



Search keywords 

Search keywords 

[Subscribe](#)

[News](#)

[Interviews](#)

[Voice of the Industry](#)

[Watch & Learn](#)

[Reports](#)

[Cross Border Ecommerce Research](#)

[Company Database](#)

[Events](#)

Voice of the Industry

# Gaining trust for self-referential CBDC (practical solutions)

Tuesday 9 January 2024 10:38 CET | Editor: Mirela Ciobanu | Voice of the industry

*Amnon Samid, CEO of BitMint, an AI-Powered Cyber-Innovation Hub, tackles current cryptography-based digital currencies, that cannot serve as a means of better financial fairness and inclusion.*

Thus, they are risking national financial systems and overriding digitalisation over users' privacy, and may not ensure smooth deployment and operation, which will hamper their widespread adoption, whether they are CBDCs or stablecoins issued by the private sector.

Amnon highlights that a well-designed quantum-based digital currency, based on demonstrated protocols, that are being ignored by most central banks, can foster innovation, convenience, security, and privacy without compromise, enabling personalised experiences, as well as regaining bilateral private payment, that was robbed by all payment rails, except cash, while granting users control on their privacy, data, and money, without being an enabler for illicit activities.

*Happy New Year! We hope you had a relaxing festive time and didn't forget to read some of our CBDC series articles. The last in line in 2023 was from [David Birch on the digital sterling](#).*

*Today we continue with an insightful article from Amnon Samid, CEO of BitMint.*

## Key takeaways

- This article is an introduction to a proper description of the digital currencies evolution and demonstrates how almost everyone would enjoy digital currencies, if well designed, from citizens to businesses, merchants, retailers, institutions, communities, and States.
- We are facing a lot of misconceptions regarding digital currency, from misunderstanding the difference between digital payment and digital money to the wrong assumption that the creation of digital currency should be based on classic cryptography and that technology cannot guarantee cash-like privacy.
- The biggest challenge for us today is to let the world gain an understanding of the disruptive use cases that a well-designed digital currency can offer, not being lured by inferior solutions of influential technology vendors, that cannot fulfil peoples' wish-list and cause a negative sentiment and scepticism.

## A new financial language is required

A common misconception of many is that digital currencies exist already, while not realising the difference between digital payments and digital money. Central Bank Digital Currencies (CBDCs), stablecoins, and asset tokenisation are all expressions of a new financial alphabet. This financial language cures a fundamental deficiency experienced by money when most of it became computer-handled. Money then lost its identity, which was there when money was physical, and it shrunk to be a number only. The new [financial language](#) restores identity to digital coins and thereby puts them at par with physical coins as to the inherent advantages held by banknotes and metal coins while offering cyber-unique advantages for being subject to cryptographic processing. Banks, merchants, and private phones will all hold money in dedicated cash registers offering clarity, security, and accountability.

## Who is responsible for the sceptic sentiment toward CBDC?

**Financial Times** argues that [‘CBDCs still have not found their raison d’être’](#) and **The Economist** writes that CBDCs [‘create new problems while solving few’](#). In the **Wall Street Journal**, we read that [Surveillance Risks Shape How Central Banks Test Digital Currencies](#), arguing that the race to explore new payment systems highlights trade-offs between performance, privacy, and security. Apart from questioning the necessity and unresolved security issues and potential intrusions, the race to explore CBDC highlights fear of government control, identification, and access.

These misconceptions regarding the benefits that a properly designed digital currency can bring to individuals and society, stem from the preference of central banks, to examine only inferior concepts, promoted by major technical vendors, which are conceptually similar to currencies created by cryptography, and which are limited in functionality, in the ability to provide privacy, while introducing new threats to the national financial systems.

China is the only country that developed its inhouse capabilities to introduce a full-fledged CBDC, following five years of the [learning process](#) from major experts, including building and testing the first ever retail CBDC that passed banking stress tests, based on an [Israeli technology provider](#), before any other central bank starts a serious exploration process.

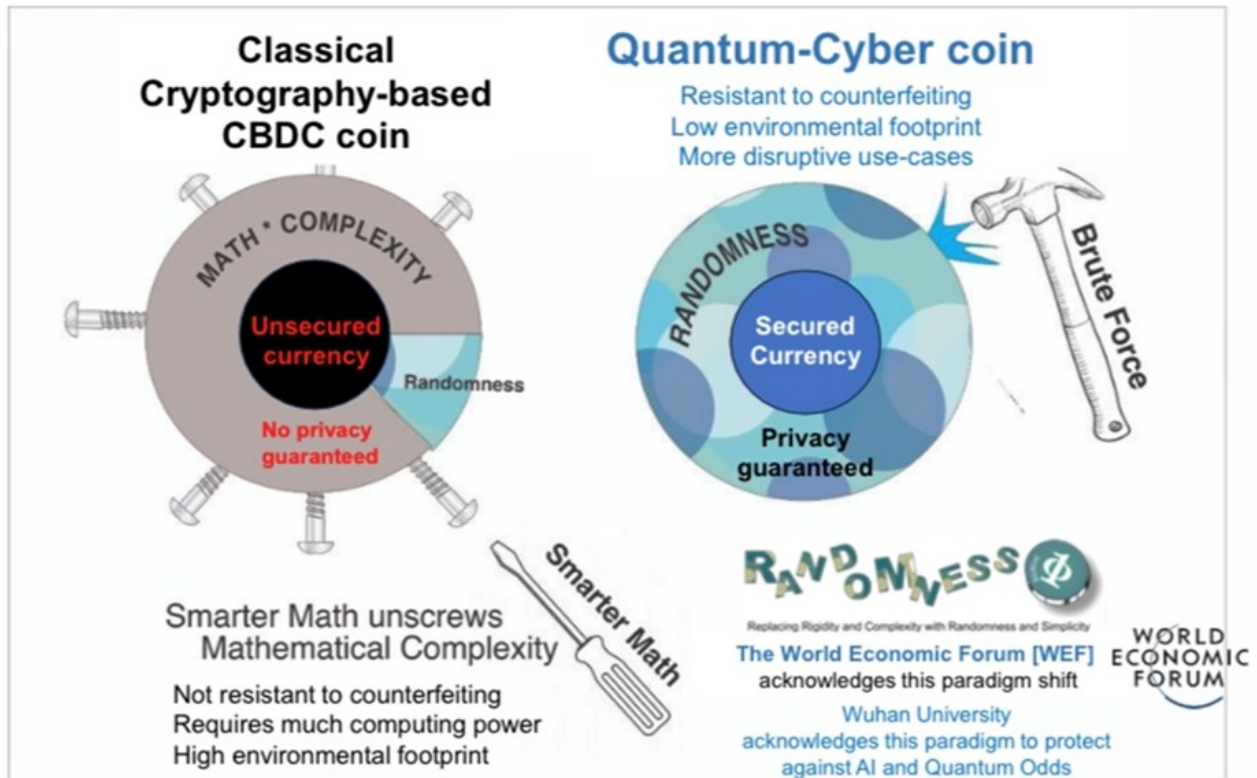
Most countries rely on major four or five CBDC solution providers as well as one huge consulting firm and various regional providers, that are playing a significant role in shaping the CBDC concepts, that does NOT provide real justification for developed countries to launch a CBDC and justifying the negative sentiment by citizens and independent experts.

Swift resolution of the wide adoption and trust challenge is crucial. To achieve critical adoption of CBDC, you must have a human-centric, fair, and ethical solution that is quantum-safe and enables cash-like privacy with compelling use cases and no trade-offs. However, most central banks explore CBDCs that are cryptography-based, that fall short of meeting all these requirements. Quantum-based solutions have the potential to overcome various adoption challenges.

---

The public should be aware that a well-designed digital currency, quantum-based, does NOT require trade-offs between performance, privacy, and security.

---



## The privacy concern: CBDC should create a bond between two strangers

Two strangers may pass a bundle of euros from hand to hand, and no one except them will know about it. If they use a payment card, they surrender the knowledge of the transaction to the card company and their respective banks. If they pay Bitcoins, the whole world knows about the transaction, and soon enough quantum computers will unveil the identities of the payor and the payee.

---

Neither card payment nor crypto payment today can replace the minted fiat coins and banknotes because they robbed people from the basic experience of bilateral payment.

---

Recently released insights from Bank of Canada public consultation suggest that [Canadians prioritise financial privacy](#), while a notable 87 percent of respondents said they don't trust the Bank of Canada to issue a secure digital Canadian dollar that is resistant to cyberattacks. This is one example of many, showcasing the importance of privacy and cybersecurity when it comes to CBDC.

To address people's fear of CBDC being used for surveillance and control or harassment purposes, privacy must be guaranteed by technology. Citizens will NOT trust the current solutions being explored by central banks that 'promise' not to have access to any data (traders' identities, transaction details, etc.).

Deploying zero-trust architecture for national currency is too risky. Trust can be shifted not removed. Zero Trust systems place trust in an abstract construct that is too sophisticated for most players to fathom. Hence when the trust place is infected and is being violated, the players have no clue. The solution for money is to place trust in a trust-bearer from which you can remove the trust at will. To do this one has to practice network dynamics in a configuration where trust-claimants compete and are motivated to stay trust-worthy lest they lose their users.

Digital currencies in general, and CBDC in particular, CAN and SHOULD enable private bilateral payments, which will be MORE convenient for users, compared to any other payment rail, without being an enabler for illegal activities.

## Addressing public concerns with practical doable solutions

Hereunder basic doable guidance for addressing public concerns includes:

**Coin creation:** CBDC coin should comprise non-algorithmic digital quantum-resistant bits, designed to withstand the most aggressive hackers' attacks, not being affected by quantum computers nor by AI-Cryptanalysis. A feasible solution [was demonstrated](#) and successfully tested in a real retail digital currency project.

**Online Transaction protocol:** If CBDCs rely on a fixed public/private key algorithm and fixed OWF (One Way Function) – it turns it into a resting target for advanced cryptanalysis. Online transaction protocols should be combined with algorithmic mutation to achieve [adjustable privacy and quantum resistance](#). [BitMint's LeVeL-Paying Field](#), that was shortlisted by G20 demonstrates how any digital tokenisation, CBDC, stablecoins, asset tokenisation enables adjustable privacy, with cash-like anonymity, both for payer and payee, which was never demonstrated before, with built-in Quantum-safe counterfeit protection, being more convenient for users than any other known solution, addressing very well also low-income households and young adults, as well as elderly and non-technology savvy users.

**Offline Trusted payment ecosystem:** The functionality of offline payments would fulfil the needs of certain sections of society that lack digital facilities or possess inadequate digital competency, giving privacy cash-like features to digital currencies, making them a legal tender, and ensuring financial inclusion.

Inadequate offline solutions are an aspect in which I agree with the opponents of CBDC because it turns out that there is still no working solution that adequately addresses the following fundamental insight: If you wish to have finality of payment in offline mode, with no risk of double spending and no risk of counterfeit coins – you should NOT trust ANY cryptographic technique! This vulnerability relates to most known secure elements/devices, stored-value cards, universal access devices, Tamper Resistant Element (TRE), such as smart cards, SIM cards, embedded secure elements, etc., that are already being tested for offline clearing and final settlement capabilities. It derives from realising that any cryptographic dialogue that convinces a payee offline may be emulated by a resourceful counterfeiter.

The good news is that the [ultimate solution](#) to enable a fast, instant, and simple validation process and payment transactions in one touch of payer's and payee's Hard Wallets, while transactions are final, with no need for later third-party approval or validation – is currently under extensive development. This HardWallet is designed with durability and maximum inclusion in mind, while paying prime attention to convenience and security, up to being quantum resistant, enabling quick and intuitive use.

## To conclude....

Many believe that central bank digital currency (CBDC) has the potential for surveillance, censorship, supervision, and detection and will only pretend to provide cash-like privacy. This article claims that [this concern is well addressed](#) by a digital currency that is created by a quantum-randomness source, which makes coin identity and coin value pattern-less, premised on unpredictability, while it is de-centralised verified and exchanged, utilising the LeVeL-Paying-Field that does not suffer from flaws of blockchain, being quantum-resilient, preserving cash-like privacy when two parties (human or devices) trade with digital money, whether Central Bank Digital Currencies (CBDC) or stablecoins. It's cutting out a network of validators and intermediaries, while still not being an enabler for illicit activities, and offering a much wider range of disruptive use cases and functionalities and accommodating the potential for high transaction volumes.

Central banks should not expect people to trust their CBDC if its design does not fulfil basic citizens' desires.

We better get it right!

### About Amnon Samid



[Amnon Samid](#) is a seasoned and forward-thinking professional with a diverse journey spanning roles from R&D and university lecturer, through co-founding and managing global technology companies in Israel, The Netherlands, Asia Pacific, and North America. He is a member of the expert panel of the Digital Euro Association. As CEO of an AI-Powered Cyber-Innovation Hub, BitMint, he was leading the first-ever retail digital currency project that successfully passed banking stress tests.

### About BitMint AI-Powered Cyber Innovation Hub



[BitMint](#) is delivering practical digitalisation and tokenisation solutions that help consumers, businesses, and communities to build wealth, without tradeoffs regarding ease of use, functionality, use cases, cyber security up to being quantum-safe, and users' privacy. BitMint is crafting comprehensive full Fledged payment solutions conducting a wide range of transactions, including CBDCs, Stablecoins, and Asset tokenisation, providing a secure and seamless experience – from issuing, through validation and transactions, tethering and smart contracts, all secure up to quantum-level, shaped by advanced Financial Language and of Pattern-Devoid Post Quantum Cryptography, the only one with a mathematical proof of efficacy.

### Free Headlines in your E-mail

Every day we send out a free e-mail with the most important headlines of the last 24 hours.

[Subscribe now](#)

Keywords: [CBDC](#), [payments](#), [cash](#), [digital currency](#), [quantum computing](#), [digital wallet](#), [central bank](#), [stablecoin](#), [tokenization](#)

Categories: [Banking & Fintech](#)

Companies:

Countries: [World](#)

This article is part of category

[Banking & Fintech](#)

[::: more](#)

## **The Paypers**

The Paypers is the Netherlands-based leading independent source of news and intelligence for professionals in the global payment community.

The Paypers provides a wide range of news and analysis products aimed at keeping the ecommerce, fintech, and payment professionals informed about latest developments in the industry.

## **This Site**

[About](#)  
[Subscribe](#)  
[Press Releases](#)  
[Advertise](#)  
[Industry events](#)  
[Tailor made Services](#)  
[Media](#)  
[Partnerships](#)  
[Contact](#)

## **Contact Information**

## Voice of the Industry

---

13:50 [Can I trust you?](#)

08:53 [The power of partnering: how public and private money drive together](#)

The Paypers 07:30 [Payment optimisation strategies for better acceptance rates](#)  
Prinsengracht 18 Jan [How embedded finance is stirring a revolution in financial services](#)  
777e 18 Jan [SaaS in payments: how banks and fintechs can enjoy convenience without sacrificing freedom](#)  
1017 JZ [::: more voices](#)  
Amsterdam  
The  
Netherlands

Telephone:  
+31 20 658  
0652

## Legal Information

© 2024 The  
Paypers BV.  
All rights  
reserved.  
No part of this  
site can be  
reproduced  
without  
explicit  
permission of  
The  
Paypers(V2.7).

[Privacy Policy](#)  
[Cookie](#)  
[Statement](#)

## Interviews


---

08:53 [Metrics of success: Evaluating Banking-as-a-Service and Embedded Finance](#)  
18 Jan [Today's trends in fighting fraud and top ecommerce risks confronting merchants](#)  
16 Jan [Unlocking the future of cross-border payments: tokenized deposits, stablecoins, and CBDCs](#)  
11 Jan [Navigating the Open Banking revolution in payments](#)  
10 Jan [Can the traditional financial market infrastructure be transformed in 2024? Partior says yes](#)  
[::: more interviews](#)

## Industry Events

24 Jan [Miami Web3 Week](#)  
25 Jan [Payments Regulation and Innovation Summit 2024](#)  
[::: More Industry Events](#)

OK  
For optimum  
operation, this  
website makes  
use of cookies.  
For more  
information  
click [here](#).

Free Headlines [::: subscribe now](#)  
 [::: follow ThePaypers via RSS](#) [::: connect](#)  
RSS  
LinkedIn [::: connect with ThePaypers on LinkedIn](#) [::: connect](#)  
Twitter [::: follow ThePaypers on Twitter](#) [::: follow](#)  
Facebook [::: like ThePaypers on Facebook](#) [::: like](#)