

The e-Foundation*
for the 21st Century
Quantum-Resistant
Exchange of Value



BULLETIN

No 101

Central Bank Digital Money Foundation

Simplicity

Security

Endurance

Versatility

Resiliency

Efficiency

Swiftness

Scalability

Integrability

Interoperability

Financial Inclusion

For everyone, everywhere

Ref. CBDC 101.102020

Special Edition

**First brief
analysis of the
ECB Report
On
Digital Euro
ECB 2020
October 2020**

A new payment language is required to guarantee secure money transfer, preventing fraud and misuse, offering quantum-safe transmission, not dependent on network availability or possessing a bank account

Se requiere un nuevo lenguaje de pago para garantizar una transferencia segura de dinero, prevenir el fraude y el uso indebido, ofrecer una transmisión cuántica, no depender de la disponibilidad de la red o poseer una cuenta bancaria

Eine neue Zahlungssprache ist erforderlich, um eine sichere Geldüberweisung zu gewährleisten, Betrug und Missbrauch zu verhindern, eine quantensichere Übertragung anzubieten, sich nicht auf die Verfügbarkeit des Netzwerks oder die Besitzmöglichkeiten eines Bankkontos zu verlassen.

Un nouveau langage de paiement est nécessaire pour assurer un transfert d'argent sécurisé, prévenir la fraude et l'utilisation abusive, offrir un transfert en toute sécurité quantique, ne pas compter sur la disponibilité du réseau ou la propriété d'un compte bancaire.

的支付语言可以保证支付的安全性 防治金融欺诈及货币用于非法途径, 不能被量子技术破解, 支付不依赖账户体系 · 不依赖网络

*in establishment

Tags: CBDC, Quantum, fintech, digital currency, regulation, digital banking, fintech. credit, balance-sheet, lending, consumer-centric, randomness, cyber, privacy, AML, CFT, Identity

The e-Foundation*
for the 21st Century
Quantum-Resistant
Exchange of Value

CONTENTS

Abstract 3
A brief analysis 5
Concluding remarks 13

It's our pleasure to share with you our insights based on vast experience - more than 12 years - in all aspects of digitizing assets, money and currencies, from technology, through regulatory, monetary, security/privacy and most important social aspects, as well as executing successful pilot monitored by a central bank, and to support you along the process, if you find it useful.

ECB Central Bank Digital Money

Abstract

The ECB's published a report on a digital euro (ECB 2020*) is definitely an important declaration of an intention for enhancing the European zone citizens welfare with the most advanced attributes that a well-designed CBDC can offer, which are much more relevant in the post-corona era. We encourage the ECB and all European National Central Bank to take the lead and push for INTEROPERABILITY between all future national CBDCs, as well as towards building a more sustainable world as well as financial inclusion, "while no body is left out", while ensuring top Quantum-security, enabling payment continuity, high performance and user-centric tools.

We dedicate this month bulletin for an immediate brief preliminary attempt to enlighten the authors and readers of the ECB 2020 report, with insights from our interdisciplinary group that is deep into this challenge before bitcoin/blockchain popped-up, published books and articles and conducted a two-tier Quantum digital money project, that seem to be most advanced in most parameters compared to other known pilots worldwide.

This brief argues that most risks and hurdles and concerns describes in the ECB 2020 report have already been mitigated (scientifically and practically), as well as most perceived dichotomy between 'account base' and 'value base', 'retail' and 'wholesale', 'ledger-bases' and 'less-ledger-base', as a unified framework that provides all can and should be implemented; Such a unified framework makes irrelevant to decide in advance on trade-offs between privacy and security, zero-remunerated digital euro versus interest bearing (positive or negative) digital Euro, and other dichotomy aspects mentioned in the ECB report, as it's flexible and comprehensive enough to provide all options.

It's strange though, that the ECB is following the DLT trend, although it's common knowledge that DLT-based CBDC cannot provide the required quantum security, speed, and scalability to grow into a replacement of physical cash, being a legal tender and an enabler for fee-free, frictionless, instantaneous, unconditional money transfer with legal finality of value between any two parties; anytime, anywhere.

□ Risk of cyber-attacks is crucial: Would a distributed ledger technology not withstand an attack by smart mathematician and definitely by Quantum computers, then the entire digital Euro is compromised..... you cannot exchange quickly the entire framework that the digital Euro system will be built upon....

□ We strongly recommend the ECB to demonstrate in a pilot how a well-designed Quantum-resistant Digital Euro (centrally minted, not crypto-generated, but crypto-treated) with no concern of fraud or counterfeiting, will enable digital transformation of financial market and investment practices, mitigate financial and legality barriers, being inclusive and resilient against a broad range of threats, and reaching also non-technology savvy citizens, even with no smart phones or poor

**The e-Foundation*
for the 21st Century
Quantum-Resistant
Exchange of Value**

Internet network, reducing complexity in payments, improve end-to-end processing, simplifying record keeping, and making a positive impact, while improving the entire global economic position.

This is not a wishful thinking! Such a framework exists and was tested in China.

□ ECB's report argument that any CBDC solution must be environmentally friendly, rules out any mining and any known distributed ledger solution to become the essence of the digital Euro! As we demonstrated in China, the quantum-random identity-bearing CBDC, that is not crypto-based, minimize the ecological footprint and improve energy efficiency compared even with current payments' ecosystem.

Important to emphasize, that with such a framework any trade-off between security and convenience is not required.

While China identified the identity-bearing attribute of quantum-cyber money as its revolutionary aspect, the EU seem to be still in a 'research mode'..... we encourage the ECB to start experimenting a few concrete types of CBDC in parallel and not only following the mainstream trend of a CBDC solution that its essence is based on cryptography...like blockchain and other known distributed ledgers.

An identity-bearing quantum-cyber digital Euro is the call of the hour !

Our analysis suggests that ALL desirable features of a digital euro are doable.

□ The BitMint financial alphabet (AIFi) is being a-priori designed to withstand even the fiercest attack by quantum computers and as such it is a most fitting language for 21st century money, while the choice of architectures, infrastructures, access and interlinkages should be tailored to fit local circumstances.

□ Indeed, there are unique requirements in the Euro zone with its 19 different national central banks, that a single central bank country does not have to deal with, even if it is as large as China. The ECB and the national central banks will be able to integrate with each other through the *InterMint*¹ providing Interoperability.

We conclude the abstract with an optimistic wish: We hope that eventually at least the leading central banks – the ECB and the FED will not stay behind the PBOC, that adopts the vision of identity-bearing digital money, and will lead to a 'Davos agreement' (or 'Frankfurt Treaty') in the succession of Bretton Woods and Maastricht, and enable global, frictionless, versatile framework for exchange of value in any form cash, debit, credit, investment stocks, bonds, tethered or fungible, cyber spirited, materially moored – stable, sustainable: the blood flow in the body of the global society.

amnon@BitMint.com

[*] ECB report on a digital Euro, October 2020

https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf

¹ David Lee Kuo Chuen, editor, "Handbook of Digital Currency", Elsevier Academic Press, BitMint's *InterMint* - chapter 20 <https://www.elsevier.com/books/handbook-of-digital-currency/lee-kuo-chuen/978-0-12-802117-0>.

1. A brief analysis of a few statements

as per order they appear in the ECB report

@#Forward:

We find the first sentence of this report of utmost importance:

[QUOTE] "*A key part of the Eurosystem's mission is to provide citizens with riskless money for their payments*" –

- ➔ Well, for ensuring riskless money – the essence of the money cannot and should not be crypto-based (e.g. should not be based on algorithmic complexity).
- ➔ The private key encryption commonly adopted for cryptocurrency wallet solutions is prone to quantum attacks, hence the need for a quantum-resistant digital currency.
- ➔ Threatening trust in the currency to date, successful cyber-attacks have “only” compromised payment systems (albeit on a large scale in some instances such as the February 2016 breach of Bangladesh’s bank system and theft of 81 million dollars using the SWIFT messaging network), but never a currency itself. If the distributed ledger or any other technology that forms the basis of a digital currency were compromised, this would heavily undermine trust in the entire system.
- ➔ The basic question is: Would distributed ledger technology be safe enough to withstand even future attacks given that it could not be exchanged quickly once an entire money system had been built upon it is compromised?
- ➔ We strongly recommend the ECB to demonstrate in a pilot how a well-designed Quantum-resistant Digital Euro (centrally minted, not crypto-generated, but crypto-treated(*)) with no concern of fraud or counterfeiting, will enable digital transformation of financial market and investment practices, mitigate financial and legality barriers, including being inclusive and resilient against a broad range of threats, and reaching also non-technology savvy citizens, even with no smart phones or poor Internet network, reducing complexity in payments, improve end-to-end processing, simplifying record keeping, and making a positive impact, while improving the entire global economic position.
 - It is doable!

**The e-Foundation*
for the 21st Century
Quantum-Resistant
Exchange of Value**

(*) Generation (minting of coins) should not be dependent on DLT (Distributed Ledger Technology), although DLT could be used for distribution, while value (amount transferred) should not be exposed; but only the unique identity of the coin.

[QUOTE]: *"It is too early to commit to a specific design of a digital euro"* –

- ➔ Indeed, BUT if you make the wrong decision by preferring a digital Euro that its essence is based on cryptography – you put the entire Eurosystem at risk, once quantum computers are in the market. A digital Euro framework should offer sustainability and resilience for the long run,
- ➔ The ECB does not need to commit now for a specific design, but to adopt a framework that is based on an identity-bearing quantum-cyber digital money (like tested in China), and that is flexible to adopt any current or future design.

Note: this is not a theoretical recommendation, as such a framework was tested and passed tough banking stress tests and fulfils ALL principles and requirements identified in the ECB report, including although not limited to accessibility, quantum-robustness, efficiency, privacy, user convenience, and much more, while complying with relevant legislations, AML, CFT.

6

@ Executive Summary

[QUOTE] *"While the Eurosystem would always retain control over the issuance of a digital euro..."* –

- ➔ Just to emphasize that it's desirable that the Eurosystem always retain control both on issuance and redemption of the digital Euro, while distribution could be conducted P2P, no intermediators.

[QUOTE] *"As regards confidentiality... Some concerns have been raised that, by introducing their own digital currency, central banks could acquire sensitive information on users"*

- ➔ Not necessary. There are several solutions for preserving users' privacy, while still enabling validating the money or the wallet (even without network connection), as well as eliminating money laundering, fraud and misuse of money. However, a DLT-based digital currency cannot provide it. It requires a different approach based on identity-bearing digital money, as well as the option to write the chain of custody on the digital coin itself, as well as authenticating the payer's wallet (*Hard-Wallet*) by the payee, and more...we'll be more than

The e-Foundation*
for the 21st Century
Quantum-Resistant
Exchange of Value

happy to elaborate, and will preserve the ECB capacity to innovate, without compromising security aspects.

Btw, trade-off between security and convenience is needless with identity-bearing quantum-cyber digital money.

[QUOTE] *"the digital euro should be widely accessible on equal terms to prospective users in all euro area countries...."*

- ➔ Right. We have to make sure that non-savvy technology users, as well as those who don't possess smart mobile phones, but only featured phones (like the Chinese tested Q-PAY enables), and those that don't possess a mobile phone, and/or are not connected to Wi-Fi/Internet network - will be accessed to the digital Euro (the Hard-Wallet can solve this challenge).

@ Chapter 2:

[QUOTE] *"to support improvements in the overall costs and ecological footprint of the monetary and payment systems"*.

- ➔ For that to happen, it requires a centralized quantum-randomized identity bearing digital Euro (not crypto-generated), while enabling mobile phones (or any other battery-operated device) to execute the payment procedure, including splitting the coin to any denomination and transferring it P2P, not dependent on any network. Good results in that respect were demonstrated in China with the Q-pay project.

@ Scenario 2:

[QUOTE] *"to ensure privacy in payment transactions and the possibility to be used without any technical infrastructure.... required by many citizens (such as population groups who are less "tech-savvy" Ideally, a digital euro should allow citizens to continue to make their payments much as they do today with cash."*

- ➔ It requires (1) payment not being dependent on a ledger/network, and authentication not being dependent on cryptography, (2) not being dependent on smart phones, (3) enabling printing the digital coin and reading it back to the phone, (4) solving the main security challenge of digital currency of any kind which is that the payee must trust immediately that the paid digital Euro is bona fide, while the real challenge in that respect is when payer and payee are offline (no Internet connection).
 - *AlFi* and *Hard-Wallet* are designed to deal with these challenges.

@ Scenario 3:

[QUOTE] *"The digital euro should have features which are at the technological frontier"*.

- ➔ As of now, the Chinese (at least one* of its pilots) is in the frontier of the technological edge, much before any other known technology that is being piloted by a few other central banks.

*This Q-pay project demonstrates a well-designed Quantum-resistant CBDC (centrally minted, not crypto-generated, but crypto-treated) with no concern of fraud or counterfeiting, which will enable digital transformation of financial market and investment practices, mitigate financial and legality barriers, including being inclusive and resilient against a broad range of threats, and reaching also non-technology savvy citizens, even with no smart phones or poor Internet network, reducing complexity in payments, improving end-to-end processing, simplifying record keeping, and making a positive social impact.

8

@ Scenario 5:

[QUOTE] *"In order to improve the overall resilience of the payment system, the digital euro should be widely available and transacted via resilient channels that are separate from those of other payment services and can withstand extreme events."*

- ➔ The *Hard-Wallet* solution is designed to meet, among others, the challenge of elevating digital Euro to the high resilience status it was deprived of hitherto, to enable society not being paralyzed when the communication highway is shut down (even banknotes and coins that cannot always be delivered in areas of natural disasters).
- ➔ On top, *Tethered-Money*² solution enables a purpose-driven relief money, transferred directly to individuals' mobile phones, with specified usability restrictions, defining time and amounts of dedicated range of products, easy for use also for non-savvy technology or elderly people that don't possess smart

² Gideon Samid, *Tethered Money: Managing Digital Currency Transactions* (Elsevier Academic Press, https://www.amazon.com/gp/product/B012FR7I3W/ref=dbs_a_def_rwt_bibl_vppi_il).

The e-Foundation*
for the 21st Century
Quantum-Resistant
Exchange of Value

phones. ECB may enable Member States to grant financial support directly to consumers. If not addressed quickly and forcefully, the financial ramifications will spread to other sectors of our economy as tens of millions of consumers will focus on survival spending habits.

@ Scenario 7:

[QUOTE] "*Requirement 7a: cost saving...Requirement 7b: environmentally friendly*"

- ➔ The Q-Pay solution demonstrated in China a significant cost saving in production (minting) digital coins and in executing payments procedures, compared to current payments ecosystem, due to significant reduction in computing power requirement, hence less energy demand (for cooling the servers), while minimizing the ecological footprint.

@ Chapter 3:

[QUOTE] "*Requirement 8: ability to control the amount of digital euro in circulation*".

- ➔ As long as the digital Euro is issued and redeemed by the ECB (and/or a designated delegate, like a national central bank), and as long as it's an identity-bearing coin with meta data (*Tethered-Money*) that may fuze terms of use to the coin itself (as well as to any split of the coin), expiration date, purpose, positive or negative value, etc. – the ECB can have full control (optional) on the digital Euro in circulation. Moreover, it enables direct real time taxation of income or VAT etc.

9

[QUOTE] "*Requirement 12: easy accessibility throughout the euro area ... It should be easily accessible by anyone, including citizens who currently do not participate in the financial system ... and should be easy to use*".

- ➔ The *Q-Pay* demonstrated in China an accessible and most user-friendly solution also for non-technology-savvy users, being interoperable with third party payment solutions. The *Hard-Wallet* is intended for users that don't possess any mobile phone or don't have access to wi-fi/Internet.

[QUOTE] "*Requirement 13: conditional use by non-euro area residents*".

- ➔ The large sums of money that flow between global and national banks is a persistent attractive target for electronic thieves. Such transfers are validated by backtracking the history of the money which is the tedious effort of reconciliation. The BitMint money language (AlFi) is a means to alleviate both

**The e-Foundation*
for the 21st Century
Quantum-Resistant
Exchange of Value**

issues. All transactions should be centrally validated at the mint that issued the transacted digital coin. No backtracking.

- ➔ The Digital Euro coin may carry with it its full chain of custody, and thereby creating an accounting Tri-log: income books compared to expense records, and both compared to the chain of custody tallied in the coin. Mistakes are prevented, untoward money routing is exposed.
- ➔ Payment may be tethered to eventual terms of redemption. The Tethered-Money solution enables fusing specific terms of use/ conditions on the coin itself, to prevent (by desire) redeeming of the digital Euro outside the Euro zone (in other words, issuance and redeeming should be only by the ECB or designated delegates (like national central banks).
- ➔ Moreover: for cross border commerce activities you can use a Cascade Coin that is comprised of several Coins, to prevent volatility due to change of exchange rates, as described in reference 1 above. The Cascade coin can express multi party contract. All the legal details in the contract will be expressed in the coin. The coin will be redeemed only if all the necessary terms are met. No need for accounting follow-up.
- ➔ The above-mentioned solution enables instant cross border payment settlement around the clock, across different currencies.

[QUOTE] *"Requirement 14: cyber resilience. Digital euro services will need to be highly resilient to cyber threats and capable of providing a high level of protection to the financial ecosystem from cyberattacks. In the event of successful attacks, the recovery time should be short and the integrity of the data protected"*.

- ➔ Quantum-Resistance is essential for any future money and payment system, since the full range of modern cryptographic products, is subject to attack by quantum computers. While experts differ on timing, there is little dispute over the power of the new machines to defeat the ciphers that protect financial transactions today. The Chinese acknowledge this crucial threat and our quantum-safe system.
 - The only known doable Quantum-resistant digital money framework.
- ➔ As to the data base (the Mint) protection, BitMint developed Post Quantum Network Penetration Prevention solutions (effective also against insiders) and springboard for quick recovery, without compromising the Mint operation.

@ Transfer mechanism

[QUOTE] *"A bearer digital euro would fall outside the direct control of the Eurosystem or its supervised intermediaries"*

- ➔ Not necessary. Payee's APP may have an option of validating any coin in real time through the Mint (or a designated delegator, that will not be able to issue new coins, but only to validate coins issued by the ECB's Mint).
- ➔ Authentication of a payment is being resolved by either authenticating the transferred money, and/or authenticating the payer and/or authenticating the wallet (instead of trusting an algorithm, the payee has a mean to check the wallet if it is trustable, and then the payee knows that any money that goes out from the wallet is valid and not counterfeit).

[QUOTE] *"If a bearer CBDC were stored locally on the payment device, loss or damage to the device may result in the loss of CBDC"*

- ➔ Not necessary. If the digital Euro is an identity-bearing coin, users can store backup on another device, as long as a double spending prevention mechanism is deployed. And if users don't require anonymity toward the Mint (which is controlled by the ECB or a designated delegate, like a NCB), then the Mint will keep a copy of the coins.

11

@ Payment device

[QUOTE] *"User-friendly devices to be used in offline digital euro payments would need to be certified and their developers highly trusted (Requirement 11 and Principle 5), as is the case with cash production, during which secret features are embedded in banknotes by private companies. However, achieving a similar level of security in a digital environment with multiple sources of cyber risk is much more complex and this risk is not yet fully understood"*

- ➔ Not fully understood by who?
- ➔ A Payment device should NOT be dependent on private or public or governmental companies that embed "secret features" like with banknotes. This is much too risky!!
- ➔ A reliable payment device is required, e.g., Hard-Wallet, which is characterized as follows:

The e-Foundation*
for the 21st Century
Quantum-Resistant
Exchange of Value

- (i) The identity/identification of the HardWallet is not based on any digital form/sequence of bits/cryptography, that eventually is hackable, but rather on the material composition of the HardWallet;
- (ii) The HardWallet [HW] is based on quantum randomness generated material composition, the identity and integrity of which is readily verified by a simple handy verification device.
- (iii) The HardWallet is designed with a very large number of measured attributes, such that given these measurements it is infeasible to manufacture a HW that would give these measures.
- (iv) If the Hard Wallet is seriously deformed, or is broken, or splits, then the reading of measurements will be different, from the genuine measurements.
- (v) Payment issued from the HW can be taken in by a second hard wallet, which will further pay to another hard wallet, creating a payment ecology of digital money for long periods without the benefit of a communication network. This off-line payment mode is applicable to fiat currency, loyalty money, or private money.
- (vi) On top (optional): Payment may be tethered to eventual terms of redemption.
- (vii) The Hard Wallet may be personalized --fitted with ownership security capability. The Hard Wallet may be engineered in conjunction with a smart phone, so people can use a single device as a phone and as an off-line wallet.

12

@ Availability and usability offline:

[QUOTE] " a digital euro that is only usable offline would be unlikely to support new advanced functionalities such as conditional payments (Scenario 1). An offline digital euro would need to exist online at some point, in order to allow users to load money onto the offline digital euro wallet through the broader payment system; hence, any offline digital euro should also be linked to an online form of digital euro "

- ➔ Issuing two kinds of digital Euro – one for offline and one for online – is not just confusing, inconvenient and complicated, but it opens more opportunities for bad actors, and should not be adopted.
- ➔ A Hard Wallet as briefly described above, and was peer reviewed by expert evaluators and received Best paper award last month at IEEE 2020

**The e-Foundation*
for the 21st Century
Quantum-Resistant
Exchange of Value**

International conference, offers a much more convenient and a real secure solution, that does not suffer from above hurdles and vulnerabilities, enables loading money into one Hard Wallet from another Hard Wallet in an offline mode.

- ➔ Cards, like suggested in the report, are not secure enough (dependent on digital data/cryptography) and on top cannot accept payments. An off-line device (that could be on a nano-size, if needed) must be based on analog (and not digital data).

In other words – digital euro with material roots, which provides Quantum-grade security.

- ➔ The community-trust HW payment option leads to a gathering of mutually mistrustful parties, each holding a HW, allowing for any which way payment to support normal societal activity, and all that through periods that may be quite extended when for whatever reason the Internet is not readily available.

- ➔ This off-line payment mode is the missing ingredient on the road for worldwide adoption of digital money in the framework of national fiat currencies. However, it is also a necessary ingredient in the ecology of loyalty money or private currency issued on limited basis.

13

Concluding remarks

CBDC is not just an advancement of electronic payment...it's a total game changer (if well designed), and it's much beyond what a distributed ledger can offer. The incentive for deploying Digital Euro should not be just as a response to "The fear of a tech giants, like Facebook", but it's the ECB responsibility to take advantage of this imaginative evolution of money for the benefit and welfare of the Europe zone citizens. Most concerns raised in the report, were solved already, and most dichotomy mentioned are not necessary.

Everything you are doing with money - Instead of writing it as you do right now, which you can call it electronic money or digital (as all the money that you handle is represented as bits in a memory location) - - you can already now switch to the language that will give you Quantum Security, which you don't have to worry about the risk of someone hacking the money or worry about the fraud that is done today all over the place; - It will eliminate - just by changing the language. When you change language, you give yourself, not only a peace of mind, but it opens up fantastic new capabilities.

The e-Foundation*
for the 21st Century
Quantum-Resistant
Exchange of Value

These bulletins aim to contribute to international discussions on the realization of a digital money scheme, that will provide the required quantum security, speed, and scalability to grow into a replacement of physical cash, being a legal tender and an enabler for fee-free, frictionless, instantaneous, unconditional money transfer with legal finality of value between any two parties; anytime, anywhere.

These bulletins aimed to promote a data-driven financial sector for the benefit of consumers and firms and improve the security and efficiency, as well as reducing energy consumption/carbon print and to enable internationalization of the digital fiat currencies to strengthen the resilience of global money polices.

These bulletins aim to support decision makers in choosing the proper road maps, technologies and regulations and fulfil their responsibility to provide the next level of customer experience, that well-designed digital-fiat currency can provide, as well as their responsibility for enhancing the operational resilience of the financial sector and not making it easier for hackers to crack the payment system, by being dependent on algorithms that are hackable.

That said, it's important to pursue a well-designed Quantum-resistant CBDC (centrally minted, not crypto-generated, although crypto-treated) with no concern of fraud or counterfeiting, that will enable digital transformation of financial markets and investment practices, mitigate financial and legality barriers, including being inclusive and resilient against a broad range of threats, and reaching also non-technology savvy citizens, even with no smart phones or poor Internet network, reducing complexity in payments, improve end-to-end processing, simplifying record keeping, and making a positive impact, while improving the entire global economic position.

As regards the international level, there are multiple and persistent inefficiencies in cross-border payments that affect costs and payment times, to the extent that the G20 has made resolving them one of its priorities for 2020. CBDC framework should enhance the interoperability of payment solutions across different jurisdictions, and increase the transparency of fees.

Working papers based on research and experimentation with digital money are being published almost on a weekly basis by financial institutions, central banks, regulators, international associations and FinTech's, however most are not providing any comprehensive solution/concept/technology that fulfils all the above.

These bulletins offers the right stage for those that are not following the risky trend of designing a CBDC that its generation is based on algorithmic complexity DLTs, that cannot satisfy by a single protocol the required Quantum-security, speed and scalability to grow into a replacement of physical cash, being a legal tender and an enabler for fee-free, frictionless, instantaneous, unconditional money transfer with legal finality of value between any two parties; anytime, anywhere .

**The e-Foundation*
for the 21st Century
Quantum-Resistant
Exchange of Value**

The CBDC Foundation (under establishment) idea is to become the leading international non-profit, membership association that connects governments, central banks, public and private sectors around the world to understand and implement Quantum-safe CBDC, demonstrating the required quantum security, speed, and scalability to grow into a replacement of physical cash, being a legal tender and an enabler for fee-free, frictionless, instantaneous, unconditional money transfer with legal finality of value between any two parties; anytime, anywhere, including complying with AML, CFT, improving regulatory compliance and the effectiveness of monetary policy for the benefit of individuals and businesses. The Foundation empowers connection, communication, and collaboration for bringing positive impacts of a well-designed Quantum-CBDC around the world, helping them evaluate and validate models and provide central bankers with the relevant education and technology, social, financial, monetary advice.

15

The views expressed here are solely those of the authors

Disclaimer: This bulletin is for general and informative purposes, to assist decision makers. It's not a recommendation and/or opinion and/or an offer to invest in any technology or product or any other service. It does not constitute due diligence and shall not be relayed on as due diligence. The assumptions, opinions, conclusions, statements and predictions are relevant for the current situation while actual results and achievements may be materially different than could be understood from this document. The authors expressively disclaim any and all liability relating to or resulting from the use of the content of this document. Authors are not held responsible for omissions, errors, and lack of updates or imprecision of the information presented in this document.

© All rights reserved. Cites permissioned if source is stated,
unless stated otherwise.

The CBDC Foundation (to be established) is a personal initiative of Amnon Samid (the editor of the bulletin)
<https://www.linkedin.com/in/amnon-samid-3057418/>

CBDC@agsPOWER.COM