our privacy, while contributing to a more prosperous future. We know it’s achievable, but NOT with the crypto-based solutions that most central banks are currently evaluating.

We demonstrated in a real-world pilot that a proper digital currency solution, can be a secure payment instrument, up to being quantum-safe, covers a broad range of transactions, person-to-person, person-to-merchant, person-to-machine, machine-to-machine, continuous payments per time or per service, being inclusive, not requiring having a bank account, can be used by all and accepted by all, it does not discriminate against age, gender, wealth or ethnicity, and on top of that very user friendly and resilient, with extremely low levels of counterfeiting possibilities.

We have also demonstrated that a new user-centric cryptographic modality shifts control from the remote designer to the engaged user, who is the rightful claimant thereto.

- **We need** Harassment-Resistant people’s digital currency that will gain public trust, by avoiding surveillance and censorship, by preserving cash-like privacy when two parties (human or devices) trade with digital money, by everyone, everywhere, anytime, and that offers disruptive use cases that does not exist today with prevailing payments protocols.
- We need Harassment-Resistant People’s cryptography. We can now establish basic privacy and data assets security without resorting to mathematical complexity that smart hackers, and definitely stronger computers can break, by using randomness instead.

It’s ONLY a matter of decision, as solutions exist!

Consequently, two things are about to change in the near future:

- users will regain control on their money, privacy, data and communications, and
- the advantage held today by smarter adversaries and faster computers will be toned down.

A new landscape is about to dominate cyber reality.

BitMint Money flows phone-to-phone, phone to POS terminal, as well as off-line

* Amnon Samid is an engineer, cyber security expert, mentor and founder of technology companies. Amnon is managing the AI-based Cyber-Innovation Hub, BitMint, promoting quantum-cryptanalytic-resistant architecture for digital currencies and asset tokenization, and the LeVeL-Paying-Field protocol, to enable bilateral payment, that is homomorphic with cash payment, putting users in charge of their data, money and privacy. Amnon is among the pioneers of the migration from fixed-security cryptography to Dynamic Response User-Centric cryptography, empowering users by putting them in the driver’s seat, endowing them with the freedom to project security up to highest quantum-resistant, mathematical grade.