

Highlights

Governing opportunities and risks of digital currencies

Highlights from
a workshop
held on 25–26
October 2022

Summary

1. It is unclear which socio-economic challenges can be addressed by digital currencies and assets
2. The monetary system is founded on trust in the currency
3. There is some added value in privately-issued cryptocurrencies and assets, and decentralised finance (DeFi)
4. Web3 has unclear implications for cryptocurrencies and assets
5. Regulation of private currencies will be critical to ensure net benefits to society
6. Central banks can and should benefit from technological innovation
7. International collaboration is critical to the success of central banks' digital currencies
8. Collaboration and complementarity of public and private sector initiatives
9. Call for position statements by distinct stakeholders
10. Cryptocurrencies can benefit illicit economies, fraud and malicious actors, which calls for tight regulation

On 25-26 October 2022, IRGC convened a multi-stakeholder expert workshop¹ to discuss the future and risk governance of digital currencies and assets. The workshop discussed in particular:

- Current trends that indicate specific needs, demands and challenges.
- Technology features and technical designs, focusing on those that central banks could adopt for Central Bank Digital Currencies (CBDCs).
- Implications of deploying or adopting various types of digital currencies (DC) for distinct actors and related motivations or preferences.
- Specific issues related to the role and responsibilities of distinct actors in the digital currency landscape.
- Three possible scenarios for the future, on the 2035 horizon.

In **scenario A**, central banks have, by that time, taken the lead and managed to organise a coordinated response to the various demands or needs. As a result, CBDCs have become the norm and payment systems' efficiency, integrity and privacy have dramatically improved.

In **scenario B**, the lead has been taken by private sector actors, such as digital platforms, that have created their own digital currencies and control most payment systems worldwide with a patchwork of attractive and competing private digital currencies.

Finally, **scenario C** describes a world where permissionless blockchain-based cryptocurrencies (CCs) are fully established and efficient. As a result, public institutions have lost control of a considerable part of the economy. Opinions at the workshop indicated that scenarios A and B seem more plausible or appropriate for the corporate world, but scenario C could also play a crucial role in the retail space and could be supported by some social innovators.

Since the workshop in late October, FTX, the second-largest cryptocurrency exchange, has gone bankrupt. It is premature to anticipate the full extent of consequences, whether it signals the end of any trust in the crypto assets domain, or whether it will be reminded as one more collapse of a fraudulent financial company, with some similarities to previous Madoff-like financial mania. Anyway, large-scale fraud and robbery that leaves "one million furious

creditors, dozens of shaky crypto firms and a proliferation of regulatory and criminal probes"² is a very serious matter. It will have cascading systemic impacts. At least it must trigger stricter regulation, which the field of crypto assets generally tends to resist, independence between financial operators, lawmakers and regulators, better investors' education and ethics, and more information to those tempted to use CCs.

In this workshop summary, we highlight ten points featured prominently during the discussions in October 2022.

Over the past ten years, a wave of thousands of privately-issued digital currencies has emerged from the deep ocean of digital technologies, including blockchain, internet and telecommunication. It is debatable whether this wave will lead to a fundamental and socially beneficial redesign of the monetary and payment systems, which increasingly appear technologically outdated and full of inefficiencies. Although these digital currencies contain seeds of benefits, they may also contribute to destabilising monetary and financial policies, with cascading effects in economic and social policies that could significantly undermine well-being and trust.

1. It is unclear which socio-economic challenges can be addressed by digital currencies and assets

What key deficiencies of the current system (where objectives are not met) could be addressed by digital currencies? There is a range of socio-economic challenges that digital currencies and crypto assets might address. However, the extent to which this can be achieved successfully is still unclear. For example:

- Financial inclusion, i.e., the ability to open a bank account and access cheap and reliable credit, is often mentioned as a desirable goal, primarily in developing countries. However, it is not evident that cryptocurrencies or CBDCs will be able or necessary to achieve financial inclusion. They may not be able because supporting pre-conditions such as digital connectivity and infrastructure, financial and digital literacy or economic status

¹ The workshop was organised in collaboration with Horizon Group and the Swiss Re Institute, and hosted at the Centre for Global Dialogue.

² www.economist.com/leaders/2022/11/17/is-this-the-end-of-crypto

are lacking in countries where financial inclusion is most needed. They may not be necessary because there may be ways to improve financial inclusion other than through cryptocurrencies or CBDCs. The priority is to improve literacy and connectivity, notably in rural areas in developing countries and among poor communities. Efforts to improve inclusion through cryptocurrencies without the pre-conditions in place may end up detrimental to individuals.

- Providing a viable alternative to cash money, which is increasingly less used, is also mentioned as an objective for central banks. However, matters of confidentiality, privacy and security complicate the implementation of CBDCs. Also, it must be possible to spend CBDC offline, and someone must agree to cover the risk of double spending, which cannot be technically eliminated.
- Improving the efficiency of cross-border and domestic payments is also mentioned as a need that can be met with digital money. However, digital currencies may not be necessary for that. Increased speed (e.g. intraday trading), reduced cost of transactions, and reduced counterparty risk are relevant and achievable technical and business objectives, but cryptocurrencies may not be needed there.
- Tokenisation of assets could increase liquidity in asset management, but also bring risks of security, scalability, privacy and accessibility.

Eventually, the main challenge for digital currencies is creating value for users.

2. The monetary system is founded on trust in the currency

There is a large variety of types of public- and privately-issued digital currencies, with different objectives. However, trust in the currency and financial system is central to the efficient functioning and stability of any economy, which implies that it is the responsibility of governments and central banks to safeguard public trust in money, maintain price stability and ensure safe and resilient payment systems and infrastructures.

- There is a significant difference between national currencies, which are issued and guaranteed by central banks and are instruments of monetary and financial policies, and (i) money, which can be used in various forms for financial transactions only, and (ii) crypto assets.
- Under certain conditions, it is absolutely fine that individuals can use privately-issued money

(local and community currencies have existed for centuries) and invest in crypto assets. However, in the digital world, users of cryptocurrencies must be informed about and protected against the risks, and aware that perceived benefits - such as encouragement of local economy or specific purpose, or convenience - may be traded against the private interests of those that create, promote or force to use those currencies. In any case, currencies must be designed in a way that they align supply and demand (needs) in view of achieving a specific objective.

3. There is some added value in privately-issued cryptocurrencies and assets, and decentralised finance (DeFi)

Overall, participants in the workshop did not view bitcoin or the majority of private CCs as a plausible future of money. Too many private CCs lack transparency and ethical purpose to add value to society. So, we need to be clear about the added value of specific privately-issued cryptocurrencies and assets and what risks are involved. Three examples:

- A major source of opportunities comes from blockchain systems in general, which introduce innovative features. For example, smart contracts enable so-called “programmable money”, i.e. the automatic execution of contractual clauses. However, much will depend on the type of blockchain system (permissionless and open, or permissioned and controlled) and validation mechanisms.
- Besides its function as an asset, the added value of a private CC for transactions will be established (i) in comparison with CBDCs, most of which are still in research or experimentation stages and (ii) the need of the economy. Therefore, private CCs should be seen as private money more than currencies, which is the privilege of central banks.
- Private actors in retail businesses may benefit from developing their own CC for marketing purposes and loyalty schemes that reward and lock in their customers.

The same is true for decentralised finance (DeFi). DeFi has not yet made the case that it benefits society. However, DeFi plays a helpful role in challenging inefficiencies. It presents potential sources of innovation for improving current financial and payment systems and is in itself very

evolutionary, currently changing to hybrid modes ('HyFi').

4. Web3 has unclear implications for cryptocurrencies and assets

Implications of possible development of Web3 for cryptocurrencies are tightly linked to the supporting rules that govern specific CCs and, in particular, the type of consensus mechanisms to validate transactions. There will inevitably be trends to re-centralising systems initially created as fully decentralised or creating powerful controlling nodes in seemingly perfectly distributed systems (as could be with PoS Ethereum). Web3 is, in theory, a fully decentralised system, but it is facing the risks of going towards re-centralisation around private nodes that could prioritise their private interests, continue to exercise control and monetise data as currently done by GAFA companies. The nodes could also impose their rules regarding security and privacy. Public oversight and control would be necessary to combat illicit and malicious actors. The dream of a fully decentralised blockchain-based internet system does not appear realistic.

5. Regulation of private currencies will be critical to ensure net benefits to society

Regulation of privately-issued currencies and assets will be critical to ensure that their potential benefits are reaped and to create or restore trust in cryptocurrencies (after significant collapses in 2022, including Terra Luna and FTX), as well as in institutions and financial intermediaries.

- Significant risks must be controlled, and those exposed and vulnerable to the risks should be better protected through various means, technical, regulatory, educational and others. The principle 'same activity, same risk, same rule' seems appropriate to start. The very fact that a vast majority of actors express the need for revision or adaptation of existing regulations reveals that private digital currencies are a reality, which shapes the currency and payment landscape and influences its future developments.
- Above all, regulations are necessary for ensuring security, integrity and privacy, which they can help achieve through adequate technology design that implements policy requirements without compromising on performance. In particular, obstacles to investing in crypto assets could be

reduced with appropriate regulation. From an insurance view, some degree of reliable regulation, clarity and standardization is important (cf #9).

- Regulation must include and complement actions to inform every CC user about the risk, to ensure informed decisions.

6. Central banks can and should benefit from technological innovation

Technical solutions developed in research and start-up blockchain and DeFi companies could offer opportunities for innovation in central banks at different levels:

- Wholesale CBDCs could rely on permissioned blockchain systems to enable smart contract programmability (transactions can be executed automatically when set conditions are met) and new functions (expanding the types of transactions between a broader range of financial intermediaries). Central banks might find promising efficiency gains and opportunities there.
- Retail CBDCs probably do not need blockchain systems for various reasons, including scalability concerns.
- Some countries with a high level of financial inclusion and efficient systems for financial transactions may just need to improve the payment systems that complement cash.
- Matters of security and privacy are essential for central banks in particular. There exist techniques and specific designs for reconciling those seemingly opposing objectives and their nuances, for example, differentiating privacy for end users and transparency for recipients, or setting different privacy requirements depending on transaction amount, application or circumstances.

Indeed there is a continuous set of options for central banks, from full-fledged retail CBDCs that would serve all three functions of money, to mobile payment systems for customers, possibly international. However, a CBDC should not be just a payment system. Instead, it should be understood as a new format of money enabling an alternative payment rail that maintains properties of a digital bearer instrument with greater programmability and possibly offline functioning. Moreover, seigniorage should accrue to central banks.

While remaining prudent, central banks would be advised to press on and intensify their research and experimentation of CBDCs in various forms,

to capitalise on the wave of innovations for digital currencies before large, established and robust private actors eventually launch their own competing private money (see #8).

7. International collaboration is critical to the success of central banks' digital currencies

However, countries must not establish their own CBDC before they fully understand and can control the effects on their international monetary and financial policy and second-order effects on the economy. For example, a country with an already strong currency should consider the risk that establishing its own CBDC would make it more easily accessible, which could further strengthen the currency. This could adversely affect the country's exports, economy, and jobs. Indeed, key drivers of central banks' projects are not only about responding to and taking advantage of technological advances. Decisions about CBDCs are primarily driven by politics, strategy or the need to strengthen the country's geo-economic situation. The latter remains a significant driving force behind CBDC projects.

International collaboration must intensify to share objectives for the cross-border interoperability of wholesale and retail CBDCs (in addition to domestic interoperability). The success of a CBDC will largely depend on how it contributes to increased efficiency in international transactions, using advanced technology designs. Collaboration must also serve to enhance the stability and integrity of the evolving monetary, financial and payment systems worldwide. While each central bank must remain sovereign and independent in its choices, and design choices must align with specific national policy choices and regional values, it seems sensible that technical and regulatory designs must also be chosen in collaboration with other countries.

The absence of international consensus on core issues such as data governance and privacy, and global governance arrangements on value creation in new digital currencies and assets, should be addressed at the political level.

8. Collaboration and complementarity of public and private sector initiatives

Public-private collaboration, including with new innovative actors, will enable central banks and traditional finance to evolve the current system without dramatic shifts such as those that would come if DeFi gained a dominant position without solid regulation. Various aspects here:

- Governments are enablers of the monetary system as an instrument of public policy to work in the public interest.
- Central banks have a narrow mandate, with a duty to act in the interests of their country as a whole. As such, they are key actors, and their collaboration with other policy bodies will be more needed than ever.
- As intermediaries, commercial banks have a role to play and a unique opportunity to shape the design and implementation of CBDCs. Their role in distributing cash, processing payments electronically, and providing safe holding of deposits and capital lending should remain. There is increasing collaboration between traditional banks and DeFi companies (to share infrastructure) or technology platforms.
- Large companies from the private sector, such as platform or retail companies, have the skills, resources and power to compete with central banks on aspects of efficiency, cost and user convenience.
- The best way for central banks to address competition from the private sector is to collaborate with it, for example, in reviewing the respective roles of central banks and intermediaries in the two-tier banking system. Partnership will be instrumental in designing future currency, monetary and financial policies.

9. Call for position statements by distinct stakeholders

Prominent economic actors would be advised to provide formal statements of their positions, intentions and objectives regarding specific digital currencies and assets. This would help clarify the evolving field of digital currencies, payments and assets, which otherwise leaves too much room for differing or divergent views and perspectives. The underlying motivations of distinct actors vary and are often unclear or ambiguous, especially if around privatising benefits. While short-term and specific goals are generally expressed clearly in marketing

terms (to motivate distinct actors to adopt and promote a particular privately-issued currency or asset or to use certain exchange services), longer-term and broader implications for other stakeholders and society in general are often kept purposely opaque. For example:

- Governments could recognise the sheer size of this global issue that requires global governance arrangements, and that landscape and actors are evolving quickly.
- Central banks could be vocal about their responsibility to the country not to compromise on the triple challenge of ensuring security, privacy and integrity, while improving performance and meeting people's needs. They need to remind their accountability to people, which KYC and AML regulations³ can help ensure. Going further, they can communicate that CBDCs are not an end in itself, but an enabling mechanism to support broader policy objectives.
- Commercial banks could take a clear position that, for example, they intend to accompany and work with central banks, and not compete with them for the future of money.
- Private actors outside the financial sector could call for regulation to reduce uncertainty and establish the legal basis they need to operate.
- Traditional insurance companies could communicate that they cannot provide coverage for NFTs loss because of instability and volatility, deficiencies in attribution and risk transferability, and sometimes even the credibility of actors.
- Investors could work to establish the benefits of investing in crypto assets while explaining why the risks are currently too high, and what would be needed to reduce the risk. Regulation can act as both a barrier to and an enabler of market entry.
- Citizens could elicit their position regarding how (and when) security, privacy and performance matter to them, thus providing important insights to policymakers.

10. Cryptocurrencies can benefit illicit economies, fraud and malicious actors, which calls for tight regulation

Relationships between cryptocurrencies and illicit actors are multi-faceted.

- What is clear is that some CC schemes can be scams and cause financial losses to digital or finance illiterates. Fraud that targets unsophisticated customers must be published, combatted and punished harder than now.
- Regarding how the illicit economy uses or is financed by CC markets, pathways to damage and measuring the extent of the problems are complex. In many cases, traditional financial institutions are also used in the transaction chain, in addition to new actors in the DeFi sector. Because money laundering is characterised by the fact that transactions look legitimate, it is possible that the full extent of the problem is not captured well. Further data and research is needed to assess how cryptocurrencies contribute to the illicit economy. In any case, regulation is necessary to pursue public policy objectives and benefit legitimate participants while being pragmatic and enforceable.
- On the one hand, public ledgers on the blockchain offer much insight into illegal behaviour and opportunities to trace currency flow. But on the other hand, the attack surface increases with the increased digitalisation of financial transactions and the use of cryptocurrencies, and cyber risks continue to grow, with a dramatic increase in 2022.

Conclusion

We seem to have a good understanding of the technical aspects, but finding evidence about the benefits that might be delivered is not easy. Some technologists indicate that digital currencies could be designed to do almost everything one wants, privacy, security, stability, scalability, etc., but that, in reality, there are tradeoffs among these goals that are the subject of ongoing research. Therefore, matching policy design and technical design is not easy for private cryptocurrencies, crypto assets, or CBDCs. This can be addressed in a tailored manner, based on different jurisdictions' decisions, but there will not be a one size fits all solution. There will be segmentation

³ Know your customer (KYC), anti money laundering (AML)

in the solutions for CBDC, especially in the current geopolitical climate. Countries are sovereign and need to protect their citizens first, so various possible solutions or designs will be implemented worldwide.

The workshop also discussed in some more depth other matters that will be presented in a next policy brief, including technical designs and regulations to ensure privacy (or anonymity, confidentiality), security (integrity, reliability) and performance (including convenience); motivations of distinct actors and implications for them of various types of digital currencies; and possible future scenarios.

Acknowledgements

The expert workshop that provided insights for these highlights took place on 25–26 October 2022, with the participation from **Rolf Alter**, Hertie-School of Governance; **Morten Bech**, Bank for International Settlements (BIS) Innovation Hub; **Maren Bodenschatz**, Swiss Re Management Ltd; **Nicolas Brügger**, Swiss State Secretariat for International Finance; **Catherine Burger**, Swiss Re Institute; **Edelweiss Choi**, Swiss Re Institute; **Jean-Pierre Danthine**, EPFL; **Othalia Doe-Bruce**, UN World Food Programme; **Margareta Drzeniek Hanouz**, Horizon Group; **Chris Fabian**, ITU Unicef Giga Initiative; **Andreas Felderer**, Swiss Re Management Ltd; **Nadia Filali**, Caisse des Dépôts; **Stewart Fleming**, Chatham House; **Marie-Valentine Florin**, EPFL; **Bryan Ford**, EPFL; **Katie Fortune**, Bank of England; **Kai Ganter**, Chainalysis; **Oliver Garrett-Jones**, OECD; **Christian Grothoff**, Bern University of Applied Sciences / GNU Project; **Jerry Gupta**, Swiss Re Institute; **Roman Hametner**, Mastercard; **Thi Hoang**, The Global Initiative Against Transnational Organized Crime (GI-TOC); **Gabriel Jaccard**, Arbitri/Crypto Valley Association; **James Larus**, EPFL; **Vincent Mele**, Accenture; **Thomas Moser**, Swiss National Bank; **Richard Olsen**, Lykke; **Gilles Papadopoulos**, Swiss Re Management Ltd; **Giovanni Piccioli**, EPFL; **Jags Rao**, Swiss Re Management Ltd; **Jean-Marc Rickli**, Geneva Centre for Security Policy; **Jean-Marc Seigneur**, University of Geneva / ITU Digital Currency Global Initiative; **Arun Sundararajan**, New York University; **Carolina Thomaz**, Sygnum Bank; **Jürg Unger**, Swiss Re Management Ltd; **John Velissarios**, Accenture; **Karl Wüst**, CISA Helmholtz Center for Information Security.

IRGC wishes to thank the Swiss Re Institute for their support and collaboration in the workshop.

Organisers and collaboration

IRGC works at the interface of research and public policy to develop guidelines, options or recommendations regarding risk issues marked by complexity, uncertainty and ambiguity. IRGC's approach to risk governance is particularly relevant for emerging and systemic risks where technology plays a role. The tight interconnection between opportunities and risk and between technical and governance aspects, which characterises the field of digital currencies, requires such an approach to capture and make sense of ongoing developments. irgc.epfl.ch

Horizon Group, Switzerland, is a research-based consultancy that combines insight and (big) data with unique expert networks to identify and leverage opportunities for investment and sustainable economic development. We help navigate uncertainty, inform major decisions and enable large-scale change. By providing metrics, insight and solutions, we support transitions to a future economy and society that is sustainable, inclusive and technology-driven.

Swiss Re Institute harnesses Swiss Re's risk knowledge to produce data-driven research across the company and with partner organisations. We foster knowledge sharing and support decision-making with our industry-focused publications, client programmes and conferences.

For any information, please contact marie-valentine.florin@epfl.ch.