Governing Opportunities and Risks of Digital Currencies

Scenarios of possible futures

Background paper

to the 25-26 October 2022 workshop at the Swiss Re Institute Center for Global Dialogue

This background paper was used to inform discussions at a workshop organised with Horizon Group and in collaboration with the Swiss Re Institute, at the Centre for Global Dialogue. The descriptions and views presented in it may be incomplete or not entirely accurate. Possible biases or errors in the description of certain aspects reflect the diversity of views on the benefits and risks of digital currencies, marked by fast changes, complexity, uncertainty, ambiguity, and significant economic and power stakes.

It was written between July and September 2022, so it reflects the state of the digital currency landscape at that time.

EPFL

irgc international risk governance center

Contents

Introduction

On 25 and 26 October 2022, IRGC convened a multi-stakeholder expert workshop to discuss benefits and risks related to the development of digital currencies (DC), including cryptocurrencies and assets. The workshop discussed motivations for various types of DCs and their implications, focusing on benefits and risks for distinct actors. It also discussed narratives (scenarios) of possible futures where digital currencies and assets significantly contribute to shaping aspects of economic and social life.

This document was written between July and late September 2022, and used as a background paper to inform the development of the workshop programme and some discussions. It does not reflect on the outcomes of the conversation, which are summarized in 'highlights' from the workshop published separately.

The collapse of FTX on 11 November adds to the numerous questions about the sustainability of the cryptocurrency business model and the value added to society. FTX was the second largest cryptocurrency exchange until it was declared bankrupt. Technically, this will not kill the cryptocurrency industry because its underlying blockchain layers remain, and trading can be made on other platforms. However, it is a cause of concern for new businesses that have grown largely unregulated, often on a lack of sound basis, and even possibly linked to fraudulent activities. Adding to the Terra Luna stablecoin collapse in May and the volatility and instability of crypto asset markets, this event raises attention again to the real value of the crypto venture. It suggests that benefits will be in niche markets and that the powerful and innovative technologies around blockchain, the internet and telecommunications might be better used to steer the established monetary and payment systems into improved delivery for the public good in a way that serves the real economy.

The facts presented in this paper have been selected to illustrate factors of benefits and risks, the role of digital currencies and assets in shaping monetary and financial policies, and meeting the needs of customers and society.

The questions asked in the paper are meant to help various organisations build their own position and objectives regarding digital currencies and assets in various scenarios, exploring digital currencies' dynamics and governance needs.

I. Background: Digital currencies in context

The possibility to capitalise on technological expertise applied to finance, the need to modernise payment and broader monetary systems, and other reasons, have triggered the development of a flurry of digital currencies (DCs) (see Figure 1) and projects from central banks. As a result, a new era for payments and financial transactions and for storing value has opened, creating many opportunities and benefits for some, but risks for others. Notably, central banks and commercial banks are no longer the only actors in money creation. The dramatic growth in the use of digital currencies will have significant implications for various economic actors, particularly consumers, investors and businesses. The field is high on the financial policy agenda and has the potential to transform the world financial system.

Technology innovators and investors are at the core of promising development. However, and because they might be the first to benefit from DC adoption, their role must be scrutinised and not exacerbate private interests, financial power or geopolitical tensions that would not benefit societies overall.

What do we mean by digital currency?
For the purpose of this paper, we use the term digital currency (DC) to describe currency that exits in electronic form and that may or may not be available in physical form. DCs may also have characteristics of a commodity or other asset. They can be based on a variety of technologies (not only blockchain) and issued by different actors, public or private. They differ from existing digital forms of money (e.g. money held in accounts) in how they are issued, governed and distributed. Our working definition of digital currencies is thus broad, in order to capture a wide range of impacts on the economy and society.
For more details, see section II.

There are several thousand digital currencies and their number has grown rapidly, particularly in the last two years (see Figure 1). The original bitcoin, created in 2009, was followed by second-generation cryptocurrencies like Ether, third-generation instruments like stablecoins, some Central Bank Digital Currencies (CBDCs), and other digital assets such as non-fungible tokens –NFTs. This is paralleled by the growth of Decentralised Finance (DeFi) and the recent trend for Centralised Finance Platforms (CeFi)[1] or hybrid models.

- The market capitalisation of cryptocurrencies peaked at 2500 billion USD in Q4 2021, falling to about half of that value in May 2022[2] when the 'crypto winter' started, and 860 billion USD on 22 November 2022[3]. Nevertheless, it is still higher than in November 2020. See Figure 2 below.
- On the side of central banks, more than 100 countries are exploring CBDCs at one level or another.

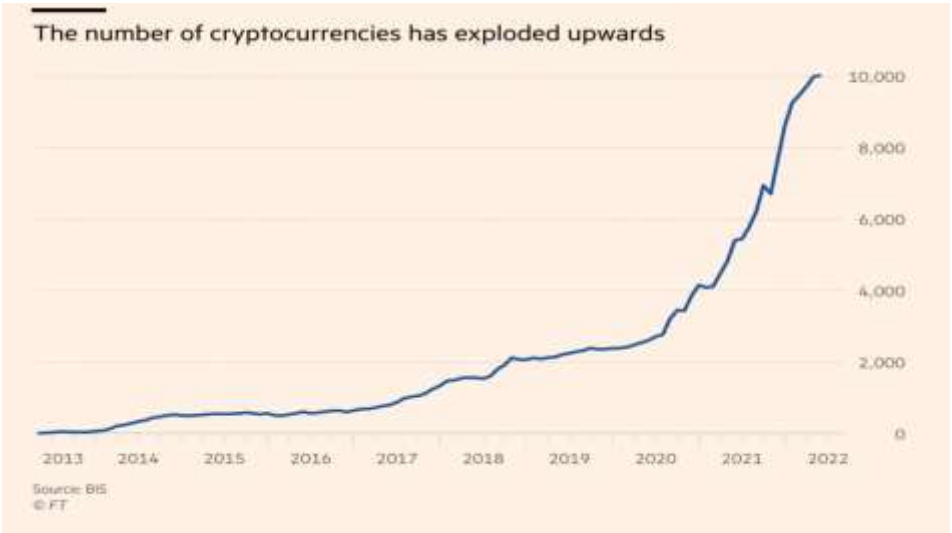


Figure 1 - Number of cryptocurrencies[4]

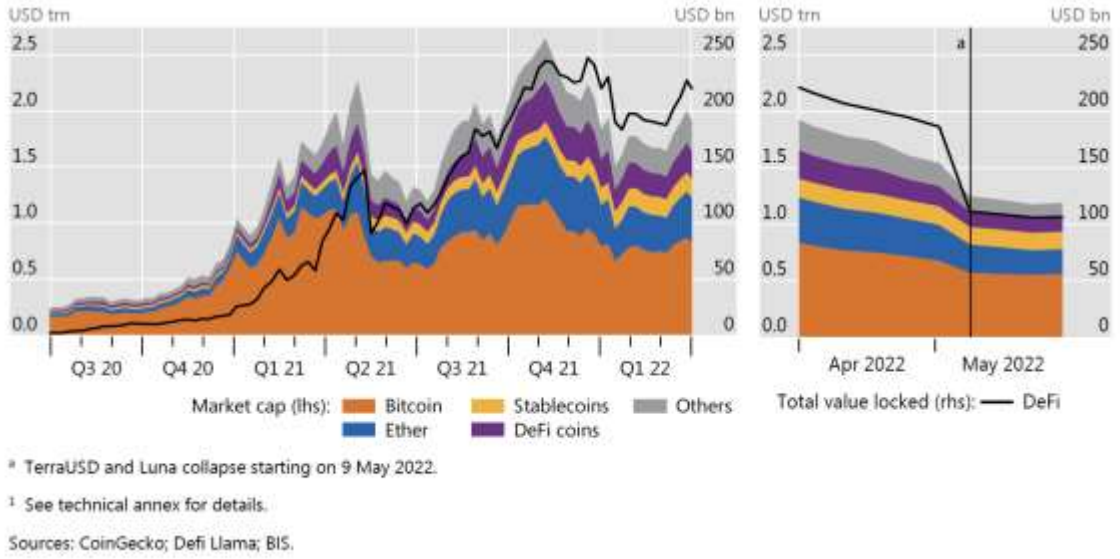


Figure 2 - Market size of cryptocurrencies and DeFi, June 2022[2].

Opportunities

The development of digital currencies presents opportunities for many because it has the potential to address a large diversity of unmet needs. Significant improvements in current systems are expected, including in payment system efficiency, as a complement to cash money and, in some countries, financial inclusion (see Box 1 below). For investors, crypto assets present opportunities for portfolio diversification, flexibility through tokenisation and value creation. [5]

At one end of the spectrum, some cryptocurrencies promise a more democratic financial system that could remove the need for undesirable or inefficient financial intermediaries and give users greater control of data. On the other end, CBDCs could contribute to governments' monetary and financial policy goals, and be designed to support the real economy and increase and distribute welfare. See G7 public policy principles, for example[6].

Financial inclusion

Today, 1.7 billion people globally have no bank account. This hampers their ability to benefit from the economy, e.g. getting a job in the formal economy with social security benefits, accumulating assets for old age through the financial system, access credit and housing or healthcare. DCs, in particular CBDCs, are often viewed as contributing to financial inclusion by reducing costs, e.g. bank fees and barriers (e.g. minimum balance requirements) to obtaining bank accounts. Cross-border payments (remittance) could be faster and cheaper.

According to a report from the Digital Currency Global Initiative (DCGI)[7], for DCs to help support efforts to bridge the financial inclusion gap, they must be interoperable, secure, effectively regulated and supervised, have universal access and availability, and operate through competitive and open networks. In addition, governments and financial intermediaries should develop digital financial literacy programs. Other important prerequisites include digital access and literacy among the population.

Although not immediately related to inclusion, the issue of price stability is also critical, as using or investing in unstable assets could have dramatic consequences for low-income individuals. In order for a currency to be meaningful, it must hold stable value and should not be speculative in nature.

In conclusion, it is not proven that new currencies are really needed to achieve financial inclusion.

Box 1 - Financial inclusion

Risks

However, digital currencies, and in particular private cryptocurrencies, also carry many risks and often fall behind expectations.
Depending on their technical design, risks related to DCs include those to privacy, security, financial stability, financial market and payment system integrity, national security, equity, and the climate and environment through electricity consumption. Also, attention to cybersecurity risk[8] is growing. For instance, for privately issued digital or cryptocurrencies:

- **Individual users, consumers and businesses** are confronted with risks of crimes such as fraud or theft, privacy and data breaches, ransomware and other cyber incidents or attacks, and unfair or abusive acts or practices. Consumer protection is currently poor.
- **Societal risks** also include a risk of friction when the mode of payment cannot be trusted in the same way as fiat currency payments that represent a contract between the government and the holder of the currency.
- **Financial risks** are linked to enabling payments in DCs and having digital assets on balance sheets.
- Recent events (cf. collapse of Terra in April 2022) have demonstrated the potential impact on **financial instability**. Crypto assets such as stablecoins show an increasing risk to financial stability due to the complexity, size and growing involvement of institutional investors. And we know from experience in the subprime crisis of 2008 that failures in an apparent small market can have systemic consequences worldwide.
- Cryptocurrencies like bitcoin that are based on proof-of-work generally adversely impact the **environment and climate** through enormous electricity consumption and electronic waste. For example, it is estimated that the annualised Bitcoin network power demand is 95.42 TWh[9]. Ethereum switched to proof-of-stake consensus on 15 September 2022, which is anticipated to reduce its electricity consumption by more than 99%. Cf. Recent updates on "The Merge", which will potentially have significant implications for the future[10].

Governance aspects

Because DCs and digital assets are becoming an integral part of the monetary and financial system and some private CCs are often considered an alternative to the currently used sovereign-backed fiat money, they need to be regulated under monetary and financial regulation. They must be part of monetary policies.

Users of digital currencies want to get assurance that their payments are made in something with stable value, involving "a design of the currency that makes it stable and flexible, a governance regime that instils trust in the currency, and the provision of sufficient liquidity and some sort of stable backing"[11]. This raises the issue of how to design regulation and organise possible competition between privately issued digital currencies and CBDCs, reminding us that the monetary system is also an important public good central to the efficient functioning and stability of any economy.

Governments and regulators have to (or at least consider whether they should):

- Adapt public regulation to address various risks potentially posed by peer-to-peer disintermediated payments, uncontrolled blockchain-based DLTs digital assets, and growth in Decentralised and Centralised Finance Platforms (DeFi and CeFi), among others.
- Set standards for transparency, privacy[12, 13], security (confidentiality, integrity and availability)[14] and interoperability.
- In the face of the proliferation of new private actors, find ways through action from central banks to ensure that the monetary system will continue to work in the public interest in a fully digital future.

- Promote the rule of law and respect of democratic practices and other fundamental principles. It is critical that institutions and processes develop response strategies that consider the public interest and encourage responsible innovation in the financial sector. Democratic practices vary across jurisdictions, so their evaluation also depends on political cultures.
- Drive the growth of the digital asset ecosystem with caution, and balance the pros and cons of decentralised finance.

International collaboration among large businesses, governments, central banks, traditional banks and other new financial sector actors will be needed because technology-driven innovation develops across borders (international trade). Regulatory fragmentation and uncoordinated oversight and control may contribute to increasing risks to financial stability for consumers, investors and businesses.[15, 16, 17]

See Box 2 on metrics and Box 3 on regulation below.

Metrics to evaluate the robustness of different DC technologies against the requirements set by various stakeholders; Standardisation

Developing robustness metrics is one of the objectives of the Digital Currency Global Initiative (DCGI)[18], a collaboration between the International Telecommunication Union (ITU) and Stanford University's Future of Digital Currency program[19]. The DCGI brings together stakeholders in the DC ecosystem to discuss, among other aspects, elaborating specifications for technical standards to foster adoption, universal access and financial inclusion. It will develop a set of methods and metrics to evaluate, validate and benchmark the different characteristics of DC technologies against the requirements set by various stakeholders. Those methods and metrics will also evaluate the performance, scalability, operational efficiency, interoperability, security and resilience of existing and future implementations, against a set of common requirements.

Box 2 - DC robustness metrics and standardisation

Public regulation to address risk and arbitrate trade-offs

When regulation is principle-based, this allows looking at the substance of a project, and providing guidance with evolving legal frameworks as needed. The principle of 'same activity, same risk, same rule' can be applied.[20] Various types of risk can be regulated to protect market stability and consumers, with one notable characteristic: in DC systems, interconnections between actors and risks are very tight, and correlations can quickly cause risk to escalate and become systemic.

Consumer protection. In contrast to money laundering, it is more difficult to agree at the international level on how to protect consumers against the risk of misusing digital currencies. There are significant variations across regulatory cultures. Ensuring consumer protection relies on multiple measures, among which proper understanding, reporting and disclosure of risks, and consumer information.

Operational risks. In the context of DCs, technology can both mitigate and create new risks, which new or revised regulations will have to consider.

Examples of passed, proposed or considered for future regulatory frameworks:

- Switzerland: Federal Act on the Adaptation of Federal Law to Developments in Distributed Ledger Technology, passed on 1 August 2021, [21]

"On 1 August 2021, Switzerland became one of the first countries in the world to enact legal regulations for blockchain technology. This creates legal certainty and enables innovation and growth. For Switzerland, the integrity of the financial centre is central. It attaches importance to ensuring that the same rules apply to cryptocurrencies as to real monetary assets, e.g. in the area of combating money laundering, Switzerland is actively working for the rapid international implementation of the corresponding international standards so that no loopholes in the law and no havens for criminal business are created…. The law will provide a secure legal basis for the trading of rights through electronic registers. Furthermore, the segregation of crypto-

based assets in the event of bankruptcy will be clarified by law. Finally, a new licence category for DLT trading systems will be established in financial market infrastructure law, thereby creating a flexible legal framework for new forms of financial market infrastructure." SIF

- In Europe: Proposed Regulation on Markets in Crypto-Assets (MiCA), adopted by the Council presidency and European Parliament on 30 June 2022.[22]

MiCA has 4 broad objectives:
- To provide legal certainty for crypto-assets not covered by existing EU financial services legislation, for which there is currently a clear need.
- To establish uniform rules for crypto-asset service providers and issuers at the EU level.
- To replace existing national frameworks applicable to crypto-assets not covered by existing EU financial services legislation.
- To establish specific rules for so-called 'stablecoins', including when these are e-money.

MiCA will protect consumers against some risks associated with crypto-assets investments. Crypto-asset providers will have to respect strong requirements to protect consumers' wallets and become liable in case they lose investors' crypto-assets. Actors in the crypto-assets markets will be required to declare information on their environmental and climate footprint. The updated legislation on anti-money laundering will now also cover crypto-assets. Stablecoins issuers will be requested to build up a sufficiently liquid reserve with a 1/1 ratio and partly in the form of deposits. Non-EU-based crypto-asset service providers will need an authorisation to operate in the EU. NFT will be excluded from the scope of MiCA except if they fall under existing crypto-asset categories.

- In the US: Executive order on Ensuring Responsible Development of Digital Assets, signed on 9 March 2022[23]

"The President's order represents the first time that the White House has sought to develop a coordinated plan for the regulation and development of digital assets, and it thus represents an important first step in direction of a consistent regulatory policy. The Executive Order specifies key policy objectives to guide this effort: (1) protecting US consumers, investors, and businesses; (2) preserving the stability of the US and global financial systems; (3) preventing illicit finance and national security risks; (4) reinforcing US leadership in the global financial system and technological competitiveness; (5) promoting access to safe and affordable financial services; and (6) promoting responsible technological development. While the Executive Order attempts to balance the risks and potential benefits of digital assets, it focuses on and prioritises addressing the risks".

On 16 September 2022, the White House released a comprehensive framework[24] that covers illicit finance risks regulation, AML/CFT regulation, supervision and standards implementation, private sector engagement and how Treasury can most effectively support the incorporation of AML/CFT controls into a potential U.S. CBDC design. The framework recognises that opportunities in digital assets exist, but those must be consistent with consumer protection policies and enforcement, and the priority is to fill gaps in the current regulatory framework.

Box 3 – Regulation

Focus on: Illicit and informal economies as important actors

A parallel driver of cryptocurrency development has been the technical possibility of avoiding some institutional oversight and establishing a new form of distributed power. Cryptocurrencies challenge current laws, regulations and commitments from institutions towards responsible financial innovation and competition. In their basic form, they are resistant to regulation and taxation. They provide a channel for conducting financial transactions outside the current legal and regulatory frameworks.

Digital currencies have facilitated sophisticated cybercrime-related financial networks and activities, and drug and human trafficking.

- The illicit economy[25] benefits from opportunities presented by private digital currencies, although it is difficult to make an informed judgement about the extent of the problem (see Box 4 below). However, gaps in regulation that enable unregulated crypto trading platforms

to engage in fraudulent activities and trade with illicit and malicious actors are not acceptable.

- The informal economy[26] might also benefit from digital currencies, but the links are poorly understood. Whether or not CBDC could be part of the public policy and legal response needs to be explored.

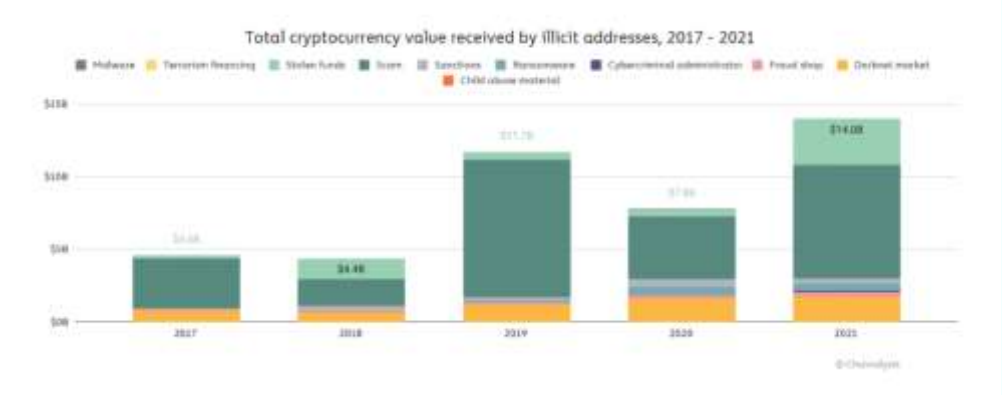
It will be critical to thoroughly understand the motivations and 'needs' of actors in the illicit and informal economies, to design DC regulatory schemes for investigation and prosecution that can be effective, implemented and enforced. To do so, and although this may look naïve, one needs to find ways to engage with actors in the illicit economy before devising desirable and plausible scenarios for the future and making policy decisions around DCs.

The illicit economy and interests of its actors

Cyber- and crypto-dependent crime, especially transnational organised crime, represents a significant part of the use of cryptocurrencies. CCs are not related to cybercrime only, but are used for different types of illicit activities that require the transfer of value to fiat currencies. These include: ransomware and cybercrime; illegal trade in licit and counterfeit drugs; illicit drugs, goods and other services such as illegal environmental markets; human exploitation and trafficking, tax evasion. Networks that provide money laundering as a service using cryptocurrencies have emerged, and are able to anonymise transactions by changing wallets.

The Global Initiative Against Transnational Organized Crime (GI-TOC) commented in "The Global Illicit Economy: Trajectories of Transnational Organized Crime", published in March 2021,[27] that:
"As innovation continues to outpace regulation, new technologies allow illicit economies to grow by improving and encrypting communications; creating new marketplaces on the surface web and dark web; changing ways of doing business (for example, by anonymising payments through cryptocurrencies)" […]. On the dark Web, the drug trade is characterised by low operating costs, high use of cryptocurrency and young tech-savvy dealers, rather than cartels". In a more recent report of June 2022, GI-TOC analyses cryptocurrencies 'as an enabler of organized crime', noting that their role in facilitating transactions is rising, although it remains relatively low compared with cash and other forms of illicit transactions [28]

The scale of using cryptocurrencies in illicit transactions is difficult to evaluate. Chainalysis Inc. estimates that:
- The illicit activities' share of total cryptocurrency transaction volume amounts to 0.15% of all crypto transactions in 2021, down from 0.62% in 2020 –noting though that the total volume of CC transactions has dramatically increased.
- CC represented in 2021 an estimated 0.86% of annual money laundering (money leaving illicit addresses), with these funds increasingly going to DeFi – noting though that most of ML still goes through traditional finance.[29]
- Illicit addresses received $14 billion in cryptocurrency-based crime, up from $7.8 billion in 2020 (see figure below). [30]



27

Box 4 - The illicit economy

Focus on: Central Bank Digital Currencies (CBDCs)

Currently, sovereign-backed (fiat) money is central to the efficient and fair functioning of the economy. Many countries worldwide are exploring retail CBDCs in complement to cash because of the many advantages they can bring. The main driver behind the development of retail CBDCs is the promise of cheap and efficient payment systems that meet the needs of a digital economy and enhance financial inclusion where this is needed. Anonymity is also expected. However, the plausibility of scenarios with fully private CBDC transactions is debatable, because it would conflict with security and transparency to central banks or intermediaries.

CBDCs must be able to compete with private digital currencies and their main strength is perhaps that, as a direct liability of the central bank, they eliminate significant counter-party risk. CBDC is a form of fiat currency, with the three functions of a unit of account, a means of payment and a store of value for a jurisdiction. However, for CBDCs to be successful, they should also present net benefits compared to other sorts of DCs.

Financial stability, payment integrity, security and privacy issues are and will remain critically important for central banks, at least in G7 countries. Those explore whether CBDCs can help them achieve their public good objective (safeguarding public trust in money, maintaining price stability and ensuring safe and resilient payment systems and infrastructures). For that purpose, the choice of particular technical design options will dramatically influence the adoption and outcomes of CBDC and associated payment systems.[31] Whether CBDCs are needed is a matter of debate, but for individuals at risk from private digital currencies, CBDCs should be able to offer better consumer protection from several risks, including those caused by digital and financial illiteracy.[32] However, some authoritarian regimes could use their CBDC to control citizens' use of money, which could have dramatic consequences on civil liberties.

Because there are significant variations between countries, there is no one size fits all solution[33], and "CBDC issuance and design are sovereign decisions to be made by each jurisdiction"[34]. However, for CBDCs to be effective beyond the domestic level, they must coordinate with others to ensure interoperability and support efficient, low-cost, safe, and secure international fund transfers and payments. Adaptation of legislative and regulatory frameworks will be needed. While general principles must be similar, some variations will reflect the specificities of regulatory cultures[35]. For example, see the EU agreement on a crypto-assets regulation (MiCA) reached on 30 June 2022[36] (cf. Box 3).

Focus on: Cryptocurrencies, DeFi and Web3, CeFi

The prospect of Web3 (see Box 5 below), a fully decentralised internet supported by distributed ledger technologies, must be considered when thinking about the future of digital currencies. Decision-making can be decentralised, making institutions more transparent and transforming how organisations are governed. Among other opportunities, Web3 could "bring back competition to digital platforms".[37]

Web3 enables Decentralised Finance (DeFi) that, in theory, eliminates the need for intermediaries, because it is built on blockchain, permissionless and interoperable, and uses CCs.
DeFi can serve many businesses, such as insurance, allowing policyholders to get coverage for certain risks (mainly against smart contract failures and the risks related to their deposited crypto assets) without any centralised insurance intermediary (e.g. Nexus Mutual).

Developments towards Centralised Finance Platforms (CeFi) would, however, add another layer that can compromise the vision of perfect decentralisation. CeFi companies (like Coinbase) deal primarily with cryptocurrencies or NFTs, but without open-source smart contracts to record operations. They do not use or need to use blockchain systems, make their own rules privately with their customers, and thus reintroduce principles of control and authority.[38]

On the side of risks, the Bank of International Settlements (BIS) annual Economic Report 2022 summarizes: "Structural flaws make the crypto universe unsuitable as the basis for a monetary system: it lacks a stable nominal anchor, while limits to its scalability result in fragmentation. Contrary to the decentralisation narrative, crypto often relies on unregulated intermediaries that pose financial risks". [39]

Web3

Web3 refers to a vision for what the internet could look like in its next iteration, a decentralised ecosystem underpinned by blockchain technology. Web3 fully embraces decentralisation and is being built, operated, and owned by its users (permissionless and trustless). The Web3 movement is tightly connected to the development of future cryptocurrencies, crypto wallets, NFTs, Decentralised Autonomous Organisations (DAO) and DeFi.[40] However, full-scale Web3 implementation faces several technical challenges regarding: computation and scalability, bandwidth and efficiency, and storage and data ownership.[41] It also faces governance challenges regarding the desirability, acceptability and legitimacy of such a system.

Web system, Type of economy	**Web1 Centralised economy**	**Web2 - The Web today Platform economy**	**Web3 Protocol economy**
Model	Corporate model: Employees within companies provide goods and services. Corporates focus on growth and wealth generation for shareholders	Marketplace model: Contributors outside companies also generate value. Markets generate value for share- and stakeholders, i.e. contributors and end consumers. Increasingly controlled by large technology companies	Permissionless model: Any participants are enabled and incentivised to contribute. Networks provide value to all contributors and users.
Data, Computing	- Low data sophistication: Lack of infrastructure, technology and business proposition for data usage and analytics - Local computing	- Increasing data usage: Industry, market and consumer data are used to enhance operations - Cloud computing	- Principle of data sovereignty: data is key to the economy and is prioritised and protected - Distributed computing
Technology design aspects	- Centralisation and control	- Privatisation and proprietary systems - Multi-tiered system relying on a central authority and intermediaries	- Web3 techno design, DLTs, smart contracts, crypto assets, metaverse - Automated and decentralised system
Examples	Nokia, MySpace, Yahoo, Walmart	Amazon, Uber, Facebook, YouTube	Bitcoin, Ethereum
Reference to section V (scenarios)	*Scenario A: Central banks take the lead*	*Scenario B: Private actors create private DCs and provide efficient and cheap monetary systems*	*Scenario C: a Web3-based, fully decentralised and permissionless system dominates monetary and payment systems*

Box 5 – Moving from Web 1 to Web3

Conclusion: fundamental questions for the future of digital currencies and assets

- What are the **socio-economic challenges and needs** that specific forms of crypto or digital currencies and assets could address from various stakeholders' perspectives? Which societal challenges may require new currency instruments and new payment systems?
- Which **fundamental shifts in society** may occur due to the large-scale deployment of specific types of DCs? Which stakeholders will be empowered by DCs, and which will lose power?
- What options are available **to manage various stakeholders' needs, expectations and risks**? How to govern risks for distinct stakeholders while reaping benefits for society?
- What role could **the non-financial sectors** play concerning DC development?
- What if cryptocurrencies would not exist? What would be better? Worse? At least cybersecurity would be less of a problem.

II. Overarching characterisation of digital currencies and assets

This section provides some overarching considerations about the various types of digital currencies and assets, acknowledging that the field is fluid and subject to various definitions and views.

Terminology

For the purpose of this paper, we use the following brief definitions:

- **Cryptography** is a branch of study at the intersection of mathematics and computer science that studies how to secure communications: masking information that must be hidden in plain sight and verifying the source of information pieces. Various types of cryptographic techniques are used in cryptocurrencies.[42]
- **Cryptocurrency:** a private digital currency that depends primarily on cryptography and distributed ledger or similar technology. (cf. FSB[43])
- **Digital asset**: a digital representation of value, which can be used for payment or investment purposes. This paper does not include digital representations of fiat currency. (cf. FSB)
- **Crypto asset**: a type of private digital asset that depends primarily on cryptography and distributed ledger or similar technology. Example: Non-Fungible Tokens (NFTs)
- **Stablecoin**: a digital asset that aims to maintain a stable value relative to a specified asset or a pool or basket of assets.[44] (cf FSB)
- **Central Bank Digital Currency (CBDC):** a **retail** CBDC is a digital form of central bank money that is widely available to the general public.[45] Example: The digital euro "would be a central bank liability offered in digital form for use by citizens and businesses for their retail payments" (ECB)[46]
- **Decentralised Finance (DeFi)**: an umbrella term for DLT-based business models. DeFi involves replacing traditional financial intermediaries with smart contracts.

Digital or cryptocurrencies, digital or crypto assets aim to replicate all or some of the purposes of traditional money – a means of payment, a store of value, and a unit of account. The terms used cover a wide range of financial instruments with different technical, legal, and practical characteristics. There are many ways of categorising digital currencies and assets (see Box 6 below), and several authors or organisations have produced typologies. These typologies reflect specific steps or phases of DC developments, or underlying choices such as goals or prioritisation of certain features.

How to categorise DCs?

Typologies or categorisation of digital currencies or assets depend on various features:

- *Issuer:* central bank or private actor; actor in the traditional financial system or in DeFi
- *Underlying Technology:* Blockchain-based, or not. When a private issuer considers creating a DC, it analyses the pros and cons of various types of blockchain systems, also considering that there is a multitude of 'blockchain' systems, from the original software used for bitcoin to simple relational databases.
- *Organisational form and governance:* There is a range of blockchain systems on the control spectrum, from fully opened (permissionless) to fully controlled (permissioned), and on the centralisation-decentralisation spectrum.
- *Backing:* Unbacked cryptocurrency (e.g. BTC) or backed (e.g. stablecoin, CBDC)
- *Function and purpose:* for the three functions of money, or only for transactions (payment) and value (asset). If a DC is primarily conceived as a means of payment, the opportunities it presents must be compared with those of mobile payment systems that do not imply a new currency.
- *Goal:* replace cash or fiat money, meet broader needs and demands of societal actors, enhance the competitive advantage of the issuer, support Web3 (see Box 5), hide from institutions and law enforcement, tokenise (fragment) assets, etc.
- *Limitation: number* limited by design (e.g. bitcoins) or decision, vs not limited

Box 6 - How to categorise various types of DCs?

Opportunities and risks must be spelt out for each type of DC

For each type of DC, distinct actors can have different answers to the questions of:

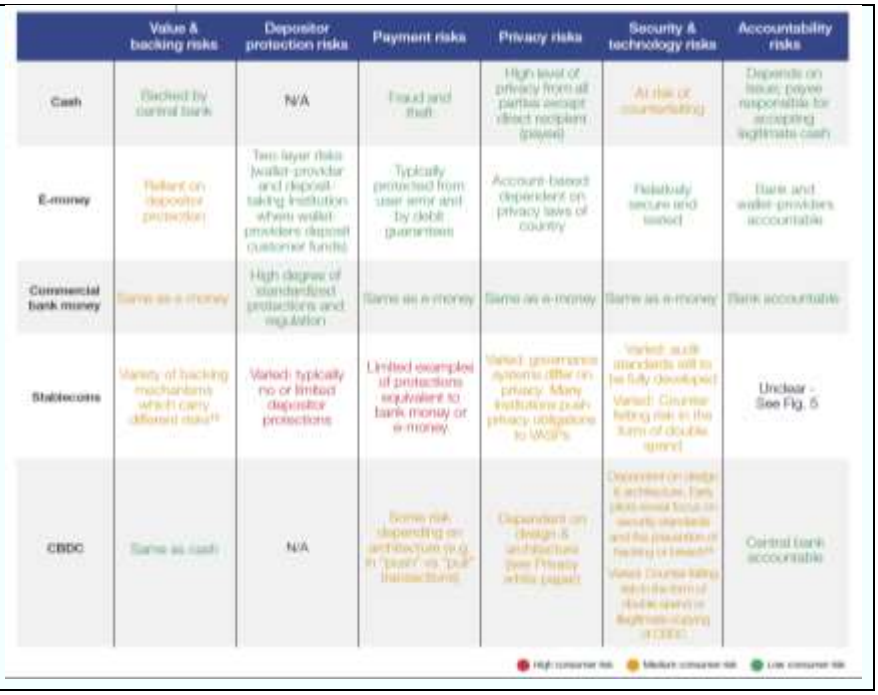
- *What are the main opportunities or anticipated benefits?*
- *What are the major challenges or risks?*

Opportunities and risks can be evaluated in terms of impacts on: monetary policy, financial stability, financial inclusion, domestic and cross-border payment efficiency, privacy (or anonymity, confidentiality), security (integrity, reliability), money laundering (and AML), terrorism financing (and CTF), scalability, etc.[47].

For example, Box 7 below offers a list of risks for consumers, posed by various types of money.

Risks posed by various types of money, from a consumer's perspective.

Comparison of current top-line consumer risks in existing systems and digital currencies



Source: Digital Currency Consumer Protection Risk Mapping, World Economic Forum White Paper November 2021[48]

Box 7 - Risks to consumers

Specific types of digital currencies and assets, usage, opportunities and risks

A. Original cryptocurrency: Bitcoin

In September 2022, 106 Mo people worldwide owned bitcoins, and 400,000 people used them daily.[49]

- Main technical features: based on the original blockchain design[50], proof-of-work, fully distributed and permissionless. The number of bitcoins that can be mined is limited by design, but it is impossible to derive any anticipation of its future value from this fact.[51]
- Is primarily used as a peer-to-peer electronic cash system[52] by a wide range of actors, but also as an investment.
- Opportunities and risks are tightly interrelated. Volatility and low-level or absence of consumer protection for many investors and end-users come first. Bitcoin is a tradeable asset that is not backed by anything. However, for some, the threat of tighter regulation is the main risk they face.
  It is also worth noting:
  - The 'blockchain trilemma', which illustrates the theoretical impossibility of reaching three competing goals of decentralisation, scalability and security (although it has not been proven yet that this is a problem and that this is true) and to address other concerns among which privacy.[53]
  - Growing criticisms from many, including software engineers[54], thinkers, and influencers[55], who quote: "pure speculation, no value at all, Ponzi scheme, fraud, etc."
- Regulatory status: evolving quickly. Authorised in some countries but prohibited in others.

B. Second generation of cryptocurrencies, such as Ether

In September 2022, Ether was the second CC in the number of traders and the first in terms of trading amount[56].
In contrast to 'all-purpose money', many private CCs are designed to address particular challenges and target certain user groups. They are developed for a specific purpose, such as ensuring users' anonymity. Based on smart contracts, they are also described as 'programmable money'.

- Main technical features: blockchain-based[57], moving to proof-of-stake (PoS)[58], more or less controlled or centralised.
- Many different types of uses. In the specific case of Ether, the main goal is to make the Ethereum smart contract and decentralised applications platform operations easier to use and monetise, rather than to establish itself as a new monetary system. Ripple was created to rival SWIFT as a payment transaction platform.
- Main opportunities and risks: depend on their purpose, technical features and uses. Additionally, there is a vast variety of opinions across actors[59].
  For example, regarding Ethereum's move to PoS, an analyst for CoinDesk wrote on 15 September (date of "The Merge"):" In proof-of-stake, the amount of ETH one stakes […] dictates control over the network. Proof-of-stake boosters say this makes attacks more expensive and self-defeating: attackers can have their staked ETH slashed, or reduced, as punishment for trying to harm the network. […] And although control of the Ethereum network will no longer be concentrated in the hands of a few publicly traded mining syndicates, critics insist that old power players will just be replaced by new ones. Lido, a kind of community-run validator collective, controls over 30% of the stake on Ethereum's proof-of-stake chain. Coinbase, Kraken and Binance – three of the largest crypto

exchanges – own another 30% of the network's stake."[60] So challenges also include the risk of power shifts.

- Regulatory status: evolving quickly. Authorised in some countries but prohibited in others.

C. Stablecoins

Tether, Binance USD, the defunct Diem (a permissionless blockchain-based stablecoin payment system), US Terra/Luna, or USDC are examples of stablecoins. [61]

- Purpose: "An attempt to address the high volatility of traditional crypto-assets by tying the stablecoin's value to one or more other assets, such as sovereign currencies".[62]
- Main technical features: Based on stabilisation mechanisms that either peg the value of the coin to a fiat currency or other recognised store of value (e.g. reserves of currencies or other assets, such as gold or debt instruments), or that rely on algorithms or other cryptocurrencies to stabilise the value.
- Use: Is primarily used by crypto investors to diversify and provide a way of exchanging CCs for goods and services. Initially intended to reduce volatility and facilitate cross-border payments, Stablecoins can also be used as a store of value.

	Investor	Retail buyer/seller	Participant of protocol governance[7]
Stablecoin usage	– Provide capital denominated in stablecoin to earn a return – Park money for future trading of cryptocurrencies	– Exchange for goods/services	– Can be either an investor or a retail buyer/seller
Risk	– Inability to redeem face value – Deposit liability claim – Price volatility	– Inability to redeem face value – Deposit liability claim – Price volatility	– Rights being infringed by majority holders

Box 8 - Risks associated with different uses of stablecoins

- Main opportunities and risks:
  - More stability, if design and institutional set-up are appropriate.
  - Instability, if fungibility cannot be guaranteed (e.g. in the case of a sell-off)
  - Price volatility
  - Deposit liability claims.

  See Box 8 and Cf. Collapse of Luna/USTerra in May 2022.[63]
- Some see stablecoins as a substitute for fiat currency in the absence of CBDC.
- Regulatory status: to address the stability risks, regulation at the national level is needed to provide supervision and oversight of global stablecoin arrangements. Fiat-based stablecoins are more likely to be regulated by the emitting governments.

D. Central bank digital currency (CBDC)

Eleven countries (e.g., Jamaica, the Bahamas or Nigeria) have already launched a retail CBDC. In addition, China is planning to launch the e-CNY in 2023. According to the BIS, 90% of central banks are considering CBDC currency projects.[64]

- Technical features will differ depending on the institutional set-up, particularly if the CBDC is (a) for retail or (b) for wholesale. Technical design choices will be critical (depending on policy choices)[65]. The infrastructure can be proprietary or not (for example, using the Ethereum platform).
- Retail CBDC would be primarily used by citizens to replace or complement cash and deposits (money): the use of cash, currently the only form of direct central bank money

available to the public, is falling in many jurisdictions. Instead of cash, individuals increasingly use mobile payments. CBDCs would be similar to 'digital banknotes'. For a retail CBDC, offline use may be necessary, but avoiding double spending will not be possible in this case, so either limits can be put on offline use, or someone must take the risk of offline money being spent more than once.

- Other challenges for retail CBDCs include security (AML, KYC), privacy (anonymity) and convenience (adoption), and there is no clear answer on how a CBDC could resolve all the trade-offs.
- Finally, trustworthiness will be a key determinant of success for investors and end-users.
- Matters of national security and sovereign control over domestic market are critically important.
- However, the primary motivation could be elsewhere: provide a competitive solution to combat the proliferation of private digital currencies controlled by private actors, which might "result in a fragmented monetary system and jeopardise universal access to public money". With CBDCs, central banks can find "ways to ensure that the monetary system will continue to work in the public interest in a digital future"[66].
- Other motivations also exist, such as greater control of the economy by the government, additional tools in a government's monetary policy toolbox, or enhancing financial inclusion of unbanked individuals in developing countries and elsewhere, with significant uncertainties, however, about effectiveness.
- Main opportunities and risks: see Box 9 below. Also, there are signs that CBDCs can be used for surveillance and social control in authoritarian, state-capitalist systems.
- Regulatory frameworks (adaptation of current frameworks) will reflect policy priorities and trade-offs between, for example, privacy (including anonymity and confidentiality, which so far can only be met by cash) and security (illustrated by legal dispositions for Anti-Money Laundering-AML, Know Your Customer-KYC, and Counter-Terrorism Financing-CTF). Technical options exist and their adoption depends on policy choices. See Box 3 for examples of regulations adopted or considered in Switzerland, the EU or the US; and their underlying principles.

Benefits and risks of CBDCs

In "Design Choices for Central Bank Digital Currency: A Position Paper", published by Brookings (July 2020), the authors [31] present "*the main potential benefits spurring central bank exploration of CBDCs as:*

- *Efficiency: CBDCs can reduce friction in existing payment systems, potentially lowering the cost and increasing the speed of transactions while ensuring finality.*
- *Broader tax base: CBDCs can potentially bring more economic activity into the effective tax base, limiting tax evasion, boosting tax revenues, and inhibiting the use of CBDC for illicit purposes.*
- *Flexible monetary policy: CBDCs could facilitate novel flexibility in monetary policy, theoretically allowing central banks to institute negative nominal interest rates and implement non-distortionary helicopter drops or withdrawals of central bank money.*
- *Payment backstop: CBDCs could act as a backstop to privately managed payment systems, avoiding the risk that payment systems will break down in times of crisis.*
- *Financial inclusion: CBDCs could serve as a gateway for unbanked and under-banked individuals to have access to electronic payment systems and, potentially, to other financial products and services as well.*

The many potential benefits of CBDCs should be weighed against potential risks, both financial and technical, including:

- *Disintermediation of the banking system: Many CBDC plans involve a two-layer architecture; the CBDC itself serves as a basic functional layer, while existing non-governmental financial institutions manage a second layer that interfaces with users. Nonetheless, by reducing transaction frictions and possibly even providing interest-bearing accounts, CBDCs could disintermediate significant swaths of the banking system, with potentially destabilising systemic effects.*

- *Miscalibration of government involvement: The balance between ensuring adequate central-bank oversight and leaving room for innovation may be challenging to strike, with risks to overemphasising either side.*
- *Financial risks due to lack of regulatory expertise and capacity: Regulators may struggle to develop the tools and expertise to address the dramatic structural changes and financial innovations brought about by CBDCs.*
- *Loss of privacy: Given the limitations of current privacy-enhancing technologies, it seems likely that a true retail CBDC will expose new forms of sensitive information to CBDC operators. CBDC designers should consider legal and technical mitigations from the outset.*
- *Technological vulnerabilities or entrenched design mistakes: Even with conservative design, CBDCs will represent a technical experiment with significant risk of information-security failures. Design mistakes may be especially difficult to fix."*

Box 9 - Benefits and risks of CBDCs

E. Digital / crypto assets (other than currencies)

From a financial system perspective, digital assets are different from DCs.
- DCs are intended as means of payment and assets.
- Some digital assets cannot be used for payment. They rely on a digital means of payment. For example, most NFT transactions are labelled in Ether and use the Ethereum blockchain network.
- Digital assets thus comprise cryptocurrencies, other digital currencies, and crypto assets, defined as asset tokens that represent rights, such as shares or NFTs, or financial or physical assets, such as stocks and bonds, goods like wine[67] or real estate. In 2021 the market for FNTs reached 44 billion USD.

- Technical features: unique cryptographic tokens, usually on the blockchain, cannot be replicated; enable the fractionalisation of assets.
- Are primarily used as a store of value by investors that ensure tradability and higher liquidity (e.g. for real estate). In some domains, the use cases are similar to notarization.
- Main opportunity: higher liquidity of fractioned assets put on smart contracts (noting that, although there are real opportunities to tokenise physical assets, there is not yet an appropriate value chain for that).
- Risks involve the theft of assets or intellectual property (for NFTs), as has been shown repeatedly (cf. theft of 600 million USD of tokens from the PolyNetwork[68]). Financial investors must pay particular attention to this risk and protect their digital wallets.
- Are crypto assets insurable (protection from theft or loss)?
- Regulatory status: Tokens are considered securities and therefore covered by financial regulatory frameworks.

III. Three possible scenarios for the future (2030-35)

The three possible scenarios (narratives) described in this section present three different futures, on the horizon of 2030-2035**.** They represent **how different actors could take the lead in the deployment of digital currencies and assets on a large scale, according to their mission or value systems**. They also describe how those actors could thus address, or not, some of the current challenges or risks to others. Each scenario presents specific risks and opportunities, including for long-term sustainability, and is tentatively designed to create real value and solve real challenges for real people.

- **Scenario A:** A world where **central banks** have managed to organise a coordinated response to the various demands or needs. CBDCs have become the norm and payment systems' efficiency, integrity and privacy have dramatically improved.
- **Scenario B**: A world where **private actors**, such as digital platforms, have taken the lead, created their own digital currencies, and control most payment systems worldwide. A patchwork of compelling and competing private DCs.
- **Scenario C**: A world where permissionless blockchain-based cryptocurrencies are fully established and efficient. Institutions have lost control of a considerable part of the economy. From the point of view of public institutions, it is challenging to operate in this world.

The narratives are purposely written to focus on extremes, although the reality will undoubtedly be more nuanced.

Questions for discussion about each scenario:

- Are there indications that we are moving towards the development of this scenario?
- What are the expected benefits and risks to various stakeholders?
  Who is pushing (for whom would it be desirable or beneficial)? Who is opposing?
- What would the implications be for society?
- How can regulation, incentives and other triggering factors steer or prevent the development of the scenario in an appropriate manner?

Scenario A: Central Banks take the lead in digital currencies

In this scenario, in 2030, central banks of like-minded countries (e.g. G7, OECD) have been able to continue to apply established principles of monetary systems and policy (with three roles of money as a measure of unit, a medium of exchange and a store of value) in a new system that progressively replaces cash by retail CBDCs, offers a competitive alternative to private digital/cryptocurrencies, and improves financial inclusion. Operators of private CCs could not solve the challenges associated with early-stage CCs.

Central banks provide a credible and viable public anchor for digital money. In the now well-established financial digital world, the monetary system continues to work in the public interest and central banks fully endorse and implement their responsibility to ensure financial stability by means of their monetary policies.

Technically, advanced technologies are being used to design retail CBDCs that meet all socially desirable goals on security, integrity, and privacy, and are adapted to political and legal cultures. Domestic and international payment systems are cheap, efficient and interoperable.

Central banks have been able to compete and co-exist with the new private actors often associated with large internet technology companies or networks that previously offered private money but with low levels of security and privacy. They have broken the circle engaged in the early 2000s that would have led to the concentration of significant market power in payments, contributing to societal fragmentation.

Governments have found ways to regain control. They strictly and effectively regulate the creation and use of private cryptocurrencies and assets, and decentralised finance. To achieve this, governments and central banks have thoroughly analysed users' needs: they have integrated the outcome of research on needs and values that the CBDC must support and have collaborated with traditional retail financial sector players and societal actors in general. The system's scale and network economies incentivise all major actors to use the new system.

In this scenario, Bitcoin, Ethereum and other CCs have lost so much of their appeal that they have almost completely disappeared, first because CBDCs offer levels of anonymity and confidentiality similar to cash yet more convenient than cash, second because users have been too hard ly hit by volatility, instability and security issues, third because concerns about energy consumption and electronic wastes have finally made the point that many of these CCs were not acceptable on a large scale, and fourth because retail CBDCs are better designed for ethics and social welfare.

In sum, central banks have listened to actual needs and responded effectively to socio-economic challenges, in collaboration with the traditional private sector.

The pace of CBDC developments varies according to regional cultures and the institutional strength of the governments. A remaining challenge is to extend the CBDC system adopted by these countries to other countries, particularly emerging economies. This will be important to avoid freeriding and illicit actors from migrating to these countries, and to enhance financial inclusion in developing countries.

Indications that this scenario is underway:

- At least 100 central banks are working on plans or are considering CBDCs
- Governments are stepping up efforts to regulate digital currencies
- See reports and statements from the European Central Bank (ECB)[69] and the Bank of International Settlements (BIS), among others.

Scenario B: The private sector takes the lead with private digital currencies

In this scenario, in 2030, large digital platforms of the internet economy, like Meta or Amazon, other businesses and perhaps some large international banks of the traditional financial system, have eventually succeeded in creating efficient currency(ies) and associated payment systems that people like and use. They have successfully convinced a majority of users (businesses and end-consumers) to adopt their digital currency(ies) instead of fiat currencies and payment systems of archaic and inefficient banks. The main reasons are (a) for customers: convenience, cost-efficiency and trust (high social acceptance and adoption) and (b) for companies: the ability to tokenise assets and the provision of support to specific underlying utility or value-added service.

Users trust these private actors (platforms or others) to control the system effectively and manage it cost-efficiently. Internal (private) regulations are clear and well-understood. Users are willing to compromise their loss of freedom and data privacy and ownership against efficiency gains and low transaction costs. Only a few transactions involving governments and their institutions or linked to public regulation requirements (such as taxation) are still made in fiat money. However, fiat money is still used for interoperability and convertibility.

Benefits that companies find through creating their own DC have resulted from a thorough assessment of what they wanted to achieve with it and include: tokenisation (through which they can raise capital for further product development), the ability to engage with and offer loyalty rewards to members of their community and, overall, the opportunity to increase their project's brand value and attractiveness to digital investors.

The world in this scenario is thus increasingly shaped by private money issuers with solid expertise and control of technological infrastructures and profitable business models. This has led to vertical integration and the concentration of significant market power in payments.

Ultimately, this scenario might result in a fragmented monetary system and jeopardise universal access to public money. As a result, governments are weakened, but like in scenario C, the development of this scenario is primarily due to their inability to adapt quickly enough to societal demand. In the past, central banks prioritized attention to the supply side, and they had lost contact with users' needs.

At first sight, the system does not allow much control by governments and fiscal authorities. However, governments or their central banks may find renewed legitimacy by collaborating closely with platforms. Indeed, platforms themselves need a clear regulatory framework, partly because they compete with each other (or as long as several large digital platforms can compete with each other).

Indications that this scenario is underway:
Recent statements from or about digital platforms or other private companies. For example:

- Amazon: in the past few years, "has confirmed the existence of its DC project…"; "is investigating creating its own native token…"; however, "It seems that this project has gone quiet for now…".[70]
- Meta Financial Technologies: "Meta Platforms is readying plans to introduce virtual tokens and cryptocurrencies to its family of apps with an aim to use such virtual tokens for rewarding creators and lending and other financial services"[71]…. "The digital currency likely isn't a cryptocurrency."[72]
- In December 2021, Walmart filed several trademark applications, including one for "providing a digital currency and a digital token of value for use by members on an online community via a global computer network"[73].

Scenario C: Web3 cryptocurrency world

In this scenario, in 2030, Web3 has made a significant breakthrough, and a permissionless DLT-based global cryptocurrency (or set of interoperable cryptocurrencies) is fully established as the most used currency for transfers and payments, at least internationally. Traditional institutions like central banks and commercial banks, whose legitimacy was established by laws and regulations, have lost control of the monetary systems in many economies.

In this scenario, blockchain-based systems have made huge improvements. Most concerns raised by the large-scale implementation of Web3 have been overcome, either by implementing technical solutions (such as proof-of-stake to enable scalability) or by increasing societal acceptance of the limitations. Other concerns around speculation, volatility and other risks have also been addressed or are accepted (risk tolerance has increased). As a result, web3-CCs now fulfil many expectations from users (B2B, B2C and C2C).

Digital assets of various types have also dramatically increased in transactions and value, becoming a preferred class of assets for many investors, including institutional investors.

Traditional businesses and organisations are now not only taking payments in CC, but also fully interacting with the Web3 world. For example, they have virtual storefronts and issue NFTs.

Central banks and governments have failed to meet the demand for modernising the currency and payment systems. They can only blame their lack of responsiveness and efficacy in developing solutions that could have met the needs. Furthermore, a lack of global coordination, partly caused by geopolitical tensions and conflicts, has led many countries to focus on strengthening their sovereignty at home rather than developing international collaboration toward more efficient international monetary policies and payment systems. Traditional regulators are failing, compliance with outdated rules is low, and enforcement is inefficient.

The advent of this scenario has breached a robust paradigm in human history: that individuals are more comfortable with some level of control over themselves than if they are entirely left free. Scenario C plays with how far it is possible to go without control from a central authority, or oversight of DeFi activities in a way that complies with regulations (e.g. AML, CTF, KYC). Society has found ways to deal with current DeFi challenges (including resilience, robustness to cyber-attacks and absence of formal governance rules) without restoring central control and oversight.

Indications that this scenario is underway:

- There is a demand for CC and crypto assets: In 2021, all CCs combined accounted for about 7% of the world's money[74]. DeFi transaction volume surged. Assets stored in DeFi applications rose from under $1bn at the start of 2020 to more than $200bn in early 2022.) Some companies accept CCs for payment.
- Some countries adopt CC as legal tenders[75] (albeit not very successfully).
- PayPal is "excited about the future of Web3 as the next iteration of payment […] paying through Web3 will become as commonplace as online payments or tap-and-go."[76]
- Google indicated (January 2022) that "we are definitely looking at blockchain. It's such an interesting and powerful technology with broad applications."

Note: Traditional economists and political scientists are uncomfortable with this scenario, which contradicts many principles and past history of control and authority as fundamental and exercised through conventional means. Discussion of this scenario forces unconventional thinking, perhaps of the type that the French Army is adopting with the Red Team Defense (In English) to provide context to training armies for the future.

IV. Motivations and implications of specific types of DCs for distinct actors

This section suggests that understanding the possible future of DC requires carefully considering the specific **motivations** of distinct actors for specific types of DCs. Motivations depend on the **implications** of adopting these various forms of DC and related **trade-offs**. Actors can[77]:
- design DCs (e.g. technology developers)
- deploy a DC (e.g. central banks, DeFi, private actors)
- adopt or use (freely or forcedly) specific DCs (e.g. consumers, businesses, commercial banks)
- regulate DCs

Here are some questions for conversation with distinct stakeholder groups:

Motivations
Causes and drivers of digital currency developments
(from research to implementation)

- What socio-economic needs and challenges could each type of DC (cf section II) address?
  For example: which types of DC are optimised for financial inclusion? Or for privacy?
- While certain DC developments can be prompted or triggered by certain actors, others may not be interested in them, or may even oppose their deployment. Which specific forms of DC are encouraged (preferred, supported, incentivised) by certain actors, or discouraged by others (in the sense that those oppose their development), and why?
  For example:
  - Very few governments and businesses accept payments in bitcoin.
  - Investors are interested in portfolio diversification but concerned about the risk of volatility and instability.
  - Businesses need currencies and payment systems that are secure, performant and that present efficiency gains in terms of transaction costs and simplicity along the supply chain. Lack of or insufficient regulation adds uncertainty and is a barrier to adoption.

Implications
Consequences of developing and adopting digital currencies and related changes in financial markets and payment system infrastructures.

- Specific types of DCs will have specific implications for distinct actors. Who will be impacted most?
  For example:
  - The effectiveness of governments and central banks' policies could be eroded if financial transactions increasingly use unregulated private cryptocurrencies
  - Commercial banks will see their role evolve with retail CBDCs
  - Citizens' rights might be threatened if retail CBDC do not guarantee their privacy and confidentiality
- What shifts in global society could come with them?

Trade-offs
Governing and balancing opportunities and risks

- What trade-offs need to be addressed? (Noting the variety of opinions regarding risks and opportunities)
  For example: privacy vs national security and AML/CTF compliance; or safeguarding user identity vs safeguarding data

- What are the current and possible technical measures[78] to resolve trade-offs (benefit-risk and risk-risk), for example, with privacy-enabling techniques?
- How to address the challenges and risks with broader risk management and response strategies: private regulation (norms, standards, …) and public regulation[79]
- What are the current mechanisms for developing collaborative partnerships between the private and the public sectors?
- What are the perspectives in terms of international governance or regulatory mechanisms?
  See Box 2 on metrics and standardisation, and Box 3 on regulation.
- Do you see that the development of Web3 will be relevant to address some trade-offs?
  See Box 5 – Moving from Web 1 to Web3

V. Issues for distinct actors

Public sector

1. Governments and regulators

- *To what extent can they combat those forms of DC that they regard as undesirable to their public and monetary policy mission and goal?*
- *What combination of public and private regulation and incentives could work best?*
- *What supporting conditions for CBDCs meet the general public, monetary and financial policy goals and financial inclusion?*

2. Central banks

- *To what extent is there a need to replace cash with a CBDC?*
  Could modern payment systems like Pix in Brazil[80], UPI in India, or Twint in Switzerland do the job?
- *A CBDC will be only as strong and credible as the central bank that issues it.*
  So, how can a central bank be strong enough to achieve its mission with a CBDC?
- *How can central banks resist the competition from new private actors?*

3. The financial sector (traditional financial institutions)

- *What is the position of the traditional financial sector concerning specific types of DCs?*
- *How can it benefit from CCs? How can it oppose or adapt?*
- *How can investors make sense of the constantly changing landscape of cryptocurrencies, and the very few reliable measures of value?*

Private sector

4. Decentralised finance (DeFi)

- *What is the DeFi business model?*
- *From the point of view of DeFi companies, what regulation is desirable?*
- *How to work in collaboration with traditional finance (institutional public and private sector), perhaps in CeFi?*

5. Digital platforms

- *What are the reasons why platforms would want to have their own currency?*
- *What are the necessary conditions for a digital platform currency and payment system to succeed?*

6. Businesses and investors (non-financial private sector companies, including **insurance**)

- *What is their position concerning specific types of DCs?*
- *Are crypto assets such as NFTs insurable?*
- *How can they benefit from DCs? Investing in crypto assets for portfolio diversification?*
- *How can they oppose or adapt?*

Others

7. Illicit economy

- *What are the motivations of actors of the illicit economy for using cryptocurrencies?*
- *To what extent could institutional actors have an impact on them through regulation?*
- *How do we expect the illicit economy to respond to CBDCs?*

8. Informal (and collaborative, sharing) economy

- *What are their needs and constraints?*
- *To what extent could institutional actors develop a DC that they would use?*

9. Thinkers, libertarians and iconoclasts

- *They inspire and influence others. Who are they?*
- *What role do they have in suggesting certain DC features that others will find desirable?*
- *Does financial inclusion require a CBDC?*
- *How to mitigate risks that end-users, such as the youth or uneducated, incur when they use or invest in CC?*

VI. A risk governance perspective on digital currency?

This section presents some principles and guidelines for risk governance that are particularly relevant when addressing the risk of cryptocurrencies or assets. They are drawn from the *Introduction to the IRGC Risk Governance Framework* (a summary of *Risk governance: Towards an integrative approach*, Ortwin Renn, 2005), *Guidelines for the Governance of Emerging Risks* and *Guidelines for the Governance of Systemic Risk*.

Risk

Risk results from uncertainty about the consequences of an activity or an event concerning something valuable to the economy, society or individuals.[1] Risks include two components: the likelihood and the severity of potential consequences. Uncertainty can pertain to the cause (hazard), the exposure and vulnerability of those affected, the type, likelihood and severity of the consequences, or the time or location where and when these consequences may occur. In many domains, risk management starts with safety and security management and expands into resilience building.

Emerging risk

Conventional risks are characterised by a well-known probability distribution over a limited scope of adverse effects. In contrast, the concept of emerging risk refers to new risks or known risks that develop in new context conditions. Management of emerging risks requires engaging in foresight activities and involves a range of strategic options such as adopting precautionary measures (do not engage), reducing exposure and including robustness and resilience.
Risks related to new forms of currencies and payment systems are emerging.

Systemic risk

The concept of *systemic risk* refers to the risk or probability of breakdowns in an entire system because of high levels of connectivity, significant uncertainties and ambiguities, and non-linear cause-effect relationships. Systemic risks are embedded in the larger context of societal, financial and economic change. Such risks cannot be managed through the actions of a single sector but require the involvement of different stakeholders, including governments, industry, academia and

[1] ISO 31000 (International Organization for Standardization, 2018) defines risk as the "effect of uncertainty on objectives" and an effect is a positive or negative deviation from what is expected.

members of civil society.
Risks related to new forms of currencies and payment systems are systemic.

Governance
In its broader sense, *governance* refers to the actions, processes, traditions and institutions by which authority is exercised, and collective decisions are taken and implemented. It involves public actors (governments and governmental organisations, national, regional and international) and private actors. Consequently, there is a range of various forms of governance, including public and private regulation.

Risk governance
Risk governance applies governance principles to identifying, assessing, managing, evaluating, and communicating risks in the context of diverse values and distributed authority. The process must include all important *actors* involved. It must also be *interdisciplinary* to generate comprehensive and accurate technical and governance knowledge for risk assessment and appropriate options for risk management.

The governance of risks related to digital currencies involves technology designs, policy choices, and behavioural norms. Thus, we need both governance that is instrumented *by/with* technology, and governance *of* technology to set specific requirements deemed desirable, acceptable and legitimate to drive change in monetary policies and payment practices.

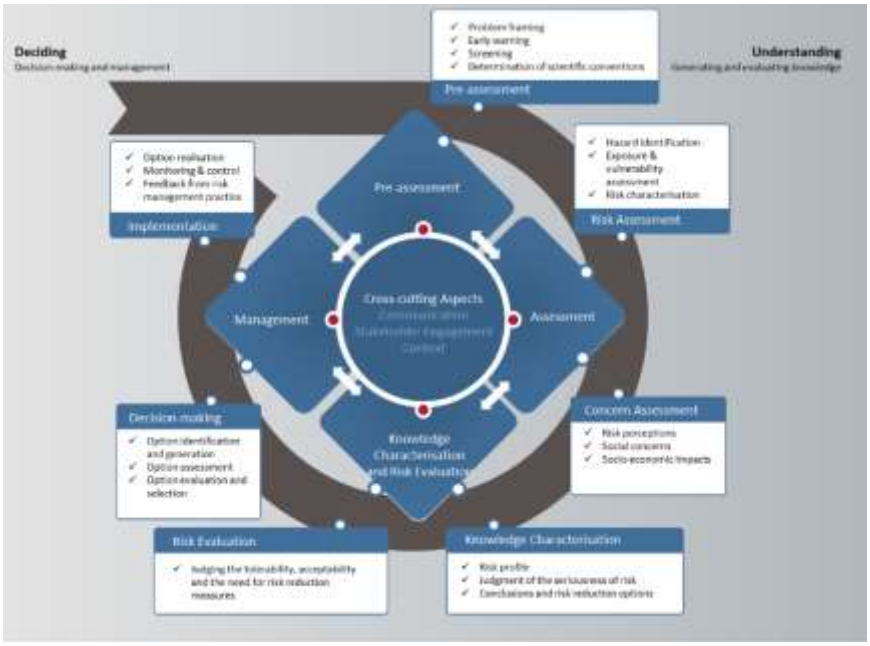


Figure 3 - IRGC risk governance framework

Risk assessment
Risk assessment in the context of comprehensive (multi-stakeholder and multidisciplinary) risk governance includes both:

- An assessment of the risk's factual and measurable characteristics, which aims to identify and describe the possibility of occurrence or a probability distribution over a range of negative consequences, considering the hazard as well as the exposure and vulne rability of the assets that must be protected;
- An assessment of different stakeholders' opinions, perceptions, concerns and attitudes about the risk, a systematic analysis of the associations and perceived consequences (benefits and risks) that stakeholders may associate with a hazard, its cause(s) and consequence(s).

Involving stakeholders in assessing risks related to digital currencies is fundamental to ensuring the relevance and acceptability of the measures taken to address the various risks, for effective adoption or implementation. Stakeholders include those who create the risks, those impacted by them (exposed and vulnerable) and those who manage or regulate them. In the absence of a complete understanding of the technical features and issues at stake, there are significant variations in both the technical assessment of the risk and the assessment of concerns, perceptions and opinions, which leads to uncertainty and, primarily, ambiguity about what should be regulated and how.

Risk evaluation

Risk evaluation is the process of comparing the outcome of the risk assessment with specific criteria to determine the significance and acceptability of the risk and to prepare decisions. To be effective, risk management requires not only an assessment of the scientific evidence about a risk but also a careful judgement of whether or not the risk is acceptable to decision-makers and stakeholders. If it is not acceptable, risk reduction measures may make it more tolerable. To make this judgement, the evidence on the risk and the concern assessment must be combined with a thorough evaluation of other factors such as economic interests and priorities, societal preferences and political considerations. Risk evaluation thus results in a strategic decision that informs risk management. Overall, decision-makers balance various expected benefits and various risks.

In the case of digital currencies and assets, and their various types, the evaluation of their benefits and risks currently depends heavily on specific private interests, which public authorities must balance with public interests. The field is complex, and many uncertainties may persist. Above all, the many different and sometimes conflicting interests, views and perspectives about opportunities and challenges create a decision space where public policy design and related technical choices cannot be straightforward.

The development of digital currencies in various forms involves numerous trade-offs between risks or priorities, in the sense that technical designs or risk management interventions to reduce one risk can increase other risks or shift risk to others. A recurrent example is between efficiency, convenience or scalability on the one hand, and privacy or security on the other.

Risk management options

Risk management is a process that involves the design and implementation of the actions and remedies required to avoid, reduce (prevent, adapt, mitigate), transfer or retain the risks. This includes the generation, assessment, evaluation and selection of appropriate management options, the decision about a specific strategy and options, and implementation.

Effective management of issues marked by uncertainty and ambiguity requires the involvement of both the stakeholders creating the risks and those adversely affected by the risk.

Robustness increases the resistance of the system at risk under normal circumstances. Resilience is a strategy to help systems and populations cope with uncertain but potentially severe risks that cause large-scale shocks and accidents. Building resilience includes a suite of approaches to understand the risk, prepare in advance for when it hits, rebound after the shock and recover critical systems functions. In contrast to robustness, where potential threats are known in advance and the system can be prepared to face these threats, resilience is a protective strategy against unknown or highly uncertain hazards.

Risk management strategies for digital currencies and cryptoassets can target the risk at the *source* by, e.g. prohibiting certain types of cryptocurrencies or assets, strictly regulating their trading and imposing specific information for users and investors. They can also target the *impact and consequences* of the risk by developing strategies for *robustness* and *resilience*, by, e.g. reducing exposure and vulnerability to the risk of specific users who lack sufficient capital reserve or financial education.

Planned adaptive regulation

Planned adaptive regulation (PAR) is an approach in which a regulation is designed from its inception to be revised over time based on experience. PAR requires: (i) planning for future review and revision of the governance arrangements, (ii) funding of targeted research, (iii) monitoring of performance and impact of existing arrangements, (iv) review and revision, (v) a vision of what the goal of adaptability is, (vi) the ability to respond to rapid changes, and (vii) trustworthiness between the actors who want to adapt the rules.

In technology domains that evolve quickly (e.g. pharmaceuticals), regulations are increasingly organised along the principles of PAR. In finance, the Swiss 'debt brake' system is an example. PAR is generally suitable when fast-moving technology development makes it impossible to fix into law specific requirements that may become obsolete if the subject of the regulation changes quickly. PAR is principle- and performance-based, i.e., it is flexible and adapts to reach a pre-agreed objective, such as financial stability. Regulatory requirements are regularly revised according to progress made towards meeting the objective.

Risk communication

Risk communication is the process of exchanging or sharing risk-related data, information and knowledge between and among different groups. It enables risk assessors and managers to develop a shared understanding of their tasks and responsibilities. In addition, it empowers stakeholders and civil society to understand the risk and the rationale for risk management. Appropriate communication about the risk is a critical success factor for an effective risk management outcome. Communication creates awareness and, together with consultation, contributes to knowledge-sharing about the issue, committing stakeholders to the management process and eventually building trust.

In the financial sector, asymmetric information is a significant source of risks to consumers, which requires better consumer protection, communication and education.

Endnotes and references

[1] cf description of CeFi in contrast to DeFi and traditional finance in CoinDesk 15 August 2022. DeFi vs. CeFi in Crypto

[2] BIS, Annual Economic Report, 21 June 2022, chapter "III. The Future Monetary System."

[3] Updates available on https://www.coingecko.com/en/global-charts

[4] Financial Times, "Cryptocurrencies Are Not the New Monetary System We Need"

[5] About value creation and tokenisation, see a report from Ripple: "New Value: Crypto Trends in Business and Beyond", 2022

[6] "*We reaffirm that any CBDC should be grounded in our long-standing public commitments to transparency, the rule of law and sound economic governance. Any CBDC must support, and 'do no harm' to, the ability of central banks to fulfil their mandates for monetary and financial stability. We emphasise the importance of rigorous standards of privacy, accountability for the protection of users' data, and transparency on how information will be secured and used, to command trust and confidence by users. Any CBDC ecosystem must be secure and resilient to cyber, fraud and other operational risks, must address illicit finance concerns and be energy efficient. CBDCs must operate in an open, transparent and competitive environment that promotes choice, inclusivity and diversity in payment options. We note the importance of considering interoperability on a cross-border basis given the potential role for CBDCs in enhancing cross-border payments. At the same time, we recognise a shared responsibility to minimise harmful spillovers to the international monetary and financial system.*" 14 October 2021, "G7 Public Policy Principles for Retail Central Bank Digital Currencies, and G7 Finance Ministers and Central Bank Governors' Statement on Central Bank Digital Currencies and Digital Payments."

[7] International Telecommunication Union (ITU), May 2022, "Report of the Financial Inclusion Workstream." See also the The World Bank, "Financial Inclusion Global Initiative (FIGI)."(accessed 20/9/2022) and BIS, 14 April 2022,"CBDCs in Emerging Market Economies."

[8] Atlantic Council, « Missing key – the challenge of cybersecurity and CBDC", June 2022

[9] See calculation of the Bitcoin network power demand developed by the University of Cambridge, "Cambridge Bitcoin Electricity Consumption Index (CBECI)." as per 20 September 2022. For comparing with countries' consumption, see Wikipedia, "List of Countries by Electricity Consumption." In August 2021, the average carbon intensity of each bitcoin transaction was 1.42 tones of CO2, compared to 0.1 gram for a Visa transaction.

[10] See Ethereum, "The Merge" update 15 September 2022
Commentaries: Vergolina, "Anticipating the Coming Ethereum Merge."; and Castor, "Why Ethereum Is Switching to Proof of Stake and How It Will Work."

[11] Queen Maxima of The Netherlands, at the World Economic Forum 2021 annual meeting. See White et al., "Key Takeaways on Digital Currency from The Davos Agenda."

[12] Referring to privacy, Grothoff and Moser, in "How to Issue a Privacy-Preserving Central Bank Digital Currency, SUERF Policy Brief" cite a survey conducted in 2021 by the European Central Bank which has found that "both citizens and professionals consider privacy the most important feature of a digital Euro"; that "citizens consistently place a high value on privacy", but "choose convenience, speed, and financial savings over privacy [which] may be due to the fact that they are not fully aware of the extent to which technological advances have improved the ability to track, aggregate, and disseminate personal information".
For details regarding the survey, see European Central Bank, April 2021, "Eurosystem Report on the Public Consultation on a Digital Euro."

[13] About privacy: see "policy and regulatory considerations relevant to privacy technology choices" in World Economic Forum, November 2021, "Privacy and Confidentiality Options for Central Bank Digital Currency."

[14] In the context of information security, security is defined as: confidentiality (the information system does not leak information to those who should not have access to it); integrity (the system should store information correctly and produce correct results to computations, allowing neither to be tampered with maliciously for example); and availability (the system should respond to users promptly when requested to retrieve data or perform some action, such as committing a digital currency transaction). All can be provided by techniques for distribution and decentralization, fundamental to cryptocurrencies and CBDCs. Allen et al., Brookings Institution, July 2020, "Design Choices for Central Bank Digital Currency."

[15] "G7 Public Policy Principles for Retail Central Bank Digital Currencies and G7 Finance Ministers and Central Bank Governors' Statement on Central Bank Digital Currencies and Digital Payments."

[16] See for example the "Digital Currency Global Initiative.", a collaboration of the ITU and Stanford University.

[17] cf OECD Blockchain Policy Forum, September 2022

[18] International Telecommunication Union (ITU) and Stanford University, "Digital Currency Global Initiative. A Collaboration between International Telecommunication Union (ITU) and Stanford University."
[19] Stanford University, "Future of Digital Currency Initiative."
[20] UK Finance "Adopting the principle of "Same Activity, Same Risk, Same Regulation" into the UK's regulatory framework" accessed on 20 September 2022.
[21] Federal Act and Ordinance available from State Secretariat for International Finance (SIF), accessed on 20 September 2022.
[22] See European Council's press release, 30 June 2022, "Digital Finance: Agreement Reached on European Crypto-Assets Regulation (MiCA)."
and Sygna, "MiCA (Updated July 2022): A Guide to the EU's Proposed Markets in Crypto-Assets Regulation."
[23] The White House, 9 March 2022 "Executive Order on Ensuring Responsible Development of Digital Assets."
Summary and analysis by Dechert LLP, 5 April 2022, "Biden Executive Order on Ensuring Responsible Development of Digital Assets."
[24] The White House, 17 September 2022, "Comprehensive Framework for Responsible Development of Digital Assets"
Commentary on the World Economic Forum blog, 27 September 2022 "what we can learn about the future of digital assets regulation from recent US government reports"
[25] Illicit economy: production and distribution of prohibited goods and services, such as organised crime (drug production, trafficking and distribution, arms trafficking and prostitution,…). See the Global Initiative Against Transnational Organized Crime, 11 March 2021, "The Global Illicit Economy: Trajectories of Transnational Organized Crime."
[26] Informal or grey economy: legal economic activity that is unrecorded and unregulated, neither taxed nor generally monitored by governments. See International Monetary Fund (IMF), 28 July 2021, "Five Things to Know about the Informal Economy."
[27] Global Initiative against Transnational Organized Crime, 11 March 2021, "The Global Illicit Economy: Trajectories of Transnational Organized Crime."
[28] Global Initiative against Transnational Organiszed Crime, June 2022, "Crypto, crime and control – cryptocurrencies as an enabler of organized crime"
[29] Chainalysis Team, "DeFi Takes on Bigger Role in Money Laundering But Small Group of Centralized Services Still Dominate."
[30] Chainalysis, "Cryptocurrency Crime trends for 2022", 6 January 2022
[31] See Allen et al., Brookings Institution, July 2020 "Design Choices for Central Bank Digital Currency"
see also: Chaum, Grothoff and Moser, March 2021 « How to Issue a Central Bank Digital Currency », Swiss National Bank Working Papers,
and GNU Taler payment system, that can be used for CBDCs
[32] As seen for example with experiences in Salvador, or with young uneducated people who invest in bitcoins.
[33] Interview with Kristalina Georgieva, IMF Managing Director, 9 February 2022, "The Future of Money."
Full paper: Soderberg et al., IMF, 9 February 2022, "Behind the Scenes of Central Bank Digital Currency: Emerging Trends, Insights, and Policy Lessons.":
[34] BIS, 2020, "Central Bank Digital Currencies: Foundational Principles and Core Features. Report"; and, Executive Paper.
[35] Example: Swiss Federal Act on the Adaptation of Federal Law to Developments in Distributed Electronic Register Technology, adopted on 25 September 2020, came into force on 1 August 2021. See: State Secretariat for International Finance (SIF), "Blockchain / DLT."
[36] See "Digital Finance: Agreement Reached on European Crypto-Assets Regulation (MiCA)." following the Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937.
[37] Andrea Catalini and Scott Kominers, "Can Web3 bring back competition to Digital Platforms?"in TechREG Chronicle, February 2022
[38] CoinDesk 15 August 2022. DeFi vs. CeFi in Crypto
[39] BIS Annual Economic Report 2022, Chapter III. The future monetary system
[40] Cf Interview with Jeff John Robbers, Harvard Business Review, 10 May 2022, "Web3 Will Run on Cryptocurrency."
and Ethereum, "What Is Web3 and Why Is It Important?" accessed 20 September 2022
[41] For example, see Stephen Diehl's blog, accessed 20 September 2022
[42] Concerning 'crypto', see a New York Times article of 30 September 2022 and Ezra Klein Show with Vitalik Buterin (Ethereum): *"Over the last decade, Buterin has become arguably the core public intellectual on the*

nonfinancial side of crypto. His new book, "Proof of Stake," is a collection of long, thoughtful essays that, taken together, lay out a vision of crypto as a truly transformative technology — one with the potential to revolutionize everything from city governance to voting systems to online identity."

[43] Financial Stability Board (FSB), 13 October 2020, "Regulation, Supervision and Oversight of 'Global Stablecoin' Arrangements."

[44] Stablecoins maintain a stable value via protocols that provide for the increase or decrease of the supply of the stablecoins in response to changes in demand. Global stablecoin: a stablecoin with a potential reach and adoption across multiple jurisdictions and the potential to achieve substantial volume, thus posing financial stability risks.

[45] Federal Reserve, "What Is a Central Bank Digital Currency?" accessed 20 September 2022

[46] European Central Bank (ECB), 2020, "Report on a digital euro".

[47] For a definition of privacy, efficiency and integrity/security concepts, see World Economic Forum, "Privacy and Confidentiality Options for Central Bank Digital Currency."

[48] Table include in The World Economic Forum, 19 November 2021 "Digital Currency Governance Consortium White Paper Series."

[49] Buy Bitcoin Worldwide, "How Many People Own, Hold & Use Bitcoins?" accessed 20 September 2022

[50] Established by Satoschi Nakamoto.

[51] Approximately 19 million BTC mined until June 2922, on a technical maximum of 21 million, which would be reached in 2078 as the speed of production decreases by design.

[52] Cf Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System.". Outline of a decentralized peer-to-peer protocol that was cryptographically secure.

[53] The 'Blockchain Trilemma' is described by Vitalik Buterin, as *"the challenges developers face in creating a blockchain that is scalable, decentralized and secure — without compromising on any facet. Blockchains are often forced to make trade-offs that prevent them from achieving all 3 aspects:*
- Decentralized: creating a blockchain system that does not rely on a central point of control.
- Scalable: the ability for a blockchain system to handle an increasingly growing amount of transactions
- Secure: the ability of the blockchain system to operate as expected, defend itself from attacks, bugs, and other unforeseen issues", CertiK, "The Blockchain Trilemma." *accessed 20 September 2022*
Further information in Ledger Academy, 6 September 2022, "What Is the Blockchain Trilemma?":
"- Scalability and decentralization are often held back by security, but security tends to be compromised by any shifts on a network that offer scalability.
- Projects either choose to focus on two out of three or work on finding a solution to tackle the trilemma once and for all. Innovative ideas like sharding, side-chains and state channels are used to address the trilemma but they're still experimental.
- A solution to the problem could lead to greater adoption of cryptocurrency and blockchain and a wide-spread use of the technology across industries."

[54] For example: "Letter in Support of Responsible Fintech Policy" by 1500 computer scientists, software engineers, and technologists, 1 June 2022

[55] see for example speakers at the 5-6 September 2022 Crypto Policy Symposium

[56] Financial Times, "Digital Assets Dashboard", accessed 20 September 2022

[57] Remind though that there is no universal definition of 'blockchain'.

[58] Proof-of- stake replaces miners by validators. Cf. Castor, MIT Technology Review, 4 March 2022, "Why Ethereum Is Switching to Proof of Stake and How It Will Work."
Proof-of-stake could also raise issues of unwanted centralisation and trust in the selection of validators, and there are concerns about whether the Ethereum network will be as censorship-resistant as the current rendition, i.e. about potential for validators that will compile transactions into blocks on the upgraded blockchain to omit certain transactions from inclusion into blocks recorded on the chain under government pressure. See Kharif, Bloomberg, 18 August 2022,"Ethereum Developers Back Sept. 15 Target for Blockchain Software 'Merge.'" and Vergolina, Bloomberg, 30 August 2022 "Anticipating the Coming Ethereum Merge."

[59] For example, Fabio Panetta (ECB) on 25 April 2022 in "For a Few Cryptos More: The Wild West of Crypto Finance."declares that "at present crypto-assets are not only speculative and high-risk investments, but they also raise public policy and financial stability concerns".

[60] Kessler, CoinDesk, 15 September 2022, "The Ethereum Merge Is Done, Opening a New Era for the Second-Biggest Blockchain", accessed on 16 September

[61] See World Economic Forum, 19 November 2021, "Digital Currency Governance Consortium White Paper Series."

[62] FSB, 13 October 2020, "High level recommendations for regulation, supervision and oversight of 'global stablecoins' arrangements"
[63] Cf early analysis by Kaloudis, CoinDesk, 15 May 2022, "The Collapse of UST and LUNA Was Devastating, but There Is Still Hope for Crypto." and Weisenthal, Bloomberg, 15 May 2022, "Meet the Hedge-Fund Manager Who Warned of Terra's $60 Billion Implosion."
[64] BIS, 2020, "Central Bank Digital Currencies: Foundational Principles and Core Features. Report"
For latest information about CBDCs launched, pilot, proof of concept or research, see CBDC tracker on https://cbdctracker.org/
[65] See Grothoff and Moser, SUERF Policy Brief, June 2021, "How to Issue a Privacy-Preserving Central Bank Digital Currency"
[66] Summer and Hermanky, Central Bank of Austria, June 2022, "A Digital Euro and the Future of Cash."
[67] Italian Wine Crypto Bank, "Homepage."
[68] Locke, "'Investors Must Be Vigilant and Cautious' Following the Massive $600 Million DeFi Hack, Experts Say."
[69] European Central Bank (ECB). See lectures by Fabio Panetta, Member of the Executive Board: "The Present and Future of Money in the Digital Age." (10 December 2021), "Public Money for the Digital Era."(15 May 2022) and "The Digital Euro and the Evolution of the Financial System." (15 June 2022).
[70] Parkin, 26 July 2021 "Amazon Lining up Bitcoin Payments and Token, Confirms Insider."
[71] Dorsey, Business Standard, 8 April 2022, "Meta targets finance with 'Zuch Bucks', creator coins: Report"
[72] Peters, The Verge, 7 April 2022, « Meta is reportedly making a 'Zuck Buch'"
[73] Thomas, CNBC, 16 January 2022 "Walmart Is Quietly Preparing to Enter the Metaverse."
[74] Reif, Investopedia, 26 November 2021 "How Much of All Money Is in Bitcoin?"
[75] Mason, Investment Week, 5 January 2022 "Bitcoin to become legal tender in three more countries this year"
[76] The Sydney Morning Herald, 2 September 2022, "Distressing: PayPal backs crypto, but worries about bad actors"
[77] For a discussion of roles of stakeholders and what shapes their interest in a digital euro, see CEPS "Seizing opportunities, mitigating risks: How can the digital euro foster a resilient and innovative future for the EU?", 2022
[78] For a high-level review of cryptographic techniques, see World Economic Forum, "Privacy and Confidentiality Options for Central Bank Digital Currency."
[79] Public regulation of private DC is needed but probably very ineffective at tackling its use by informal and illicit economy. Public regulation of stablecoins is needed and expected to be effective. Public regulation is de facto embedded into a CBDC that would have the same role as money as a unit of account, means of exchange and store of value
[80] The Economist, 14 May 2022, "Digital Payments Have Gone Viral in Brazil."

About IRGC

The EPFL International Risk Governance Center (IRGC) is an interdisciplinary unit dedicated to extending knowledge about the increasingly complex, uncertain and ambiguous risks that impact human health and safety, the environment, the economy and society at large. IRGC's mission includes developing risk governance concepts and providing risk governance policy advice to decision-makers in the private and public sectors on key emerging or neglected issues. It emphasises the role of risk governance and the need for appropriate policy and regulatory environments for new technologies where risk issues may be important.

EPFL International Risk Governance Center
EPFL IRGC Station 5, BAC
1015 Lausanne Switzerland
+41 21 693 82 90
irgc@epfl.ch
irgc.epfl.ch