AUTOMATED EMBEDDED PAYMENT SYSTEMS

Amnon Samid

AI-Powered cyber–Innovation Hub, BitMint
Tel-Aviv, Israel

ABSTRACT

Payment industry is largely aligned in their desire to create embedded payment systems ready for the modern digital age. The trend to embed payments into a software platform is often regarded as first step towards a broader trend of embedded finance based on digital representation of fiat currencies. Since it became clear to our research team that there are no technologies and protocols that are protected against attacks of quantum computing, and that enable automatic embedded payments, online or offline with no fear of counterfeit, P2P or device-to-device to be made in real time without intermediaries, in any denomination, even continuous payments per time or service, while preserving the privacy of all parties, without enabling illicit activities, we decided to utilize the Generic Innovation Engine [1] that is based on the Artificial Intelligence Assistance Innovation acceleration methodologies and tools in order to boost the progress of innovation of the necessary solutions. These methodologies accelerate innovation across the board. It proposes a framework for natural and artificial intelligence collaboration in pursuit of an innovative (R&D) objective. The outcome of deploying these Artificial Innovation Assistant (AIA) methodologies was tens of patents that yield solutions, that a few of them are described in this paper. We argue that a promising avenue for automated embedded payment systems to fulfil people's desire for privacy when conducting payments, and national security agencies demand for quantum-safe security, could be based on DeFi and digital currencies platforms that does not suffer from flaws of DLT-based solutions, while introducing real advantages, in all aspects, including being quantum-resilient, enabling users to decide with whom, if at all, to share information, identity, transactions details, etc., all without trade-offs, complying with AML measures, and accommodating the potential for high transaction volumes. It is not legacy bank accounts, and it is not peer-dependent, nor a self-organizing network.

KEYWORDS

Payment, Finance, Digital, Privacy, Quantum, Security, DeFi, Mobile, Online, Offline, Cash, AI

1. INTRODUCTION

The payments industry, regulators, banks, third party payments providers as well as software and technology companies are largely aligned in their desire to create embedded payment systems based on digital representation of currency, and identified cyber resiliency, scalability and privacy as core features of embedded payment systems. However, designing them involves complex trade-offs between these three elements. For example, higher resiliency against cyber-attacks, especially from quantum computers, requires additional cryptography, which can slow down payment processing. Privacy must be weighed against the need to counter money laundering, terrorism financing and other illicit payments.

Digital Technology Ledgers (DLT), blockchain and alike are being praised as a technological innovation which allow to revolutionize how society trades and interacts. This reputation relies on the assumption that they allow mutually mistrusting entities to exchange financial value and interact without relying on a trusted third party, while providing process transparency. In this paper we critically analyze whether a blockchain based on elliptic curve, permissionless (e.g.,

DOI : 10.5121/ijesa.2022.12401 1

Bitcoin/Ethereum) or permissioned (e.g., Hyperledger/Corda), is indeed the appropriate technical solution for automated embedded payment, and contrast its properties to those of decentralized Mathematically Digital Coins – the Legacy Extended Value Entrusted Ledger (LeVeL)-Payment-Field technology.

Automated embedded digital money payment systems should focus on the full process from issuance to distribution, mindful of programmability and control. The challenge to do it right so that society and citizens everywhere anytime can leverage the new form of money -- cyber quantum money to advance prosperity, progress, accountability, equity, fairness and social justice. It is consistent with the design philosophy used by the LeVeL-Paying-Field designers, while considering as value added the need for payment privacy consistent with oversight accountability, and law enforcement. It also considered the added value of the requirement not to ignore the threat of quantum computers, but rather to project an effective defense against the coming quantum attacks.

Many papers have underlined some of the trade-offs that embedded digital money systems may face when deploying Distributed Ledger Technologies (DLTs), but still policymakers around the world and most central banks follow the buzz words or the business agenda of their vendors and continue to grapple with risk-prone crypto-based central Bank Digital currencies (CBDCs) and DLT based online CBDC solutions, just ignoring an emerging world of quantum-safe online digital currency that is already here under the banner LeVeL-Paying-Field, which will eventually enjoy legal and regulatory clarity, along with mass adoption.

Similar challenge with offline payment: Under the wrong assumption that a counterfeit-safe quantum-resistant offline payment solution is not in reach in the near future, the software/hardware-based solutions evaluated by several central banks are inferior from security and functionality aspects, and don't really provide payment continuity with final irrevocable payment through durable periods of damaged connectivity.

This paper aims to reconcile these challenges by combining proven technologies such as the LeVeL-Paying-Field [2] and the Tethered-Money [3] with the latest research on post quantum cryptography by professor Gideon Samid (Pattern Devoid Cryptography [4]).

The progress summarized in this paper rests on many years of research and development. These efforts became much more productive due to the profound contribution of 'Artificial Intelligence Assisted Innovation' (AIAI), summarized in reference [1], comprises on (i) a comprehensive exploitation of rich innovation history, and (ii) advanced Monte Carlo computation of credible estimates of cost to complete and time to finish the innovation process. The processor element includes the AI computation power, mainly: (a) AI engine; (b) Monte Carlo State Evaluation; (c) BiPSA [Binary Polling Scenario Analysis] operation; (d) multi-variate analysis; (e) The AI database, and (f) the Innovation^{SP} map processing.

2. MAIN CHALLENGES

The main challenge of an embedded payment system is to enable two parties (human or devices) to trade cash-like with digital money, whether Central Bank Digital Currency (CBDC) coins, or stablecoins, with no intermediators and not being dependent on a network of validators, in a connected environment (in which a public ledger is accessible) or in situations when connectivity is dysfunctional.

It is aimed to fulfill the vision of restoring the old way of payment with cash and to fit it for the digital age, capable of being owned, held and used directly by the general public, enabling

instantaneous, convenient, direct, peer-to-peer transactions, with the same level of privacy of trading with physical cash, for law-abiding users. Protecting privacy is key for digital money in order to maintain public trust, while maintaining quantum-grade cyber-security, resiliency and sustainability.

In principle there are two technology archetypes - Quantum versus Crypto – which may have a potential impact on resilience, sustainability, speed, financial inclusion, as well as usability and macroeconomic and microeconomics aspects. Therefore, the technology that underlines the digital money creation requires closer attention. As central banks consider sophisticated technologies that are superior to crypto-based solutions, cybersecurity up to quantum level, should be the primary concerns.

An embedded digital money solution should introduce a wide scope of attributes that makes it more attractive over other known payment rails. It should be Quantum-cyber resilient, centralized-minted, while traded in a decentralized manner, with a public ledger, being universally accepted, while achieving the following:
(i) financial inclusion;
(ii) privacy controlled by users;
(iii) not being a shelter for illicit activities; and
(iv) enabling offline payments during short or long periods of no Internet connection and no electricity.

2.1. What should we expect from embedded digital money payment in connected environment?

About eleven emerging markets have already rolled out digital currency, with expectations to enhance financial inclusion, reduce tax evasion and introducing alternative to cash and strengthen currency local position. It seems that they reciprocate the permissionless or permissioned-blockchain infrastructure, albeit its vulnerabilities, to create what seem to be an inferior CBDC compared to quantum-based CBDC, and on top of that not fulfilling all citizens' wish-lists. The only major economy that launched digital currency is China, following developing deep internal competencies around digital currencies and not rely entirely on vendors to establish a vision for the future of money in China. This includes hiring hundreds of team members, many of them technical people, as well as consultation with experts [disclosure: the author was one of them], followed by developing proof-of-concept projects in order for understanding alternatives, including the two main technology archetypes - Quantum versus Crypto. If Chinese strategy is to break the US dollar hegemony, they will definitely prefer the superior technology archetype – the quantum-random digital currency, assuming that the Federal Reserve as well as the European Central bank (ECB) documents still hinged on same encryption standard used by bitcoin. Chinese aim to introduce a better alternative and as such the Chinese CBDC, the e-CNY, may become the tip of a technological spear to spread a parallel global money movement network positioning the yuan as an attractive currency alternative [5], at least in Asian and Africa countries, by creating the most efficient digital currency under the planet, not being lured by crypto and DLTs promoters, and not ignoring the quantum threat.

It seems that the business interests of vendors that are aimed at crypto-based CBDCs, still set the rules of the game. This "brainwashing" has already permeated the public. Just for illustration: A survey published lately indicates that 45% of the Digital Euro Association (DEA) Community believes a CBDC should be built based on blockchain and digital ledger technology, while comments by 6% that recommend other technologies were not even published for the public to review [6].

The case for CBDCs in major economies is often framed as response to cryptocurrencies, stablecoins and the Chinese e-CNY. However, if you wish to bit another solution, you need to offer a much better one. The most prominent features that citizens expect from CBDC are value-added features, non-intermediated instant transactions online and offline, privacy preservation and censorship resistance. Central banks should worry about technological obsolescence, which characterizes the blockchain, cybersecurity (quantum-computers threat), monetary and financial stability and compliance concerns. Based on this wish-list we have to militate against most CBDC structures as presented up today. Among other risks that is being ignored, is the basic right of everyone everywhere to financial access.

We argue that not only account-based systems, like bank deposits, also token-or-value based approaches that transmit digital currencies peer-to-peer in decentralized manner based on DLTs with a consensus mechanism, are not efficient enough to make micropayments, pay-as-you-go, continuous payments, M2M and IoT payments attractive. It is not just the tokenization that enables these features, it's how the coin is structured at the Mint.

A CBDC to be accepted by citizens in most countries, needs to offer instant payment from payer to payee (whether a person or a device), with no-intermediaries, online and offline and being anonymous – cash-like, yet not enabling even the smartest adversary or the most powerful computer, up to quantum computers, to jeopardize the money, and not being an enabler for illicit activities, without violating traders' privacy (while privacy means that traders decide who will be exposed to their identity or the transaction details).

Apart from fulfilling privacy concerns, it's of digital currency issuers' responsibility, and especially if it is CBDC, to present a quantum defensive strategy that ensures that the digital money will stay live no matter what happens with quantum computers, how advanced they are. Which means that only quantum-safe digital currency should be deployed, not being dependent on the wrong assumption that we can add more and more complexity layers in accordance with the development progress of quantum computing.

An insightful document by a team of experts of the Digital Euro Association (DEA), "Ahead of the digital euro: Public Digital Euro Working Group Recommendations" [7] supports the need for fulfilling the above main uncompromisable requirements: "bilateral payment privacy", and the need for "a new approach that puts users in charge of their data", and citing the IMF saying that "Vulnerable algorithms will need to be transitioned to post-quantum cryptography". While the 3rd recommendation of the paper, says that "Failure to implement a robust cyber-attack-resilient strategy from day one (i.e., not just as a layer or complexity to be bolted-on) would not only compromise citizens' data and funds, but could put the entire eurozone stability at risk".

2.2. Peer-to-peer online payments – introducing a practical solution

A solution that fulfils all the above was shortlisted by the respectful G20/BIS TechSprint CBDC competition [8]. It is comprising of the BitMint's Qpay project [9], successfully tested by central and commercial bank, demonstrating digital currency coins creation which leverage the inherent cyber resilience of Quantum-Randomness, and of the LeVeL-Paying-Field [2], which provides Quantum-Defensive Strategy [*QDS*] for the entire cycle from issuing through trading and redeeming of digital currency. It is designed to serve the society, being a tool for prosperity of the community as a whole. It shied away from vulnerabilities related to validators review and avoid the algorithmic stagnation vulnerability of most CBDCs tested so far. It enables cash-like privacy without exposing identities to anyone with no tradeoffs, e.g., security versus privacy and ease of use [Disclosure: the author is involved with BitMint, the group behind these technologies].

The LeVeL solution is hinged on the fundamental experience of payor passing a transactable instrument of value to a payee, with no intermediaries, within a community-sanctioned protocol, while leaving to the parties to adjust their privacy to their needs. While the LeVeL privacy is robust, the LeVeL protocol has a built-in route for law enforcement to catch and prevent criminal activity. The LeVeL solution is universal and programmable; it applies to exchanging any financial instrument. Alas, the single most compelling argument in LeVeL's favor is the innovative solution to the threat of quantum computers.

It is imprudent to select a digital money solution that ignores the looming threat from quantum attacks. Most actors opt for increased mathematical complexity. We argue that such added complexity is wrong headed. The LeVeL defends against the quantum threat with algorithmic mutation: it does not rely on single algorithm, mostly the same encryption standard used by bitcoin that is based on the elliptic curve. It is definitely a risky strategy since we don't know what will be the nature of our adversaries' attack. With the LeVeL protocol each time a coin changes hands it adds another lock for the quantum locksmith to pick, another private key and another random algorithm. It is the count of the locks that keeps LeVeL coin safe.

The solution is based on fifteen years of careful design work motivated by the idea that cyber medium money can be fashioned as a most powerful tool to bring about progress, prosperity, fairness, equity and social justice. It considers as value added the need for payment privacy consistent with oversight accountability, and law enforcement. It also considers the added value of the requirement not to ignore the threat of quantum computers, but rather to project an effective defense against the coming quantum attacks.

2.3. Bio-inspired innovation [The algorithmic-mutations' advantage of LeVeL]

Algorithmic stagnation is the hidden fault in the sweeping success of crypto currencies, including those with CBDC aspirations. There is no excuse for a digital currency issuer to pick a digital currency platform to be of reliable long-term service, which has no good answer to the ticking bomb of the quantum threat. Some of those unprotected digital coins are very attractive on many counts, and some are being traded by millions. Such glaring success can blind the uncareful decision makers, but should not sweep away the good judgment of responsible policy makers.

Examining the so-called post-quantum digital currencies shows that they deploy a similar strategy: building up an extended computational complexity to be too much of a hurdle against the quantum dragon. We consider this line of thought unproductive. The reason being: the quantum threat is developed behind veils of secrecy. The public knows only what quantum developers want the public to know and not more. You cannot be sure that a computation hurdle will be good enough to forestall an attacking computer you don't know how fast it computes. The LeVeL team opted for an innovative turn. If you lock your treasure box with a lock, that would take 10 minutes for a locksmith to crack, then you cannot expose it for more than so many minutes. And it would not do, to sweat it and build a stronger lock, which will take 15 minutes for the locksmith to crack, or 20 or 30 minutes. What you can do though, is to fit your box with another lock, say every two minutes. Then, by the time the locksmith cracks the first lock, he will face five more locks, which will take him 50 minutes to crack, but in these 50 minutes you installed 25 more locks. On it goes -- you keep mutating the locks and guarding your treasure. Keep in mind that this only 'laymen-wording' for illustrating the defence strategy for non-technology savvy readers. One of the advantages of this approach is that you don't need to wait for quantum computers in order to introduce quantum-safe digital currencies. Todays' computers, Turing machines, are indeed much slower than quantum computers, but are fast enough to install new codes to be cracked at a pace that will keep the quantum machine always behind. The LeVeL coin is fitted with another lock every time it changes hands. The more it trades, the more secure it is.

Again: the innovative LeVeL solution is not based on adding more and more layers of complexity that eventually quantum computers will crack, but rather on using Turing machines to post more and more computational challenges to the much faster quantum predators, and safeguard digital commerce.

Covid escapes the high-tech vaccines that humanity throws at it, by the evolutionary tactics known as biological mutation. LeVeL escapes the ominous quantum threat through algorithmic mutation.

2.4 The basic embedded payment experience of LeVeL in cyber space

The LeVeL Paying Field was designed to implement the basic payment experience in cyber space, which is the core of the universal monetary exchange. Everything else is built on this foundation. The Basic Payment Experience in Cyber Space Payment is an interaction between a payor and a payee. In cyber space both payor and payee use a computing device, and are served with digital communication channels for these two devices to communicate with each other. Payment is expressed through a flow of a string of bits from payor's device to payee's device, and an optional digital receipt going the opposite direction. Payment is only meaningful in the context of a community of traders that need to recognize the act of payment. This recognition requires a network encompassing the members of the community of traders. For payment to happen the flow of bits from payor to payee has to be designed to assure the payee that it implies money transfer.

Furthermore, the community must recognize this transfer, and the right of the payee to pay that money to a third party. This is the basic payment experience: two members of a community, each holding a computing device, which communicates with each other -- carry out a payment. Please notice that this basic act does not require that either party will have an account with some financial institution; it does not require the parties to mutually identify themselves, nor do they have to surrender their identity to the community. The parties may be near each other or an ocean apart, may be acquaintances or strangers, may be friends or foes.

Two computing devices, a channel for bilateral communication, and community visibility -- that is all that is needed to exercise the basic payment experience in cyber space. Once this basic cyber payment experience is implemented, it can support a host of terms, conditions, restrictions, as the community sees fit. But these are overlaid upon the basic experience -- perhaps in a dynamic fashion.

We now let this vision of the basic payment experience to guide us to the simplest, most general, most secure, most intuitive design to bring this vision into reality. Operational assumptions: payor and payee have a sufficient supply of batteries to power up their computing devices, and to establish a bilateral channel of communication over short distances. The community of traders is served by a communication network that is at least intermittently operational.

We introduce the notion of a cyber coin: a digital string that represents a numeric value of a given currency. Payment amounts to a transfer of such coin from payor to payee. Unlike material transfer, a digital transfer leaves the transmitter with a copy of the transmission, it is therefore necessary to ensure that the payor cannot pay the same coin again, to another payee (by error or by malintent). We tackle the goal of so ensuring in two ways: one for the case where the network is on, and one for the case where the network is off.

We expect the network to be on most of the time, so we start with this case. Online LeVeL design elements: The essence of the LeVeL design is a two-face expression of a coin. One public and the other private. In its public expression a coin is known to the community at large, but in its private expression it is known only to the single trader that claims that coin as his or her own. By proving possession of the private expression of a coin, its owner proves his ownership thereof. While the

public ledger is a concept used by all digital currencies, the LeVeL offers an important distinction: the coin owner does not need to prove ownership to the entire community of traders (as in bitcoin), rather only to the payee, which checks it against the public expression which is listed on the public ledger. If they fit, then payee is satisfied that payer is indeed the coin owner. The payor complies and passes to the payee the private expression of the coin. In order for the payment to be carried out, the payee comes up with a private update for the state of coin. Only the payee knows this private update. The payee will then compute a corresponding update to the public expression of coin and post this public update on the public ledger. As soon as the update is posted, the payor cannot any longer claim ownership of the coin because he/she does not know the private update, only the payee does. No other than the payee has the private equivalent of the updated public expression of coin. This establishes the payee as the new recognized owner of coin Z -- payment executed - and settled. One will wonder: what then prevents any arbitrary trader to take the initiative and generate a private update to a coin, then post the corresponding public expression on the public ledger, claiming to be the new owner of coin? To prevent such theft the LeVeL protocol dictates that the update of the LeVeL coin must be an 'add on'. Namely, it must add to the previous expression of the coin -- not to replace it. This add-on limitation is what will prevent a stray trader to claim ownership of a coin. That stealing trader will not be in possession of the private expression of a coin before the update, and hence he will not be able to prove to any payee that he is the rightful owner of this coin. The only trader that is in possession of all the pre-payment private expressions of the coin, and the post-payment add on, is the payee, who received the private expression from the payor, then added his own to establish himself as the new owner of the coin. So, the payor cannot practice double-spending. The coin owner posts the public expression of a coin on the public ledger, asserting that he/she has the corresponding private expression. When the payee wishes to pass the coin to a third trader -- the new payee -- he will exercise the same procedure used by the original payor, only that now the private expression of the key will be longer (it has the recent update). The new payee will repeat the updating procedure, and further increase the 'signature' of the coin -- public and private. This way payment continues indefinitely. No intermediation from any financial institute is needed.

The LeVeL payment solution requires an undertaking agency, denoted as The Mint. The Mint mints the LeVeL coins, and passes each coin to the first trader. The Mint also redeems the LeVeL coins from their last trader. Both minting and redemption can be done against some consideration, which is a secondary point. The power of LeVeL rests with its utter simplicity: a community of traders served by a connecting network, comprising members where each member is equipped with a computing device that can exercise bilateral communication. The network facilitates a public ledger that lists all the circulating coins at their current public expression. Trade is carried out by the payor proving his or her ownership of the coin by revealing the corresponding private expression of the posted coin, and on it goes. Trade happens.

This embedded payment protocol is a first step towards a broader trend of embedded finance. Advanced commerce, debit and credit, investment, risk management, and other banking functions are all built upon this simple trading protocol. This is the LeVeL solution to payment in cyber space.

3. Sustained Off-Line Digital Payment Technology

Sustained offline digital payment technology is the last technological hurdle before digital money becomes the money people use. Offline payment refers to the ability of two parties to trade with digital currency when the network is off, which means that public ledger is not visible and no mobile phones. Offline transaction is often defined as a peer-to-peer validated transaction with finality of payment, operated in close proximity, excluding the need to involve a third party to either validate or settle the transaction.

In these situations, payment will take place via a trusted physical wallet (a HardWallet). There are two high level archetypes of hard wallets: One with offline clearing only capabilities, in which transaction is cleared instantly, but is settled only when payee resumes connectivity; Second with offline clearing and final settlement capabilities, so that payee can spend the funds received right away with no fear of receiving non-genuine coins. Most offline solutions in the market derive from the first form, which means that they require the transacting parties to connect to some third-party for finalizing the transactions, which is possible only when connectivity is back. It means also that payee cannot really validate that the locally stored digital coins at payer's device are genuine and making the payment final in the offline mode. Several such devices have already been deployed at a relatively small scale in closed-loop systems, albeit their deficiencies and not being able to provide the required security and counterfeit resistance, and definitely not being able to support a general-use fiat currency system at the scale of a national population. Worst-case risk is that adversaries would be able to distribute counterfeit digital currencies without payee and without the central bank finding out.

Only a very few solutions in the market belong to the second archetype, presenting a secured hardware device capable of storing different kinds of digital currencies, used for instantly settling peer-to-peer offline transactions between other hardware wallets, enabling finality of payment with no need for third-party approval or validation. In this section we analyze what we should expect from an appropriate HardWallet and search for the ultimate solution.

The functionality of offline payments would fulfill the needs of certain sections of society that lack digital facilities or possess inadequate digital competency, thus giving digital currencies and embedded payment solutions cash-like features for making it a legal tender and ensuring financial inclusion. The ability to transfer balances directly between devices that are offline, is crucial to making a digital currency that is viable population-scale alternative to cash.

Apparently, Central banks see it as an important challenge to solve. For example, the Bank of England, after evaluating existing so called offline solutions, including 'stored-value cards', cards attached to mobile phones, etc., announced in October 2022, that offline payment is still one of the most complicated elements of a potential UK CBDC and requires thoughtful consideration and design. It could increase acceptance and resilience of CBDC but heighten the risk of double spend as there is no online connectivity to verify the provenance of the money [10], [11]. A Forum Member presented a view on why offline functionality should be a key feature of CBDC. The presentation exposed why offline settlement finality was important in a world where physical cash usage is diminishing. The presentation also mentioned that, without offline finality, any CBDC system would be difficult to differentiate from any other real time payment system. The presenter mentioned also drawbacks of offline systems including the higher risk of counterfeiting and double spending due to added technical complexity. Bank of Japan also expressed concern that offline CBDC usage, without proper security protocols, could deteriorate CBDC security and make it more prone to counterfeiting (Bank of Japan, 2020).

3.1 Experimented solutions

We followed closely one of the trials of deploying 'secure elements' for offline payments (due to ethical reasons, the vendor and the user names will not be exposed). In the beginning of the process, they assumed that the main threat is cracking through the offline wallet to get to the code of the digital money which resides inside. Later on, they realized, that malicious actors do not need to crack the offline wallet, but to manufacture identical (but fake) offline wallets and store inside fake digital coins, that will be accepted even by payee's genuine offline wallets. Later on, it was realized that fake digital coins could have been circulated. However, eventually, such scheme will be exposed only when network connection is retrieved… and even then, it would be impossible to retrieve who initiated the counterfeit digital coins and spread them into the market.

Realizing those vulnerabilities and threats, and until the technology challenge is solved – it was suggested to enforce limits on transaction amounts and balances, in order to minimize the risk, and to execute periodic online synchronization with a trusted third party for verification of the coins inside the device and to identify suspicious transactions.
One should ask: are such measures and inefficiencies acceptable? - - Apparently not.

Eventually, it was realized that offline wallets, whether autonomous credit-card-sized battery-powered devices, or credit-cards size wallets being attached to or in proximity with a mobile phone (even a featured phone), that are based on tokenization and cryptographic signatures, cannot really secure payment transactions, cannot combat card information hacking and counterfeit and are vulnerable to malicious actors or to quantum computing attacks.

These vulnerabilities relate to most known secure elements/devices, stored-value cards, universal access devices etc., that are already being tested for offline clearing and final settlement capabilities.

Obviously, the challenge is not only making an affordable device (low cost), but there is a real unsolved technology barrier....

3.2. The technology challenges

Based on analyzing existing solutions, hereunder a partial list of hurdles, vulnerabilities and weaknesses that need to be solved:

First challenge: Tamper resistance devices exist with the shape of a smart card as secured environment, or wearable etc., but they seem to be vulnerable to:

(i) superior tampering, *and more important*:
(ii) counterfeit wallets.

The conclusion is that there is a need to develop a solution to enable a payee to have a simple and instant manner to validate that the payer's offline wallet is genuine, while the offline wallet's price is affordable for everyone.

Second challenge: to overcome weaknesses of published solutions:

(iii) cannot provide finality of settlements in the offline mode;
(iv) are limited in number and volume of transactions;
(v) the security device cannot split the coin to any desired resolution;
(vi) transactions are being dependent on signing the transaction with a special vendor key maintained by the offline wallet, hinged on cryptographic protocols based on the primitive cryptography (AES, or elliptic curve digital signature algorithms), which are vulnerable to faster computing attacks, and definitely to quantum computers;
(vii) in several solutions, only when either party has connectivity restored, the transaction generated by the secure wallet will be reconciled with the ledger using the usual rules, however, this should be unacceptable, as it puts the payee or the following payees or the issuer at risk.

3.3 The ultimate solution

Aiming at these challenges, the BitMint team developed a Hard Wallet [12], for low-cost mass production by 3D printers, that is constructed from quantum-randomness input, so that even the manufacturer and definitely any fraudster cannot duplicate or 'fake' it or intercept the digital coins. The solution is based on introducing pattern-devoid technique material identification: Using quantum randomness through nanotechnology to fabricate hardware devices to secure billions of numeric measurements characteristic of a unique material entity. The Input is true randomness,

captured in material composition, so no one and no computer can crack it. The output is digital quantum-resistant bits, easily measured, captured, stored, transferred.

The outcome is a counterfeiting immune (up to quantum-resistant) universal Hard Wallet, resistant to tampering, capable of storing different kinds of CBDCs (centrally minted coins, unifies value and identity), being used for instantly settling peer-to-peer offline transactions between two Hard wallets, enabling finality of payment with no need for any third-party approval or validation.

How does it work? – very simple: Touch and validate. Touch and pay. The private expression of the paid coin is transferred from payer's Hard Wallet to payee's Hard Wallet through physical contact between the two Hard Wallets. Once passed, the payor's Hard Wallet will erase the private expression of the passed coin (the payload), thereby leaving the payee's Hard Wallet as the only wallet that carries the private expression of the coin. Same will happen when the payee will transfer the coin to the next payee. Payment is finalized in the offline mode. At any instance there is only one trader that has possession of the private expression of the coin. The security that guarantees that the coins inside the Hard Wallet are genuine is not based on a cryptographic protocol, which other solutions hinged on, as it should be realized by now that all these cryptographic primitives are not immune against smarter mathematicians and definitely not against stronger computing machines.

In other words, each and every Hard Wallet, that successfully passed the very quick and straight forward validations process ("touch and validate") contains only genuine coins. This 'touch & authenticate' is enabled, since the Hard Wallet is 3D printed, feeding on quantum randomness, while each Hard Wallet is characterized by billions of physical embedded properties, a subset of them is kept in a public ledger, that is published by the Hard Wallet's manufacturer in advance. Users synchronize with a public ledger before the Internet shuts down and download it into their Hard Wallets. For population segments that are permanently excluded from Internet access, the ledger will be downloaded to their Hard Wallets in advance by the provider.

Values are stored locally in the Hard Wallet and transferred peer to-peer without ever having to be online. The Hard Wallet will readily split offline the amount of cash it holds, making smaller payments as needed. The HardWallet authentication and the payment are executed by a quick touch of payer's and payee's Hard Wallet, achieving payment finality. Very convenient for use also for elderly or nontechnology savvy users. Any tampering attempt will skew the results of the measurements and fail.

To conclude, the above-described solution scores highly across all following criteria, that should not be compromised:

- The first and of utmost importance, which is the main challenge to fulfil: defending against counterfeiting;
- Enable a fast, instant and simple validation process and payment transactions in one touch of payer's and payee's Hard Wallet, while transactions are final, with no need for later third-party approval or validation;
- Ease of use for elderly or non-technology savvy users;
- Prevent double spending;
- Enable payment continuity without mobile phones;
- Device can split each coin to any desired resolution;
- Resistant to tampering;
- Technically not limited in number and volume of transactions, with a long duration of operation without charging;
- Being quantum-safe with low-cost devices and with no functionality, usability and convenience tradeoffs;

The functionality of offline payments would fulfill the needs of certain sections of society that lack digital facilities or possess inadequate digital competency, thus giving privacy cash-like features to digital currencies, making it a legal tender and ensuring financial inclusion. The ability to transfer balances directly between devices that are offline, is crucial to making a digital currency that is viable population-scale alternative to cash.

4. The Mint

The Mint is where the cryptographic engine operates, and the digital coins are being generated. It includes a physical oracle for securing data off the digital grid, the Rock-of-Randomness, in which true randomness is captured in material composition, being the source for non-algorithmic digital quantum-resistant bits, for digital coin creation. It is designed to withstand the most aggressive hackers' attacks. Operation includes coin generation and coin voiding.

Each digital coin has a unique alpha-numeric id, like a serial number on banknotes, that is separated from the coin value. The power of BitMint's digital coins is in the inseparability of the value and the identity of the coin. Hence the id is as important as the value. Coins will retain unique id even after they split, while each split with have a new id, derived from the original. The coin id is fully randomized. Coin traded in a public ledger or even if on a DLT platform, only id is exposed, so there will be no information leakage as to the coin value, time minted, etc.

The Mint has full control on the initiation (purchasing) and on the termination (redemption) of each coin, while the in between traders execute a quantum-safe public-ledger based cryptographic protocol, as explained above, with no involvement of the Mint or any intermediator. The mint, when redeeming a coin will verify that the redeemer has knowledge of all the private keys and different random protocols corresponding to all the listed public keys. The mint will provide to the genuine redeemer the denominated amount of its coin, and will then destroy the coin and mark its image on the coin image database as voided (redeemed).

Currency solutions hinged on blockchain and alike are limited in throughput by the need to spread each transaction to a large number of peers. Legacy money solutions are limited by the singularity of the authentication entity. BitMint developed a well-defined methodology to enable an open number of mints to serve the public. All these mints will be connected via an InterMint [13], that is a network of mints constituted with a public protocol, so any entity can join. This will promote innovation and competition.

5. Conclusion

Governments, central banks, regulators and the private sector are rightly spending time thinking about the huge opportunities that digital representation of assets may bring and their possible adverse implication, and hence looking for how to design the ultimate digital currency to take advantage of these technologies in an appropriate most secure manner to fulfill citizens desire for a trustful reliable independent (with no intermediators) payment rail, that preserves their privacy.

Given the potential of digitizing real-world assets by tokenizing them, in particular, to streamline / automate payments as well many back-end processes, we have to consider whether crypto assets as they are structured and designed today can really provide the security, privacy, convenience of use and financial inclusivity, that are essential attributes.

The challenge for the current digital currency and the embedded financial revolution is to create a form of public money that is not dependent on a network of validators (peers' review) for making a payment, while replacing the old cash with Hi-Tech quantum money, with same privacy, respecting features of physical cash for the law-abiding users. This paper demonstrates how to

extract the underlying principles of the blockchain revolution and re-assemble them in a way that preserves its benefits and gets rid of its faults, while complying with what the International Monetary Fund (IMF) is saying that vulnerable algorithms will need to be transitioned to post-quantum cryptography. Quantum-resiliency through algorithmic mutation was presented, the same way a virus mutates against the vaccine, as opposed to relying on a single algorithm. The following characters were demonstrated: (i) payor-payee privacy with strong anti-money laundering weapon; (ii) payor-payee fast, frictionless, cross-border, instant settlement in online as well as offline modes; (iii) payor-payee resilience: no need for peers' approval; (iv) payment continuity when Internet is down; (v) 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; (vi) continuous payment per time or service is enabled, relevant also for automated M2M and Internet-of Things payments; (vii) terms of use ('Tethered-Money', programmability) can be written on the coins themselves, as well as their chain of custody (optional); (viii) serves unbanked and underbanked consumers, as well as non-technology-savvy users, all from top to bottom of pyramid; (ix) accommodating the potential for high transaction volumes; (x) it is not legacy bank accounts, which are not relevant for embedded payments, and it is not peer-dependent, nor a self-organizing network.

ACKNOWLEDGEMENT

The author would like to thank professor Gideon Samid, faculty of computer science at Case Western Reserve University, that laid the foundation of the revolution currently underway in post quantum cryptography as well as AI-based quantum money evolution. His increasingly achievements in natural sciences and mathematics and refined tools and most powerful methodologies confer expedite manner of introducing realistic innovative applications and practical use cases.

REFERENCES

[1] Osaba, E. et-al, Editors, (2021), Artificial Intelligence; Chapter written by professor Gideon Samid: "Artificial Intelligence Assisted Innovation", DOI: 10.5772/INTECHOPEN.96112 HTTPS://WWW.INTECHOPEN.COM/CHAPTERS/75159

[2] Samid, G. (2022) "The LeVeL-Paying-Field, a comprehensive cyber platform to deliver robust cryptographic security and game-changing digital money solutions", Paper 2022/130 https://eprint.iacr.org/2022/130

[3] Samid, G. (2015) "Tethered Money – managing digital currency transactions", Elsevier Academic Press https://www.amazon.com/gp/product/B012FR7I3W/ref=dbs_a_def_rwt_bibl_vppi_i1

[4] Samid, G. (2021) "Pattern Devoid Cryptography", Paper 2021/1510, https://eprint.iacr.org/2021/1510

[5] Zongyuan Zoe Liu (2022) "China Is Quietly Trying to Dethrone the Dollar", https://foreignpolicy.com/2022/09/21/china-yuan-us-dollar-sco-currency/

[6] The digital Euro Association, (2022), Based on which kind of technology should CBDC be built?, https://twitter.com/DigiEuro/status/1585521397731921921/photo/1

[7] The Digital Euro Association (DEA), (2022), "Ahead of the digital euro: Public Digital Euro Working Group Recommendations" https://lnkd.in/etq-EF3m , Section 2.5

[8] G20 TechSprint, (2022) The LeVeL-Paying-Field shortlisted by G20 TechSprint CBDC 2022 Competition, https://lnkd.in/ddKNsaWk

[9] DigFin, (2019) "Q-Pay could mark the next sea change in finance" https://www.digfingroup.com/bitmint-q-pay/

[10] Bank of England (2022), “Digital outcomes and special opportunities”, https://www.digitalmarketplace.service.gov.uk/digital-outcomes-and-specialists/opportunities/18203

[11] Bank of England (2022), “Minutes of meeting of CBDC forum, June 2022”, item three, https://www.bankofengland.co.uk/minutes/2022/june/minutes-of-cbdc-forum-june-2022

[12] Samid, G. (2020) IEEE conference, Hard Wallet: Digital Payment without Network Communication: No Internet, yet Sustained Payment Regimen between Randomness-Verifiable Hard Wallets https://ieeexplore.ieee.org/document/9216456

[13] David Lee Kuo Chuen, editor, (2015) "Handbook of Digital Currency", Elsevier Academic Press, chapter 20 https://www.elsevier.com/books/handbook-of-digital-currency/lee-kuo-chuen/978-0-12-802117-0

AUTHOR

Amnon Samid is an independent researcher and expert in cyber security and digital assets with academic credentials in engineering and business administration. Amnon enjoys vast practical experience worldwide, serves on the experts panel of the Digital Euro Association, led a retail digital Yuan project, and is leading an AI Powered Cyber Innovation Hub, BitMint, that has come up with powerful citizen-centric digital currency solutions, that aim to serve society, to enhance the prosperity of the community and empowering individuals around the globe. BitMint provides the platform of choice for driving quantum-safe digitalization for all financial rails, current and futures, across all verticals.

in: **https://www.linkedin.com/in/amnon-samid-3057418/**