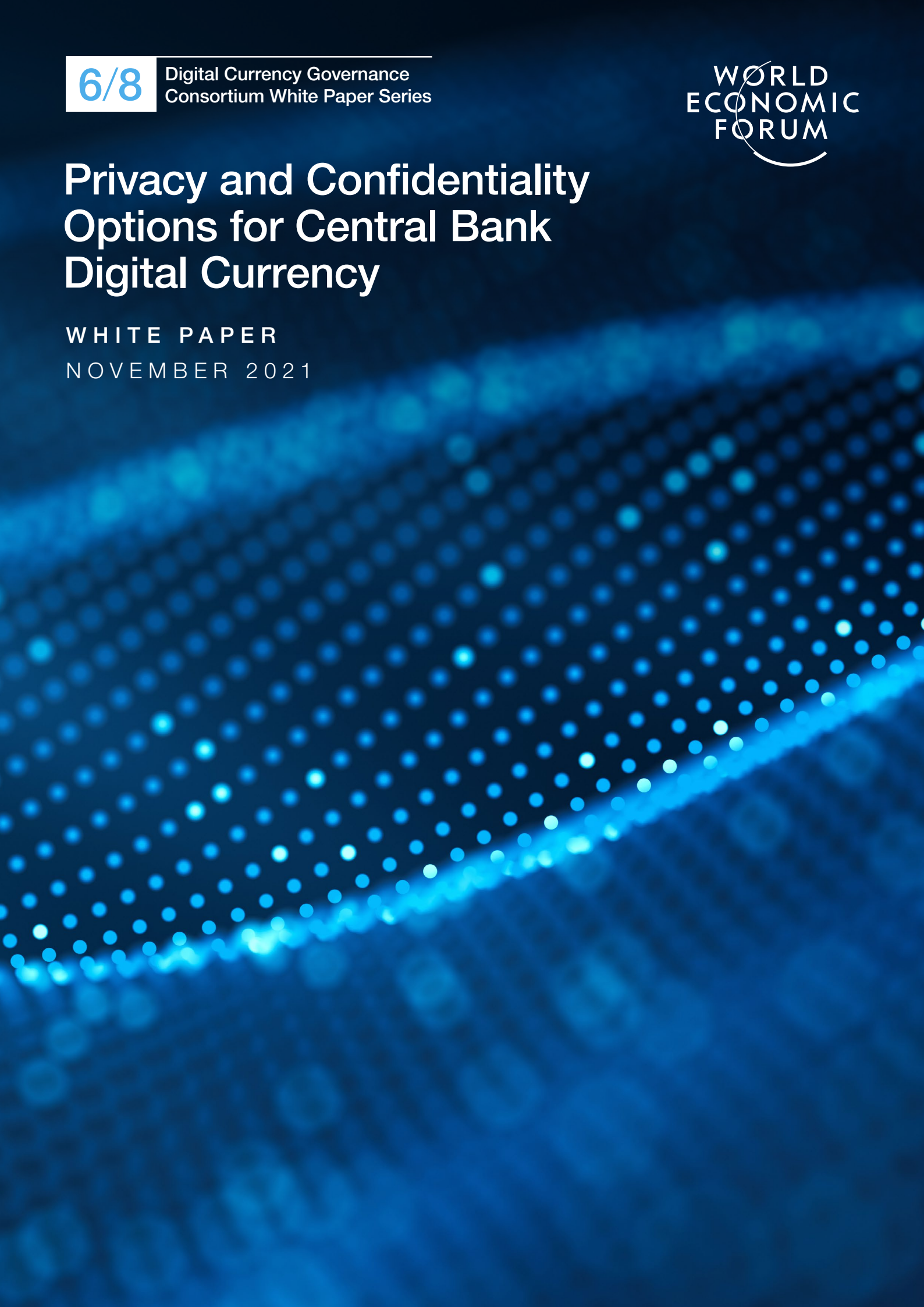
6/8 Digital Currency Governance Consortium White Paper Series

WORLD ECONOMIC FORUM

Privacy and Confidentiality Options for Central Bank Digital Currency

WHITE PAPER

NOVEMBER 2021



Images: Getty Images

Contents

This white paper is part of the Digital Currency Governance Consortium White Paper Series. Its authors, contributors and acknowledgements can be found in that compendium report.

Preface

This paper explores the spectrum of technology-based privacy and confidentiality options for designing central bank digital currency (CBDC), with a focus on cryptographic techniques. It discusses the range of technologies that central banks have available to support the implementation of CBDC and outlines the principles and policy choices that lie behind those options, without making recommendations.

As more central banks begin researching the possibilities of issuing a CBDC, there is a common concern around the impact this will have on privacy. Of the 8,200 comments received by the European Central Bank (ECB) during its consultation period on the potential for a Euro-denominated CBDC, 41% of all replies centred around privacy.[1] CBDC acceptance will therefore depend in part on users' trust in the privacy offered by CBDC. However, the notion of privacy is not consistent across the globe and privacy preferences, policies and laws vary significantly by culture and region. Privacy is not a binary choice – there is a spectrum of configurations to enable varying levels of privacy. In many jurisdictions, privacy rights need to be considered in light of the disclosure requirements of policies aimed at combatting money laundering or terrorism.

In comparing CBDC to current alternatives, physical cash is typically used as a benchmark. Physical cash is generally unrivalled in its ability to provide a high degree of privacy and anonymity to its users. This feature is not limitless, however, as many countries have transactional reporting thresholds and payees often see a payer's identity. Understanding the technology choices available may allow policy-makers to better replicate the privacy-enhancing features of cash in CBDC architecture, if desired. Privacy-enhancing techniques can be configured or designed to maximize the potential of CBDC for achieving policy goals while providing privacy.

This white paper is divided into two chapters. Chapter 1 examines the current technology options, beginning with examples of privacy architectures in use today, before setting out the requirements of a privacy-preserving financial system. This is followed by an exploration of cryptography methods and how they could be employed in CBDC.

Chapter 2 examines the current state of trust in governments and why this is relevant to privacy. Such trust is the bedrock of CBDC adoption. The chapter then highlights important policy and regulatory aspects relevant to the technology options described in Chapter 1, calling out some of the policy and regulatory challenges that policy-makers face.

This paper takes a technology-first approach, clarifying the options available to policy-makers without recommending one option over another. The guidance can be used to implement successful CBDC design that respects user privacy while reducing risk and meeting regulatory requirements.

1 Privacy technology choices

1.1 Privacy architecture examples in use today

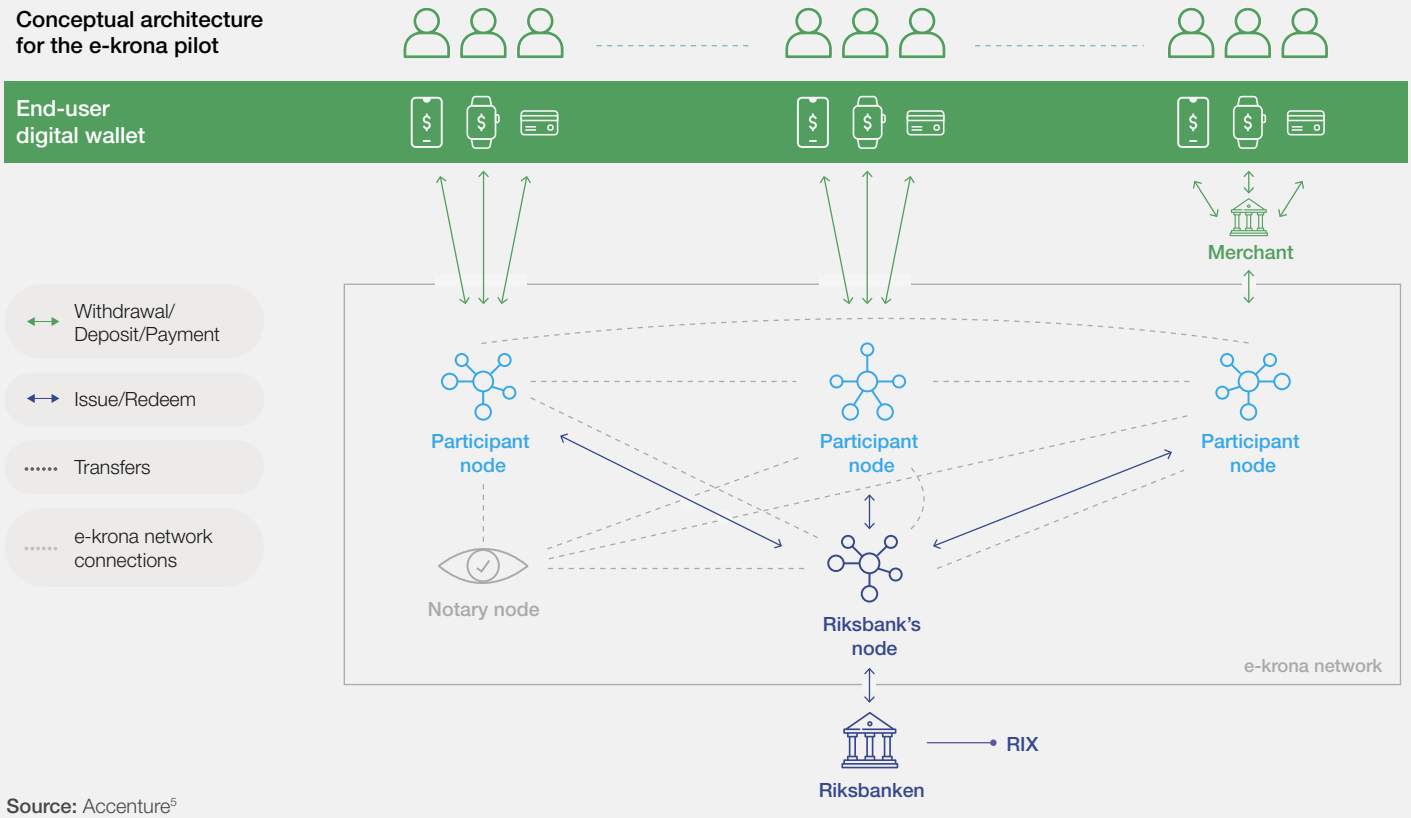
To identify the current state of privacy design in CBDC systems, it is worth mentioning privacy architectures already in use today. Below are some important examples.

The Riksbank's e-krona on Corda – "need-to-know basis"

Corda is an open-source distributed ledger project developed by R3. Currently, Corda uses a need-to-know data distribution model, which provides a degree of physical separation between transactors and the central bank or regulatory actors. Only the transactors receive the data for that transaction (i.e. the Corda nodes themselves).[2] This method provides both privacy and confidentiality (see Glossary for definitions). The e-krona pilot is a CBDC with a direct claim on the Riksbank.[3] This is a two-tiered model: in the first tier, the Riksbank will issue or redeem SEK (Swedish krona) to intermediaries in an e-krona network such as banks. In the second tier, the intermediaries will distribute SEK to end users, granting them pseudonymous identities that are used as network addresses for CBDC payments (see Figure 1).

Participants will be able to obtain or redeem SEK against the debiting or crediting of reserves held directly by the participants or via a representative in the Riksbank's real-time gross settlement funds transfer system (RTGS), known in Sweden as the RIX. Corda's network architecture, in which information is only shared to central bank and financial regulatory authorities and financial intermediaries on a need-to-know basis, allows for a level of privacy that is akin to the two-tiered model used by central banks today. To prevent double-spend in this model, notaries keep track of inputs and outputs of transactions and double-spending attempts by noting transaction IDs.[4]

FIGURE 1 **Conceptual architecture for the e-krona pilot**



Source: Accenture[5]

China's Digital Currency Electronic Payment – "controlled anonymity"

China's CBDC system, the Digital Currency Electronic Payment (DC/EP), uses a concept known as "controlled anonymity" in its current trials to ensure transactions remain confidential.[6] This method ensures that transactions remain private to those outside the system, except for the People's Bank of China (PBOC), which can trace DC/EP movements. The corresponding relationship between addresses and user identity is known to PBOC only through a KYC (Know Your Customer) process.

Commercial banks will play a key role in the issuance and redemption of DC/EP and will be responsible for implementing KYC checks. DC/EP transactions only involve DC/EP senders, DC/EP receivers and the PBOC. Differing standards can be applied depending on whether users are institutional or low-volume users. Public-key infrastructure (PKI) creates digital certificates and manages public-key encryption. PKI can be used for authentication of financial institutions or other similar high-volume users, while identity-based cryptography, which uses a string of identifiers (e.g. IP address, email address, etc.) to represent a user, can be used for authentication of low-volume users.

1.2 The frontier of privacy-enhancing techniques for financial systems

With the advancement of cryptography, newer systematic and mathematical methods to achieve privacy, confidentiality and anonymity in a wide range of financial systems and applications are being developed. Although many of these methods are at the frontier and require further development to be used at scale and without impacting system performance, they could be developed to increase privacy from outside parties or to enhance the robustness of the privacy features of a CBDC system.

The tools introduced in the cryptography section of this paper could be applied to various aspects of or entities involved in CBDC implementation. This text is strictly meant to explore technology options and possibilities, rather than to recommend or imply the appropriate degree of privacy from various parties, potentially including the central bank itself. The actual CBDC privacy scheme would depend on local policies, laws and regulations and other constraints, along with policy-makers' preferences.

Importantly, cryptography techniques alone cannot prevent failures such as hacking, unwanted data dissemination and leakage, censorship, corruption of information, privacy subversion or other issues that can affect financial and communication systems. Rather, a robust and holistic protocol that ensures the properties of the security model will need to be built.

> **Cryptography techniques alone cannot prevent failures such as hacking, unwanted data dissemination and leakage, censorship, corruption of information or privacy subversion**

For more insights into these techniques, refer to the following publications:

- World Economic Forum, *The Next Generation of Data-Sharing in Financial Services: Using Privacy Enhancing Techniques to Unlock New Value*, White Paper, September 2019.
- Tinn, Katrin and Dubach, Christophe, *Central bank digital currency with asymmetric privacy*, McGill University, 11 February 2021.
- Miers, Ian, "Blockchain Privacy: Equal Parts Theory and Practice", *Zcash Foundation*, 2021.
- Ben-Sasson, Eli et al., "Zerocash: Decentralized Anonymous Payments from Bitcoin (extended version)", *Cryptology ePrint Archive, Report 2014/349*, 18 May 2014.
- Solomon, Ravital and Almashaqbeh, Ghada, "smartFHE: Privacy-Preserving Smart Contracts from Fully Homomorphic Encryption", *Cryptology ePrint Archive, Report 2021/133*, 6 February 2021.
- Ma, Shunli et al., "An Efficient NIZK Scheme for Privacy-Preserving Transactions over Account-Model Blockchain", *Cryptology ePrint Archive, Report 2017/1239*, 22 December 2017.

1.3 Requirements for a privacy-preserving financial system

To assess which cryptography methods may be useful, central banks must first make decisions about the level of privacy they would like to create and enforce within their financial system. These decisions can be divided into three main technical components or features:

1. The **functionality** that enables the features of the system (e.g. minting, transferring, governance, etc.)

2. The **privacy guarantees** that ensure the privacy and confidentiality of the information, and the anonymity of the participants (e.g. sender anonymity, amount confidentiality, etc.)

3. The **integrity or security requirements** that ensure the system's robustness to attacks and fraudulent activity (e.g. stealing funds, double spending of the digital currency, etc.)

One of the most important aspects to consider when moving to a privacy-preserving system is ensuring the preservation of integrity requirements. In a transparent system, the operators of the system ("validators") usually verify the integrity requirements by looking at the transaction data and accepting transactions that are integral and follow the established rules, for example transactions that are not attempting to double spend. However, when building a privacy-preserving system, where the information is hidden even from the validator itself, the validator needs a way to accept the correct transactions without seeing the transaction data. This is where the power of cryptography reveals its potential.

Functionality

The points below set out the basic functionality and integrity requirements of a CBDC system as they relate to privacy.

Onboarding of individuals and institutions

This is particularly relevant for a system that requires unique identification of participants. A PKI system, for instance, could be used to identify every entity in the system (both institutions and individuals).[7] Such a protocol will ensure that all transactions are sent by someone identified in the PKI. However, privacy guarantees could ensure that third parties to the transaction will not be able to associate the transaction with a particular key (which represents a user) in the PKI. Furthermore, if auditing is required by law (e.g. for disclosure of fraudulent or illicit activity), additional functionality could uncover which key and identity are tied to a certain suspicious transaction.

Issuance

Only central banks are responsible for issuing CBDC. The issuance action can be both public, where all the issuing details are public, or private, hiding the amount issued.

Transfer currency between participants

The transfer transaction is where a sender (e.g. CBDC owner) transfers CBDC to the receiver of the transaction.

Privacy guarantees

The following is an overview of some basic privacy options within a CBDC system.

Sender and receiver anonymity

Sender and receiver anonymity are achieved if the sender and receiver details are kept private from various participants in the transaction. In the case of a CBDC, the receiver may not need to know who the sender is. The cryptography section below sets out the way in which identities can potentially be revealed to the central bank or a government authority, in the event of a fraudulent transaction or criminal activity. However, the central bank authority may have the power to de-anonymize at their discretion.

Funds and owner confidentiality

In a privacy-preserving financial system, each participant could be enabled to keep their funds and accounts private and confidential. The authority and even intermediaries might not initially need access to account information until it is determined necessary to address fraudulent or criminal behaviour.

Transaction unlinkability

This is the property that ensures that two transactions by the same participant cannot be connected to each other. Unlinking every pair of transactions ensures that the transaction graph is hidden, enabling the highest form of privacy.[8] Formally, this property is called "ledger indistinguishability",[9] since any two transactions look the same to an external party to the transactions.

Integrity or security requirements

Lastly, for the system to maintain its integrity and functionality, any CBDC should ensure that the following basic guarantees are fulfilled.

Ownership

This fundamental requirement ensures that funds cannot be transferred by an identity other than the legitimate owner of the funds. To own funds, a transaction with you as a receiver must have been verified and validated by the network. In a privacy-preserving setting, the address could be ensured while keeping hidden both the identity of the transacting parties and the amount transferred.

Balance preserved

This is the concept that the amount of money sent by the sender is the same as the amount of money received by the receiver. It is a basic requirement that prevents parties from spending more money than they have by creating money out of thin air. In a privacy-preserving setting, the balance of the transaction must be preserved in a hidden manner.

No double-spend

Similar to the concept of "balance preserved" above, this requirement prevents participants from spending the same money twice, ensuring they cannot spend more money than they own.

The above requirements are only a sample of features, options and guarantees relevant to a privacy-preserving financial system. A more extensive study should be conducted for any cryptographic protocol to be built securely.

1.4 The cryptography

In this section, the relevant advanced cryptographic techniques are described at a high level, together with examples of how they could be used to enhance privacy in CBDC and a review of their readiness for use.[10] As noted above, regulatory requirements with respect to privacy and the specific role of central banks and various authorities in CBDC differ across jurisdictions and are critical in determining the privacy tools employed in CBDC. The discussion below is exploratory and focuses solely on technology possibilities, rather than recommendations for specific CBDC architecture or privacy choices.

Zero-knowledge proofs (ZKPs)

This technique enables an individual to share the output of some computation with a second party, without sharing the inputs to the computation, while ensuring that the output is valid according to a publicly available function. This maintains the privacy and confidentiality of the data. ZKPs are viewed by both academics and open-source experts as a fundamental cryptographic tool to enhance the privacy and confidentiality of financial systems, for three reasons:

– Unlike other cryptographic techniques, ZKPs enable verifiability of local computations

– ZKPs enable auditability and prevention of fraudulent activity, even within the scope of private transaction data

– ZKPs are efficient enough to be used for verifying all the protocol rules in a blockchain-based financial system with auditing capabilities

Potential uses for CBDC

Zero-knowledge proofs can be used to prove that a transaction is legitimate, while hiding the data, or for revealing information about a CBDC account balance without revealing the balance itself. For instance, the central bank could calculate an interest payment or benefits for a stimulus payment for a certain account, without seeing the size of the account balance. ZKPs can indicate to the central bank whether an account balance is within certain ranges (for remuneration or KYC/AML purposes), without revealing the specific balance and while hiding information from all other parties.[11] ZKPs allow parties to transact in a private manner but also allow the central bank to conduct audits to extract insights about the economy.

Readiness for production

ZKP cryptography is being standardized through ZKProof, an open-industry academic initiative. ZKP has caught the attention of organizations such as the Defense Advanced Research Projects Agency (DARPA), part of the US Department of Defense, which cited in 2019 that zero-knowledge proofs have seen an uptick in use and efficiency in recent years, particularly in cryptocurrency. In 2019, DARPA launched an initiative called SIEVE (Securing Information for Encrypted Verification and Evaluation). SIEVE aims to develop computer science theory and software that can generate mathematically verifiable statements that can be shared publicly without giving sensitive information away.[12] Today, the technology can take millions of lines of code, input this to a zero-knowledge system and quickly identify whether there is a bug in the code. ZKP is also being used by Mozilla and Cloudflare, which implemented a scheme called Privacy Pass.[13]

Symmetric-key cryptography

This form of cryptography refers to those schemes that require a single key to perform the algorithms. One basic building block (known as a "cryptographic primitive") of a cryptographic system involves commitment schemes.

Cryptographic commitments allow a party to irreversibly pledge to a message or data in a private manner. A commitment scheme has two fundamental security properties: it must be *hiding* so that the message itself is private (by making the commitment random-looking) and *binding* so that, once the message is revealed, anyone can verify that the message is indeed the one that was originally intended and was not modified. In order to send a commitment message, a "commit algorithm" is employed that uses a random key to hide the message securely, even when the commitment output is shared publicly. A "reveal algorithm" is then used to reveal the underlying message, with the assurance that it was not changed since the time of commitment. Commitments are one of the most fundamental tools used to hide information that must be used as a reference for future verification.

Hash functions

Mathematic hash functions are a type of deterministic algorithm that generates a unique random-looking fingerprint of the input message. Any two computations of the same message will give the same hash result and no other message would give that result, which is how the unique fingerprint is generated. The algorithm has the property that it is relatively easy to compute the hash given the message, but it is almost impossible to find the input message given the output hash. Put another way, a huge amount of computation is required to *invert* the function. Hash functions are used everywhere in cryptography: to build commitment schemes, to enable non-interactivity in zero-knowledge systems, to hide information with a unique fingerprint and for integrity checks.

Public-key (asymmetric-key) cryptography

In a public-key cryptographic system (also referred to as asymmetric-key cryptography), there is a secret-public key pair that enables two parties to perform cryptographic operations (such as sending and receiving messages, authenticating data, etc.) without having to share private keys.[14]

Digital signatures

Digital signatures serve to authenticate the origin of data by providing a cryptographic connection between the identity (some public key) and the data, represented as a message. A signature algorithm allows the address of the secret key to sign a message, indicating that they are authenticating the message. A verification algorithm then takes the associated public key and verifies that the signature is correct. In a CBDC system, signatures can serve to authorize the transfer of assets. Mainly, once a transaction has been verified to come from the rightful owner of the assets, then it is validated.

An aggregate signature scheme can aggregate many signatures on a single message, making the resulting signature look like a single entity signed, maintaining the anonymity of the signing parties.

Encryption

An encryption algorithm allows parties to share messages by privately communicating over insecure networks. They can be employed with symmetric or asymmetric-key cryptography (for the former, the same key is used for both encryption and decryption; for the latter, different keys are used). Encryption systems enable peer-to-peer communication where, in the case of asymmetric-key cryptography, for a given key-pair the communication is directed to a single individual. This means that anyone who has a public key can encrypt any message, but only the address of the secret key associated with the public key will be able to decrypt and read the message. In a privacy-preserving financial system, this property is used to "warn" a receiver that there is a transaction for them. This is achieved by the sender encrypting some secret information using the public key of the receiver. Once the receiver sees the transaction, he or she will try to decrypt the message and, if successful, read the transaction data.

Symmetric-key cryptography, hash functions and public-key cryptography are used to put together different components of a financial system. One example is to derive a one-time address from the initial identity in a public-key infrastructure (PKI): for every new transaction, a receiver can derive a new address by computing a hash of the secret key associated with the public key in the PKI. This then allows a zero-knowledge proof to be used to prove the relationship and legitimacy of the identity. Another example is where hash functions are used to burn a token.

Potential uses for CBDC

In a privacy-preserving CBDC, transactions may not contain data in-the-clear, but instead contain commitments to the relevant data, such as the identity of the sender or receiver and the amount of currency transferred. When a transfer is being executed, the sender can "use" an existing commitment and create a new commitment, which would contain the address of the receiver of the transfer.

To ensure the *balance* of the transaction is preserved without revealing the amount transferred, the system can use a third functional property of certain commitments called "homomorphism".[15]

PKI enables individuals to send and receive funds while keeping account information secure. It can work together with a digital signature scheme, which enables a CBDC account owner to sign a transaction to send funds with his or her private key (a process that demonstrates his or her ownership of the account). The recipient would see the transaction incoming and verify its origin using the sender's public key. Signatures can be used to identify people on a CBDC as they enable verification of the origin of a transaction. Encryption can be used to communicate between two parties in a private manner, where encrypted information such as for a receipt or invoice can be sent alongside the transaction. Using encryption (with asymmetric keys), a receiver can be made aware that the transaction is meant for them and can use a private key to decrypt it.

Readiness for production

The cryptography functions described above are already in common use or are extensively available for production. Computing a hash function within a CPU is very fast. However, computing a hash function within a zero-knowledge proof is not as efficient and entails slower computation, depending on the number of functions being executed.

Multi-party computation (MPC)

MPC enables several parties to jointly compute some function on their individual inputs, without revealing their inputs to the other participants. The output is visible to all parties. In the academic realm, there are fully generic schemes that allow us to compute any such function or program. However, these generic schemes are not yet efficient and their implementation is not easy to use. On the other hand, there are "specific-purpose" schemes which allow computation of one type of function and are extremely efficient.

Secure secret sharing

One such function is secure secret sharing (SSS), and it is widely used in the blockchain space. SSS is a method for breaking down a secret into random-looking pieces, such that the secret can be reconstructed if and only if all the pieces are put back together. Importantly, the reconstruction itself can be done in a private way, where no single individual reveals his or her random piece. The most basic security assurance from secret sharing is that no subset of the parties with the individual pieces can reconstruct the full secret, maintaining its privacy. Private keys, as part of public-key cryptography, are fundamental to the functionality of financial systems, enabling assets to be fully controlled by the entity or entities in possession of the private keys. Secret sharing can be used today both to ease the recoverability process of a lost private key without losing security and to enable multi-signature accounts.

By combining SSS with public-key cryptography, different parties that are onboarded in the PKI can create a shared account by using secret shares derived from each other's public keys, such that the transactions from this shared account will not leak the identities of the owners.

Potential uses for CBDC

MPC can be used for multi-party wallets to generate secrets in a distributed way. Another potential application could involve multiple central banks in a multi-CBDC or cross-border CBDC arrangement contributing suspicious transaction data from their operations and jointly computing on such data. The data they contribute is kept private from the other central banks. They could determine whether transactions are illegal (by benefiting from a greater amount of data), without seeing the details of the transactions occurring in another country's CBDC.

Readiness for production

Although secure multi-party computation (SMC) is generally computationally inefficient, several research efforts are underway to improve its performance. Some schemes, like secret sharing, are being used widely in production within internet protocols and in some blockchain spaces. The more generic protocols, which allow computation on any function (e.g. machine learning or AI in a private computer) are not quite ready for production because they do not yet generally meet desired expectations for efficiency. There may be insufficient tooling to make the development easy for deployment. There are several companies, such as Inpher and Tripleblind, focusing on MPC and they are working to make this form of cryptography scalable.

Differential privacy (DP)

Differential privacy allows for one entity to keep the low-level data within a dataset private while sharing publicly the higher-level patterns, statistics or model outputs based on the data. It is well known that when analysing large sets of data, a minimal change in the underlying data can be identified only by looking at the results of analysis. This is called privacy leakage. Although not original to cryptography, differential privacy has become one of the most important tools to formally measure the amount of privacy leaked from a system as well as to hide the actual leakage from it. Data privacy comes in many flavours, but the general method is to add randomness to specific parts of the data set that are queried. This generates a fundamental trade-off to be considered between the amount of leakage permitted and the exactness of the results in the analysis.

Potential uses for CBDC

DP could potentially be used in a CBDC to aggregate data on the total amount transacted in a time period, while not leaking the individual data entries used across aggregations. Additionally, central banks may want to analyse transaction data to generate information, for example, on the

state of the economy. Differential privacy will allow analysis of datasets without allowing leakages of the original datasets. While DP enables statistical inference, it is still difficult to identify an individual.

Readiness for production

DP is efficient and usable today; there are several open-source implementations available, either for use or as reference. Mozilla Firefox is using differential privacy to do large scale analytics on users in Firefox browsers today. Differential privacy is working with legal departments in universities to explore the intersection between data and law. This technology is currently ready for production and will continue to improve in efficiency and in robustness of result, while minimizing leakage of information from the original dataset.

Homomorphic encryption (HE)

Homomorphic encryption is one of the most promising methods to enable computation on encrypted data. HE makes it possible for a party to compute on, analyse or manipulate encrypted data and never see the data in readable plain-text.

Homomorphic encryption can be partially or fully employed. Partially homomorphic encryption keeps sensitive data secure by only allowing select mathematical functions to be performed on encrypted data.[16] Fully homomorphic encryption (FHE) enables analytical functions to be run directly on encrypted data and yields encrypted results, which can then be decrypted by the appropriate parties or owner of the data.[17]

The client can encrypt their data, send the encryption to a server that will perform some computation, and then the client can decrypt the output to get the actual result of the computation on their data stored unencrypted (in clear). Even if HE is not currently efficient enough to run large computations on encrypted data, it can be used to do some basic operations. The Homomorphic Encryption consortium has produced a set of standard secure parameters to be used in production systems.[18] Several research efforts are underway to improve the efficiency of HE.

Potential uses for CBDC

HE could be used to aggregate and compute on encrypted data across accounts in a private manner, for example to check that the sum of a set of accounts does not exceed a certain amount. It could also be used to aggregate and analyse encrypted identity data from different transactions for KYC or anti-money laundering (AML) purposes. The central bank could also provide encrypted CBDC account or transaction data to a regulator, law enforcement organization or private firm that could compute to generate findings from it for various purposes.

On a cautionary note, HE is an encryption scheme, so one must consider who holds the secret key that enables eventual decryption. If multiple parties want to aggregate their data using HE, or perform a complicated function on it privately, they can certainly do it. For example, two parties could create joint HE keys using secret sharing, or using a "multi-key HE" scheme, and then separately encrypt their inputs. They would then have to cooperate to decrypt the result, using their respective pieces of the key. One must be mindful of where the eventual decryption happens.

Readiness for production

HE is being standardized. The most efficient schemes are quantum-secure. Quantum-secure cryptography refers to algorithms that are resistant to attacks by future quantum computers. For certain function types or small functions, HE is doable and efficient. There are many companies today that are using HE; however, it has not reached full maturity. For central banks, this may be ready for use today for simple computations. DARPA, part of the US Department of Defense, is leading interesting efforts around HE hardware acceleration, among other organizations.[19]

1.5 Advanced features

Advanced cryptography can enable several kinds of functions, for example:

- Auditing of specific transactions, addresses or entities by central banks and regulatory bodies
- Automated transaction flagging: preventive features that automatically enforce certain restrictions or behaviour on the participants, such as maximum transaction amount auditing keys

Auditing

Central banks and regulatory bodies (e.g. the US Securities and Exchange Commission) will most likely require some visibility on transactions of specific types, as well as on specific "tagged" people and on transactions between specific individuals. Techniques such as ZKP and MPC could be used to provide this kind of auditability, while minimizing the details shared and ensuring that the control is fully in the hands of the user.

Automated transaction flagging

Most countries impose a limit on the maximum transaction size that can be completed with cash. With CBDC, a similar control can be programmed, where a flag is raised on an attempted transaction that is larger than the permitted amount. The flag could even reveal some secret about the transaction that would allow an authority (such as an auditor or regulator) to see the sender's identity. The CBDC system could also be programmed to prevent certain transactions from occurring altogether.

1.6 Cyber threat protection considerations

It is not easy to design a CBDC protocol in a fully secure manner. Each cryptographic scheme has its own security requirements and putting them together can add more complexity.[20] One needs to keep in mind the size of the anonymity pool (the number of users or entities conducting transactions). The smaller the pool of users, the less privacy the whole system will have.

While privacy and security are two different concepts, it must be acknowledged that data loss prevention is also an important component of privacy preservation. Drawing from the World Economic Forum's Presidio Principles[21] and the Privacy Principles for Digital Development,[22] central banks will need to do the following:

- Assess the risks of unauthorized access to or leakage of any stored data
- Investigate which groups may be motivated to acquire your data and how capable they are
- Determine the sufficiency of information and access controls around data
- Track personal or sensitive information captured and create a plan for potential mid- and post-project destruction if necessary

Additional information on cybersecurity for CBDC can be found in the white paper in this report series entitled *CBDC Technology Considerations*.

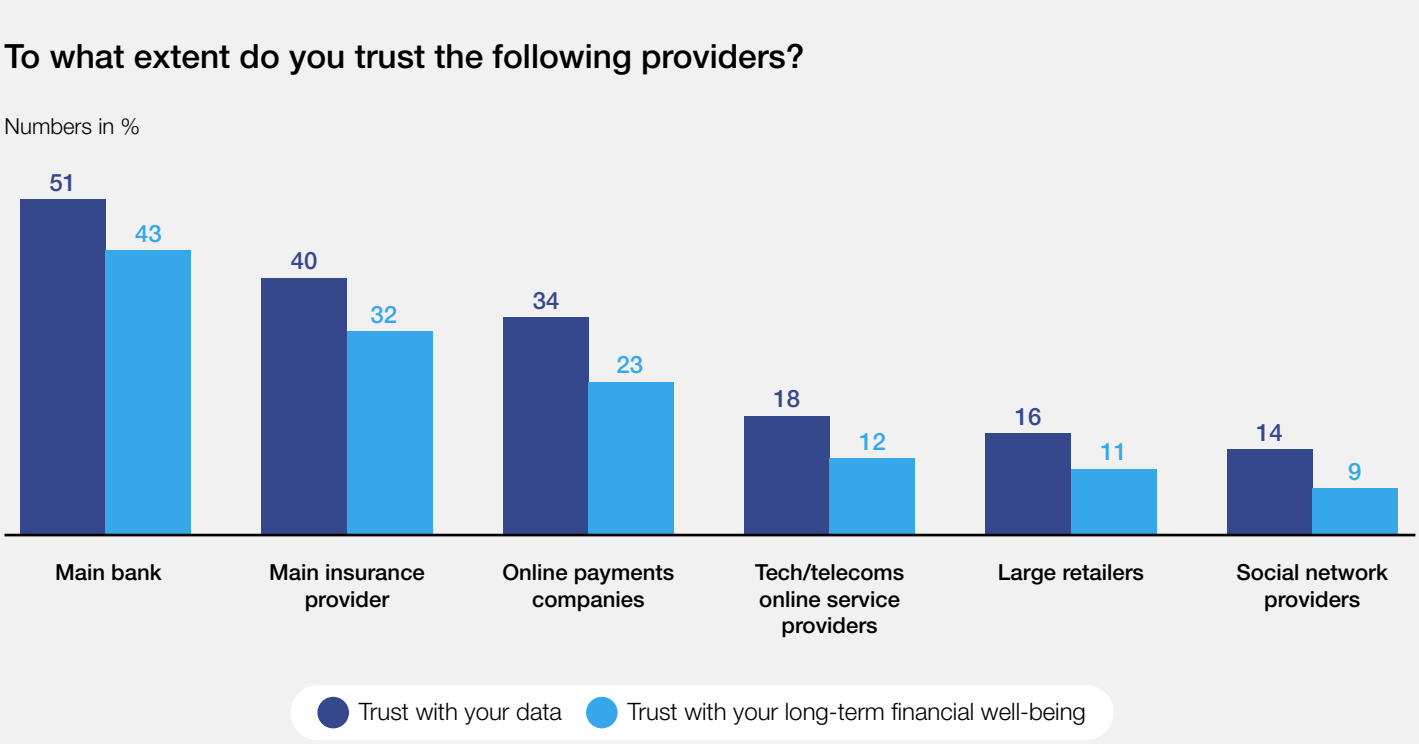
2 Policy and regulatory considerations relevant to privacy technology choices

2.1 The current state of trust

Consumers are becoming increasingly aware of and concerned about to whom they entrust their data and how it is used. According to Accenture's *2019 Global Financial Services Consumer Study*,[23] which surveyed 47,000 banking and insurance customers across 28 markets, the percentage of consumers who trust financial service providers with their data ranges from 14% (social network providers) to 51% (main bank) – see Figure 2.

In addition, many citizens do not trust their government to use their data to their benefit. A survey of 18,800 adults in 26 countries on consumer acceptance of information technology, commissioned from Ipsos by the World Economic Forum, found that only a minority of citizens trust their own national governments (39%), while trust in foreign governments is lower still at 20%.[24]

FIGURE 2 **The state of consumer trust in financial services**

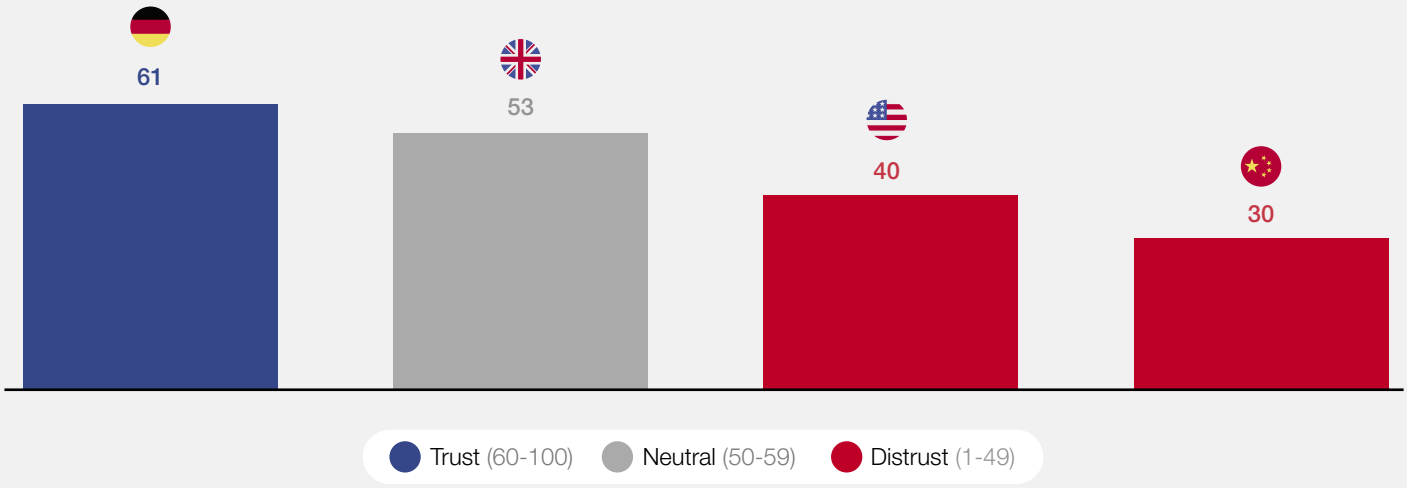


Source: Accenture *Global Financial Services Consumer Study*, 2019

The *2021 Edelman Trust Barometer* shows that businesses have become the most trusted institution, helping fuel the rise of stakeholder capitalism.[25] Business is more trusted than government in 18 of 27 countries, while some major governments registered neutral or negative trust levels (see Figure 3).

Successful adoption of CBDC requires a level of trust in the central bank – or trust in the government, for individuals who do not distinguish between the two or where the central bank lacks independence.[26] A primary concern of policy-makers is therefore to develop CBDC in a way that fosters user trust, particularly in how data is gathered and used.

FIGURE 3 **Percent trust in the national government of foreign countries**



Source: *2021 Edelman Trust Barometer*

2.2 Privacy principles and data subject rights

When it comes to safeguarding the privacy of data, there are three core principles – informed by the World Economic Forum's Presidio Principles[27] and the Principles for Digital Development project[28] – which central banks may adopt to inform their policies:

1. Prioritize the best interests of citizens, especially vulnerable populations, when collecting data
2. Limit the collection of personal identifiable information to what is necessary
3. Use data only for the purpose for which it was provided

For example, with respect to a possible future United States CBDC, the Digital Dollar Project proposes the following guiding principles for privacy:

1. People should be able to use a US CBDC without making themselves subject to undue corporate tracking or government surveillance
2. People may opt to benefit from legitimate, contractual sharing of information with financial services providers, or they may refuse it
3. Law enforcement access to CBDC usage data should be controlled by applicable US law, due process and the Fourth Amendment

Beyond any consideration of principles such as these, there remains the question of trust around a government's or institution's ability to instil and uphold consumer trust in the process.

2.3 Privacy regulations

Regulators across the world are introducing increasingly strong data protection regulations due to growing consumer awareness and demand. According to global research and advisory firm Gartner, 65% of the world's population will have its personal information governed under modern privacy regulations by 2023, up from 10% today.[29] By 2024, more than 80% of all organizations globally will need to comply with privacy and data protection requirements.[30] The European Union's (EU) General Data Protection Regulation (GDPR) and other privacy regulations improve institutional accountability and enforcement around data protection for consumers and citizens. Yet many of the privacy rules vary depending on geography and lack standardization across privacy mandates.

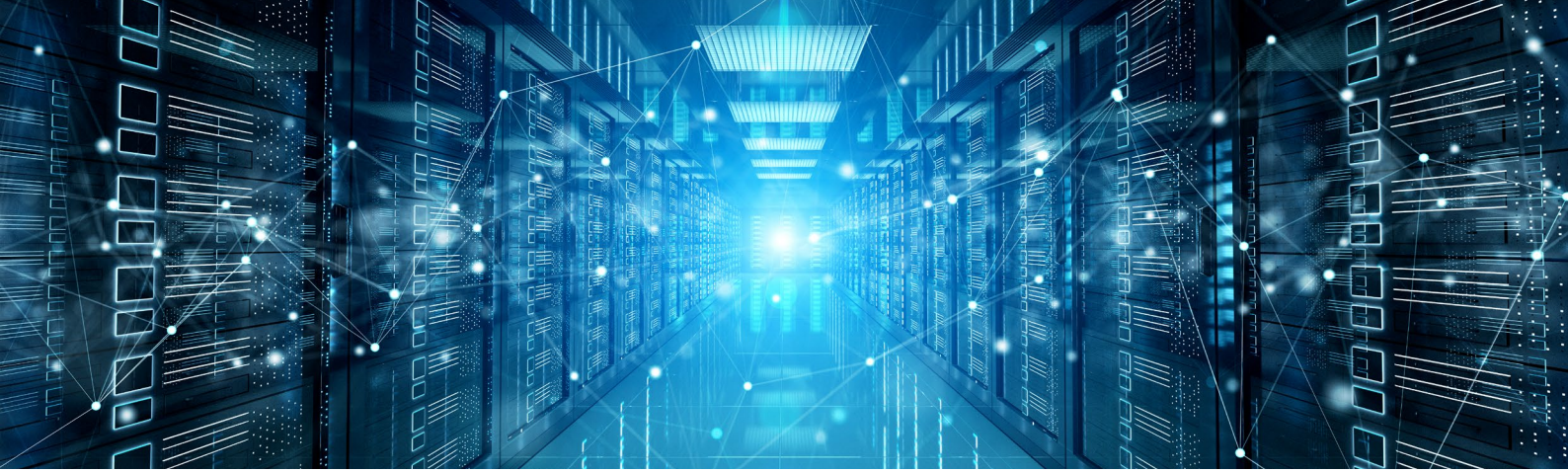
CBDC designers must negotiate varying national baselines of privacy regulation, especially when considering cross-border CBDC interoperability. They may benefit from designing architectures based on the stricter regulations (e.g. GDPR) to ensure longevity and standardization.

Table 1 summarizes personal data principles and rights, as dictated by three examples which have a considerable impact on data privacy and confidentiality discussions and regulatory developments around the world:[31] the EU's GDPR,[32] the California Consumer Privacy Act (CCPA),[33] and Canada's Personal Information Protection and Electronic Documents Act (PIPEDA).[34]

TABLE 1 **Data subjects' rights as protected by GDPR, CCPA, PIPEDA**

Data subjects' rights over their personal data	GDPR	CCPA	PIPEDA
Informed and expressed consent needed to process the data	Yes	No	No
Possibility of objecting to the processing of data	Yes	Yes	No
Special categories of personal information	Yes	Yes	Yes
Access to data	Yes	Yes	Yes
Correct incomplete or incorrect data	Yes	Limited	Yes
Right to be forgotten (data erasure)	Yes	Yes	No
Obligation to designate a data privacy officer	Yes	No	Yes
Obligation to provide transparency in data processing	Yes	Yes	Yes
Obligatory security measures	Yes	Yes	Yes
Breach notification	Yes	Yes	Yes
Privacy by design	Yes	No	No
Privacy by default	Yes	No	No
Employees' data protection	Yes	Limited	No

Source: Accenture



2.4 Policy choices for privacy

When enacting policies, policy-makers choose what rights they believe to be fundamental for their citizens and craft policies intended to protect those rights. This is especially important in the context of privacy, as policy concerns surrounding privacy differ across jurisdictions and can also differ in respect of private versus public actors. Some important considerations include the following:

- Many jurisdictions have laws which are geared towards the processing of personal information. If a CBDC drastically increases the scope of citizens' personal information being processed by the public sector, then new policy considerations will be raised. There will need to be consideration around whether such information will be shared between different government departments or bureaus.
- The approach that a country takes in its surveillance laws may have a cross-jurisdictional impact. This has been acutely experienced in respect of the GDPR's adequacy requirements and the invalidation of the EU-US privacy shield by the Court of Justice of the European Union due to the surveillance laws of the US.[35] Taking significantly different policy positions in respect of CBDC architecture could result in similar issues in privacy regulation being ported into the policy concerns of CBDC.
- Many of the regulatory regimes are designed around governments taking positive action to gain access to private transactional data, such as through a court-issued warrant. A change in this position resulting from CBDC architecture choices may require consideration on how these approaches are mimicked in CBDC frameworks.

Table 2 lists further considerations for policy-makers in the context of surveillance and CBDC adoption.

TABLE 2 **The spectrum of privacy**

Surveillance disincentivizes adoption	Opportunity cost of surveillance prevention and nuance	Most extreme risks of surveillance
– Lack of trust in government could hinder CBDC adoption, due to fear and ease of digital surveillance – Populations more engaged with the informal economy might be financially excluded	– Citizens may prefer that their data be used in an anonymous way for certain purposes, such as the advancement of science and research – Citizens may not want their data used for commercial marketing purposes	– Aggregated and anonymized data still presents the possibility of surveillance, such as the monitoring of demographic migrations based on transactional data

2.5 Balancing privacy and financial crime management in a CBDC world

In addition to data privacy laws, there are multiple regulations and policy obligations related to data privacy and financial services that must be considered when designing for CBDC. These regulations include anti-money laundering (AML) and counter-terrorist financing (CTF).

Central banks will have to make choices that balance privacy with law enforcement. This debate centres around the societal trade-offs between zero monitoring and stringent laws, as a CBDC operating at either extreme is likely to face significant adoption challenges.

At the foundational level, CBDC systems verify the uniqueness, security and settlement of a transfer of a CBDC by answering the questions: "Is this money genuine?", "Has the user spent this money before?" and "Did a transfer of money occur successfully?" The operators of the system (e.g. the central bank and/or its designated regulated entities) may not necessarily need to have visibility into account balances, identity information or other transaction-related information. The choice to have visibility into that information is a policy choice and can be limited, threshold-based and audited.

From the government perspective, one of the most promising advantages of privacy-preserving techniques applied to CBDC is the potential to enable more effective AML and CTF activities. Depending on the choices made, CBDC could enable appropriate regulatory entities to develop a topographical view of aggregated monetary flows and more effectively identify suspicious outlier transactions. This could be achieved in an aggregated way, by utilizing techniques (e.g. differential privacy) that would protect the privacy of individuals while providing the appropriate tools to regulators.

Lastly, the roles of the central bank and other institutions that engage with the CBDC, regarding maintenance, control, custody and other activities, will determine their requirements with respect to AML/KYC/CTF and other policies and the privacy requirements and protocols they adhere to.

2.6 The role of digital identity in privacy for CBDC

The design choices related to privacy need to allow for adequate identification mechanisms to meet national policy and legal requirements associated with, for example, anti-money laundering laws. The Bank for International Settlements (BIS) report, *Central bank digital currencies: foundational principles and core features*,[36] written in collaboration with a group of central banks, asks: "Digital identity is an emerging field in many jurisdictions. In the absence of digital identity infrastructure, what are efficient approaches to KYC/ AML/CTF?" The UK has proposed a digital identity and attributes trust framework,[37] which seeks to govern how organizations use digital identities.

This highlights a number of questions. Do national digital identity systems exist to support CBDCs? Will CBDC be implemented with standards closer to physical cash, for which typically no identification is required? Will central banks need to account for full population identification schemes, which some jurisdictions may require for their resilience and inclusion requirements?[38]

A middle ground solution is that central banks would connect to externally managed sources of digital identity information, such as a national digital identity scheme. These would need frameworks for integration with CBDC administration. Non-centralized solutions have also been considered, such as credential-based, "self-managed" or "self-sovereign" alternatives, which leverage digital wallets, generally in the form of mobile applications, to build digital identities off decentralized identifiers and verifiable credentials.

CBDC policy-makers will need to be keenly aware of developments in respect of digital identity architecture and how choices made in respect of CBDC frameworks impact or are impacted by these developments.

Conclusion

As with all technology innovation and advancements, there will be significant learning and evolution in CBDC over the next decade. Early designs and implementations will need to support constant modernization. Several frontier technology developments, while still requiring scalability, already reveal that privacy in CBDC will require a dynamic and nuanced approach to technical design and choices.

Core needs such as privacy may be central to CBDC designs. “Privacy by design” can be integrated with “security by design” to enable higher CBDC adoption and responsible deployment.

However, keeping pace with the variety of techniques to support the privacy objectives of a nation’s CBDC system is critical and requires constant engagement across the public and private sectors. Policy-makers will need to develop forums in which governments and other stakeholders can accurately communicate their goals, while exploring the potential of cryptographic, security, identity and other technology solutions. Without such a space, policy-makers will run the risk of adopting an approach without a full view of non-regulatory tools available to achieve desired privacy and compliance goals.

Endnotes

1. "ECB digital euro consultation ends with record level of public feedback", *European Central Bank*, 13 January 2021, https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210113~ec9929f446.en.html.
2. "Corda Documentation", *R3 Ltd*, 2021, https://docs.corda.net/docs/corda-os/4.6/key-concepts-ecosystem.html#admission-to-the-network.
3. "The e-krona pilot – test of technical solution for the e-krona", *Riksbank*, 2021, https://www.riksbank.se/en-gb/payments--cash/e-krona/technical-solution-for-the-e-krona-pilot/.
4. "Spending Corda State on Different Notaries", *Corda*, 27 July 2020, https://www.corda.net/blog/spending-corda-state-on-different-notaries/.
5. "The Riksbank in Sweden launches e-krona pilot", *PaymentsCM LLP*, 26 February 2020, https://www.paymentscardsandmobile.com/the-riksbank-in-sweden-launches-e-krona-pilot/.
6. Kharpal, Arjun, "China has given away millions in its digital yuan trials. This is how it works", *CNBC*, 4 March 2021, https://www.cnbc.com/2021/03/05/chinas-digital-yuan-what-is-it-and-how-does-it-work.html.
7. This could alternatively be achieved by designs such as a central authentication service in other architectures.
8. Miers, Ian, "Blockchain Privacy: Equal Parts Theory and Practice", *Zcash Foundation*, 2021, https://www.zfnd.org/blog/blockchain-privacy/.
9. Ben-Sasson, Eli et al., "Zerocash: Decentralized Anonymous Payments from Bitcoin (extended version)", *Cryptology ePrint Archive*, Report 2014/349, 18 May 2014, https://eprint.iacr.org/2014/349.
10. It is important to note that such cryptographic schemes are based on abstract mathematical models that provide a basis for the security of the schemes. Where necessary, cryptographic schemes can be modernized to account for evolving security threats, such as those that may arise from advances in quantum computing technology.
11. World Economic Forum, *CBDC Policy-Maker Toolkit – Appendices*, 2020, http://www3.weforum.org/docs/WEF_CBDC_Policymaker_Toolkit_Appendices.pdf.
12. "Generating Zero-Knowledge Proofs for Defense Capabilities", *DARPA*, 2019, https://www.darpa.mil/news-events/2019-07-18.
13. "Using Privacy Pass with Cloudflare", *Cloudflare Help Center*, 2021, https://support.cloudflare.com/hc/en-us/articles/115001992652-Using-Privacy-Pass-with-Cloudflare.
14. Tinn, Katrin and Dubach, Christophe, *Central bank digital currency with asymmetric privacy*, McGill University, 11 February 2021, https://www.mcgill.ca/engineering/files/engineering/central_bank_digital_currency_with_asymmetric_privacy_mcgill_tinn_dubach.pdf.
15. "Homomorphism, mathematics", *Encyclopaedia Britannica Inc.*, 2021, https://www.britannica.com/science/homomorphism.
16. Marr, Bernard, "What Is Homomorphic Encryption? And Why Is It So Transformative?", *Forbes*, 15 November 2019, https://www.forbes.com/sites/bernardmarr/2019/11/15/what-is-homomorphic-encryption-and-why-is-it-so-transformative/?sh=452d426c7e93.
17. "What Is Fully Homomorphic Encryption?" *Inpher*, 2021, https://inpher.io/technology/what-is-fully-homomorphic-encryption/.
18. Albrecht, Martin et al., "Homomorphic Encryption Security Standard", *HomomorphicEncryption.org*, 2018, https://homomorphicencryption.org/standard/.
19. "Building Hardware to Enable Continuous Data Protections", *DARPA*, 2020, https://www.darpa.mil/news-events/2020-03-02.
20. ZKProof, *ZKProof Community Reference, Version 0.2*, Chapter 4: Applications, 31 December 2019, https://docs.zkproof.org/pages/reference/reference.pdf.
21. World Economic Forum, Global Blockchain Council, *Presidio Principles: Foundational Values for a Decentralized Future*, http://www3.weforum.org/docs/WEF_Presidio_Principles_2020.pdf.
22. Principles For Digital Development, *Principle 8: Address Privacy & Security*, https://digitalprinciples.org/principle/address-privacy-security.
23. Accenture, *2019 Global Financial Services Consumer Study: Discover the patterns in personality*, 4 March 2019, https://www.accenture.com/us-en/insights/financial-services/financial-services-consumer-study-2019.
24. Ipsos and World Economic Forum, *Global Citizens & Data Privacy*, 2019, https://www.ipsos.com/sites/default/files/ct/news/documents/2019-01/ipsos-wef_-_global_consumer_views_on_data_privacy_-_2019-01-25-final.pptx_lecture_seule_0.pdf?mod=article_inline.
25. Edelman, *Edelman Trust Barometer 2021*, https://www.edelman.com/sites/g/files/aatuss191/files/2021-03/2021%20Edelman%20Trust%20Barometer.pdf.
26. Casey, Michael, "Money Reimagined: Warnings From an Argentine Tragedy", *CoinDesk*, 7 August 2020, https://www.coindesk.com/money-reimagined-warnings-from-an-argentine-tragedy.
27. World Economic Forum, Global Blockchain Council, *Presidio Principles: Foundational Values for a Decentralized Future*, http://www3.weforum.org/docs/WEF_Presidio_Principles_2020.pdf.

28. Principles For Digital Development, *Principle 8: Address Privacy & Security*, https://digitalprinciples.org/principle/address-privacy-security.

29. Moore, Susan, "A proactive approach to privacy and data protection helps organizations increase trust", *Gartner*, 20 January 2020, https://www.gartner.com/smarterwithgartner/gartner-predicts-for-the-future-of-privacy-2020/.

30. Moore, Susan, "A proactive approach to privacy and data protection helps organizations increase trust", *Gartner*, 20 January 2020, https://www.gartner.com/smarterwithgartner/gartner-predicts-for-the-future-of-privacy-2020/.

31. Although not an extensive sampling, the examples chosen in Table 1 are based on some of the stricter privacy regimes in place today, with similar regimes in Australia, Brazil, Chile, China, India, Japan, New Zealand, South Africa, South Korea and Thailand. See: Simmons, Dan, "13 Countries with GDPR-like Data Privacy Laws", *comforte AG*, 2021, https://insights.comforte.com/12-countries-with-gdpr-like-data-privacy-laws.

32. European Commission, *Data protection in the EU*, https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en.

33. State of California Department of Justice, Office of the Attorney General, *California Consumer Privacy Act (CCPA)*, 2018, https://oag.ca.gov/privacy/ccpa.

34. Office of the Privacy Commissioner Of Canada, *The Personal Information Protection and Electronic Documents Act (PIPEDA)*, 2021, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda.

35. "Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems", Case C-311/18, *ECLI:EU:C:2020:559*, 16 July 2020, https://curia.europa.eu/juris/liste.jsf?num=C-311/18.

36. Bank for International Settlements, *Central bank digital currencies: foundational principles and core features*, 2020, https://www.bis.org/publ/othp33.pdf.

37. Department for Digital, Culture, Media & Sport, UK Government, *The UK digital identity and attributes trust framework*, 2021, https://www.gov.uk/government/publications/the-uk-digital-identity-and-attributes-trust-framework.

38. Such as the Bank of England.

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org