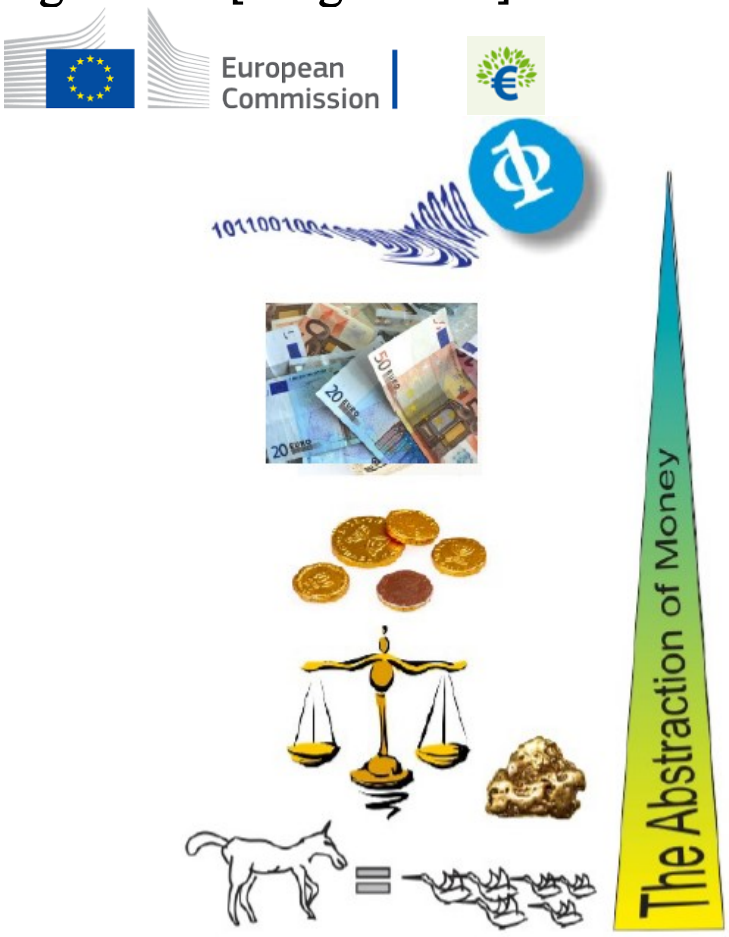
BitMint
AI-Powered
Cyber-Innovation
Hub

Commentary & Response on the

Proposal for a Regulation of the European Parliament and of the Council on the establishment of the digital euro ["Regulation"]



September 2023

Submitted by: Amnon Samid
amnon@BitMintMail.com

We advocate a centralized minted, Human-centric, trustworthy, non-discriminatory and ethical, fair, quantum-based digital euro, that will re-establish money as a truly public good; that serves interests of people and society, and that grant citizens control on their money, data and privacy (that was robbed by technology giants), without being an enabler for illicit activities.

Proposal for a Regulation of the European Parliament and of the Council on the establishment of the digital euro ["Regulation"]

BitMint AI-Powered Cyber-Innovation Hub Commentary & Response

1. Abstract

We applause the European Parliament and of the Council for getting into the regulatory challenge of introducing a digital euro and taking the opportunity to rethink the future of money and to re-evaluate security and financial stability issues of current payment rails. Introducing regulatory tools to preempt potential liquidity issues and preventing currency collapse, are indeed one of the crucial challenges you are facing regarding the introduction of digital euro. It's worth also considering shaping a regulatory framework to govern deposit tokens and stablecoins as 1:1 collateral guaranteed at the central bank. Harmonious coexistence of both public and private money forms will foster innovation, while the singleness of the ECB monetary system should stay intact. The BitMint AI-powered Cyber Innovation Hub [BitMint] is willing to contribute to these efforts, and now takes pleasure in responding to the proposed Regulation.

We are in agreement with the assertions a robust regulation and supervision is required for maintaining trust in the financial and monetary system. We note the desire of the authors of the proposed Regulation to balance between fulfilling citizens' expectations from the digital euro to support their welfare and desire for privacy and liberalizations, alongside

taking care of financial stability and monetary stability, and between preserving commercial banks' role in the financial system, as well as minimizing the possible exploitation of digital euro for money laundering and other illicit activities.

In order to foster broad adoption and public trust, apart from educating the public BEFORE issuing the digital euro, we recommend that the following principles will be guaranteed by the technology, not just by regulations, that could be changed in the future: digital euro will adhere to the principles of responsible and trustworthy public good currency, such as fairness, privacy, accountability and inclusivity. We strongly believe that cash-like privacy should not be bound to offline payments only, but be extended to online payments with close proximity under a certain threshold. Strong privacy should be a key differentiator of the digital euro. Privacy should be backed by technical assurance.

The digital euro platform could allow users to exchanging money bilaterally without intermediaries in the transaction process, and without validators, nodes and peer review, as well as to transact with digital euro settlement components.

The selection of technologies for the digital euro components is of major importance. A high focus needs to be on resiliency and scalability and on creating a quantum-safe digital euro, that is not being hinged on vulnerable cryptography, as well as building a solid foundation that will preserve privacy as well as keeping payment behavior unexposed, while offering powerful tools to prevent money laundering and other criminal activities.

Part of the advanced technologies are currently not being evaluated by the ECB, and should be included in the evaluation process.

Since so many challenges in the selection of technologies for the digital euro components (creation and validation/transaction) are of major importance, we strongly advocate for the EC to encourage the ECB to initiate designing and testing two MVPs (Minimal Viable Projects), that are based the two different architypes: One – quantum-generated digital euro coins, and a transaction protocol based on a centrally governed distributed public ledger, that is not based on nodes, peers and validators (the LeVeL), and is combined with algorithmic mutation to achieve controlled privacy and quantum-resistance; and Second - crypto-generated digital euro, and a permissioned-DLT, combined with zero-knowledge proofs to achieve strong privacy.

Both MVPs should be focused and with minimalistic set of functionalities and being tested in a closed eco system, for example to be used by employees of the ECB, with built-in learning and feedback cycles.

The advent of digital euro can advance the financial stability and payment rails security - if well designed; however, it may degrade it if its design is not taking advantage of the new face of money that digitalization brings (separate value and identity, which are inseparable), and not properly treating threats and risks.

1.1 Key general observations:

We would like to outline a few recommendations, that we think need to be considered, before making a final decision on the digital euro.

- In general, we would recommend a deeper look on how introducing digital euro may affect stability of the financial system and how replacing private money creation with public money will affect the monetary policy, on one hand, and how can it

contribute to more competition in the services of payments, on the other hand.

- We would recommend a deeper look into the possible technologies that underline the digital euro creation, as well as different settlement systems, that are essential for effectively processing low and high value digital euro transactions. The differentiation is not necessarily only between centralized and de-centralized architecture. For example, digital euro creation and minting, as well as redemption – could be centralized, while distribution and trading could be de-centralized – instantly transfer ownership and value via a public ledger (not necessary a blockchain and alike).

- Another differentiation that should be taken into consideration, is the two technology archetypes for digital currencies creation – **Quantum-based** versus **Crypto-based**, which may have a potential impact on resilience, sustainability, speed, financial inclusion, as well as usability and macroeconomic and microeconomics aspects, and as a consequence also on the proposed regulations.

- There is no excuse to pick a digital euro platform to be of reliable long-term service, which has no good answer to the ticking bomb of the **quantum threat** and to the new **AI-cryptanalytics threat**. We strongly recommend that the EC and the ECB will consider sophisticated technologies that are superior to crypto-based solutions, while cybersecurity up to quantum level, and users' privacy should be the primary concern. It is also imperative that

the digital euro meets strict data protection requirements and adheres to the principle that users retain their data sovereignty.

- It seems that the proposed Regulation didn't fully consider whether the digital euro platform should function as a currency, e.g., being token-based (sometimes called value-based), Or will it function as a settlement mechanism, e.g., being a pointer to the currency (sometimes called account-based).

- In compliance with the European Parliament latest publication PE 741.508 from April 2023, expressing doubts about distributed ledger technology (DLT), we recommend to evaluate other public ledger technologies, that are not DLT, like the LeVeL-Paying-Field, that is resilient to technical failure, counterfeiting and cyber risks, up to being quantum-resistant and it foster innovations in decentralized finance.

- It remains unclear how the offline will work. Offline capability is a key feature of digital euro, which means it should be possible to transfer a digital euro in any denomination instantly with finality of payment, with no risk to payee or to the euro financial system, when neither the payer nor the payee has access to the Internet. However, if you wish to have robust unlimited, sustained transactions in offline mode with digital euro, with instant finality of payment, you need a physical procedure (not a cryptographic dialogue), that will authenticate that the payer's wallet does not contain counterfeit coins, in order to prevent a potential currency collapse.

- The proposed Regulation focuses very strongly on account-based solution. It is not clear, however, how far the account-based approach could be designed with the potential use cases, like micropayments to be split by the users' phone without the network; continuous payments; machine to machine payments; conditional – purpose driven payments (without jeopardizing the legal tender nature of the digital euro); payment infrastructure for security tokenization use-cases, and even more innovative future use-cases in mind.

- We view value-based quantum digital euro as a more secure, more cost effective, offers more use-cases, functionality and flexibility, and it's more easily maintained solution than crypto-based solution.

- We would strongly advocate a validation/transaction protocol that is based on a public ledger, but not a distributed ledger technology, and not being dependent on peers or validators review.

- We share the EC view that the EC will monitor the **offline** digital euro scenario, and the ECB will monitor the **online**, and it is desirable to treat them as **two separate systems that will have no connection between them.**

- Furthermore, division of responsibilities between the European Commission [EC], the European Central Bank [ECB] and the users should be more precise, while much control over the data should be given to law-abiding users. These aspects are key for the digital euro to be widely adopted, as users expect the digital euro to

provide cash-like privacy, alongside speed and convenience of use at least like mobile payments offer. Privacy vis-à-vis government and payment providers, without being an enabler for illicit activities, should be guaranteed not only by regulation, but also by reliable technology. Otherwise, citizens in Europe may have limited faith in the digital euro.

1.2 To conclude this section

It's a common knowledge that Europe must shape, promote and massively accelerate digitization. Without the promotion and use of digital solutions, Europe may lose competitiveness and fall behind in the global technology race. The digital euro can make digitalization affordable to everyone, so no one in Europe will he left behind, and the continent will lead the way, not 'me too' and not being dependent on American technology giants.

With its implementation, both citizens and entrepreneurs will have equitable access to the benefits of a digitized economy, fostering innovation, economic growth, and financial empowerment for all. By introducing a well-designed and unique digital euro, Europe can lead the way in standard setting, effective regulation and sustainability for Central Bank Digital Currency.

Backed by 16 years of academic and practical experience in this challenge (including conducting a real world pilot of retail CBDC), the team of the BitMint AI-Powered Cyber-Innovation Hub is uniquely qualified to contribute to the narrative of the digital euro to become a potential differentiator and would welcome any opportunity, in any form, for further contribute and be engaged with the EC and the ECB in piloting, in

consultation or any other beneficial format, and maybe bring some fresh and different points of view to make the brain storming more fruitful.

2. ***Hereunder we set out brief comments on specific Articles:***

Chapter I

Article 2 – Definitions:

[31] Mobile device definition includes a device to enable also offline transactions. Connotation of mobile device is a device that is linked and can be connected to the Internet. However, eventually offline payments for preventing any risk of counterfeit digital euro to be stored in an offline device – should not be able to connect to the internet. We recommend adding a separate definition for offline device.

Chapter IV

Article 13 - Payment service providers (PSPs)

We assume that it's in the interest of the EC and the ECB to encourage PSPs to compete with each other with added value services based on the digital euro, in order to foster innovation. It's important to provide to the public accessible information what services by PSPs should not be charged. Another question: will the ECB control the costs for the non-free services?

Is it not clear why to limit visitors and former EU residents from using digital euro. It sounds conflicting with the free use of the euro as a single currency, as indicated paragraph 84, and with the legal tender status of the digital euro, as indicated in chapter III.

As to funding and defunding of digital euros (article 13.3) – it is not clear that no fees may apply, as we think should be.

The entire issue of putting limits on the digital euro should be debatable, but the procedure of automatic defunding of digital euro accounts that exceed the limit to a non-digital euro payment account, as described in article 13.4, sounds very complicated. Clarification is required what will happen when user does not have a linked non-digital euro account to top-up the transaction value or receives funds in the digital euro wallet that exceed the holding limit. Clarification is required regarding what might occur in such instances. Additionally, it is questionable why the digital euro should be linked to a digital euro payment account, and not being value based (what other define as token-based). Having the digital euro as value-based, and not adopting limitations, will eliminate also the problematic issue of the need to check all times that users' holding limit is not exceeded.

Chapter V

It's is not clear what are the instruments and parameters and procedures to maintain the limits to the use of the digital euro as a store of value in online use (article 16.1), and if it will imply also on transactions limit. As mentioned above, we strongly recommend to reconsider the concept of limits to the use of the digital euro as a store of value in online mode.

As to limits on offline payments – we agree that they should be applied, as long as there are no feasible solutions for offline payment, that can resist fraud and counterfeit. It makes sense that the commission will define transaction and holding limits for offline payments, since offline digital euros shall not be accessible to use online, for security reasons. This segregation should be clarified in article 16.4.

Chapter VI

We suggest to consider two aspects regarding using the digital euro outside the euro area:

- If the American currency goes off center stage, it will happen perhaps because of the huge debt it has built. And when that happens, the digital euro - if it presents clear advantages to the end users, the monetary system and the local and global financial systems, will have a chance to replace the hegemony of the dollar, on the way to the next money system. Alternatively, not one currency will replace the dollar, but a **cascade of currencies**. Following a period in which the mere trade with digitized fiat currencies becomes a norm, central banks will start cascading and minting a composite digital coin composed of a proportion of US dollar and euro. This cocktail currency will become the one quoted and specified in bilateral US-European contracts. From there, the idea of mixed fiat currencies will spread to the Yuan, the Yen, etc.

- For making cross-currency payments and cross border payments smoother and to facilitate the digital euro's international use, it is recommended that the digital euro platform should enable a token-based solution, sometimes called a value-based.

Chapter VII

Technology features: The Bank for International Settlements (BIS) recommends **to prepare in advance two alternative architectures** for

each financial infrastructure, that are deploying totally different technology solutions, so in the event of a cyber intrusion that has managed to compromise the core systems of the primary facility, the alternative solution, using a different technology, will immediately kick in. In that sense we strongly advocate for the EC to encourage the ECB adopting the BIS recommendation and to build the digital euro on the two major different technology archetypes for digital currencies: **The Quantum-based and the Crypto-based,** which may have a potential impact on resilience, sustainability, speed, financial inclusion, as well as usability and macroeconomic and microeconomics aspects.

Offline payments present unique risks that should be treated carefully. The future is digital representation of assets, currency included. As we move forward, it is imperative that we exploit these innovations with prudence and a vision for an inclusive and robust financial ecosystem, without adding new risks. Fully Offline solutions, while both the payer (sender) and payee (receiver) can remain fully offline and the value exchanged is instantly transferred to the payee, enabling them to use the funds immediately without requiring any online final settlement - are necessary for financial inclusion and in order for the digital euro to be always accessible as well as working as a backup option, if access to the internet is unreliable.

Eventually, Fully Offline functionality will offer a viable alternative processing route of transactions to occur with no network connection, potentially reducing the burden on the back-end payment infrastructure while providing additional benefits such as improved convenience, resilience, trust and on top of that being MORE secured compared to ALL current payment systems, including online transitions with digital euro.

In that sense, offline payments functionality should be developed as part of the core offering of the digital euro. And it should be Fully Offline solution, contradicting what is implied in Article 30-3, stating that final settlement of offline digital euro payment transactions shall occur at the moment when the records of the digital euro holdings concerned in the local storage devices of the payer and payee are updated. Definitely it does not enable consecutive continuous payment – a chain of payment that runs indefinitely, money can be split as desired – ongoing payment between touching wallets for as long as the Internet is off.

However, ALL known prevailing offline solutions (hardware-based or software-based), - (1) require trade-offs between crucial elements, and MORE important (2) rely on a cryptographic dialogue to convinces the payee, while any such cryptographic dialogue that convinces a payee offline may be emulated by a resourceful counterfeiter.

The risk of distribution of counterfeit digital euro, CANNOT be mitigated by using robust cryptographic protocols, no matter how “robust” are such protocols.

Obtaining the ultimate offline solution would require NEW thinking around offline, including a significant breakthrough in innovation with respect to performance and cost limitations, without trade-offs with respect to security, in general, and counterfeit in particular.

Some implementations use deferred communication between hardware wallets and the central bank register: transactions instantly settle even offline, but wallets keep a record of digital signatures to upload them to the register and have them validated at a later point. Such a protocol is

too risky and it does not provide continuity of payment, with no risk or double spending and counterfeit digital euro coins.

A Trusted Secure Element (TSE or HardWallet-HW) should be used for offline transactions, and it should NEVER EVER be connected online, to ensure that only genuine digital currency coins reside in the HardWallet. In that sense, article 23.2 suggesting that the digital euro will be convertible at par between online and offline, presents a huge risk of introducing **counterfeit digital euros into the offline wallets**.

The offline version should be closer to cash since it requires, instead of an internet connection, merely a bilateral connection between two devices (Hard Wallets). The settlement of a payment would occur between two Hard Wallets and they should provide sufficient security so that users can trust they will not be manipulated by other users and a payment received from another user's Hard Wallet is as good as receiving a banknote at your bank or withdrawing banknotes from an ATM.

Arguably using Bluetooth/uwb/nfc or some other wireless secure protocol is too vulnerable. A physical contact between payer's HardWallet and payee's HardWallet is required, for authenticating and for paying.

If you wish to have finality of payment, with no risk of double spending and **no risk of counterfeit in offline mode, you need a physical procedure (not cryptographic!),** that will authenticate the physical wallet (TSE, HW). it requires sender and receiver to authenticate their hard wallets by physical touch (touch & authenticate/ touch & pay).

Specific design types to fulfil all crucial parameters of an ultimate fully Offline solution are still being explored, in the prototyping laboratory stage.

Until such ultimate solutions are feasible – it's strongly recommended to avoid offline scenario of digital euro, although to prepare the core infrastructure and the regulatory framework in advance.

Chapter VIII

Privacy: The main challenge for the digital euro to be trusted is to fulfill the vision of restoring the old way of private bilateral payment with cash and to fit it for the digital age. The digital euro to be accepted by citizens, needs to offer instant payment from payer to payee (whether a person or a device), up to a threshold, with no-intermediaries, in online and in offline modes, and being anonymous – cash-like, guaranteed by the technology, not only by regulation, yet not enabling even the smartest adversary or the most powerful computer, up to quantum computers, to jeopardize the money. All that without being an enabler for illicit activities, and without violating traders' privacy.

Conclusion

It is of vital importance that a digital euro is built on a legal foundation that protects a centralized minted, Human-centric, trustworthy, non-discriminatory and ethical, fair, quantum-based digital euro, that will re-establish money as a truly public good, that serves interests of people and society, and that grant citizens control on their money, data and privacy (that was robbed by technology giants), without being an enabler for illicit activities.

To that end, we would like to outline the following important recommendations:

We recommend the European Commission not being agnostic to technology, and to take a deeper technology approach. The ECB focuses very strongly on crypto-based solutions, while it's essential to evaluate also the other technology architype. We argue that an emerging alternative to crypto-based currencies that is based on a different technology architype, deploying quantum randomness instead of mathematical complexity, is more suitable for obtaining bilateral payment protocol for the digital euro, which is homomorphic with cash payment and gives users control over their privacy, data and money, while not being a shelter for illicit activities.

In that sense, we strongly advocate for the EC to encourage the ECB to evaluate in parallel the two technology architypes and then initiate designing and testing two MVPs (Minimal Viable Projects), for each of the different technologies: **One** – quantum-generated digital euro coins, and a transaction protocol based on a centrally governed distributed public ledger, that is not based on nodes, peers and validators (the LeVeL), and is combined with algorithmic mutation to achieve controlled privacy and quantum-resistance; and **Second** - crypto-generated digital euro, and a permissioned-DLT, combined with zero-knowledge proofs to achieve strong privacy.

To foster trust, inclusivity, scalability and broad acceptance of retail digital euro, it’s recommended to combine a conventional data base for centralized minting and redeeming of pattern-devoid digital euro, while transactions being executed peer-to-peer via a public ledger, with no intermediaries and NOT being dependent on validators, nodes or peers review, eliminating complex consensus mechanisms.

Thus, enhancing all critical elements of a reliable payment system, including decentralization, security, useability and scalability, WITHOUT anyone to come at the expense of weakening another, taking advantage on both centralized and de-centralized protocols' added values, without their faults and deficiencies, being highly scalable by design without facing from a 'single point of failure', and on top of that being resistant against future quantum computing capabilities and against foreseeable threat of AI-cryptanalysis.

The above is doable!

We share a lot of the European Parliament views and welcome the fundamental importance in the regulatory proposal on public access to public money, and the strong focus on maintaining trust within the euro zone a well as on privacy preservation and data protection. We also appreciate the realization of the European Parliament that there is room for improvements.

We, the interdisciplinary team of BitMint AI-Powered Cyber-Innovation Hub, are competent and are willing to contribute to this challenge of developing a digital euro that is more future-proof and ultimately enable the EU to maintain a position of global leadership and to lead the way in standard setting.

BitMint
AI-Powered
Cyber-Innovation
Hub

Humoney designed for the benefit of people and society