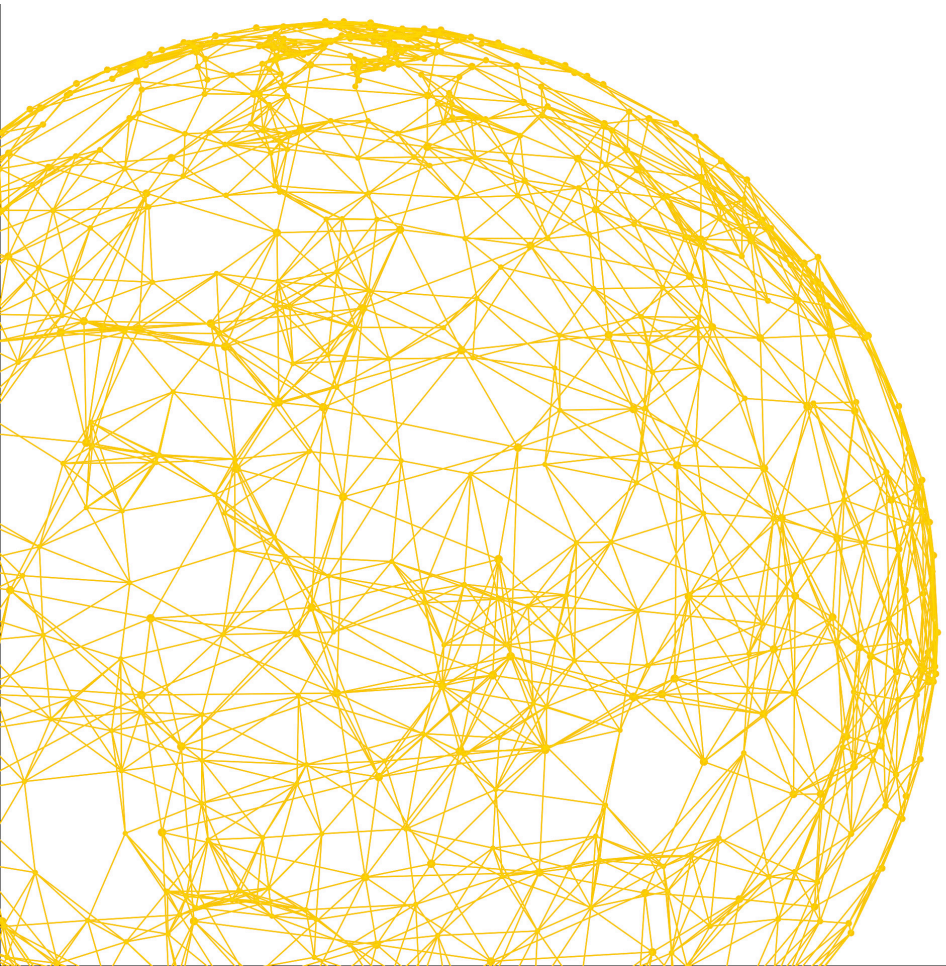
Visa
Economic
Empowerment
Institute

Imagining an open
future for payments

Designing for success:
How to build on the G7 foundational principles for retail CBDC

The art of public money **concluded with some important questions for policymakers to think through as they consider introducing central bank digital currencies (CBDCs). This follow-up paper provides our perspective on how some of those questions can be answered by examining: which of the principles should be considered first; what matters in payment transactions; and, based on our experience operating VisaNet for several decades, what have we learnt that can be applied to CBDC.**



VISA

Synopsis

The amount of activity, analysis, and experimentation surrounding CBDC is by no means surprising given its potential and importance. The decision to launch a CBDC involves complex and often interlinked policy, technology, and societal factors. The G7 principles for retail CBDC published last year provide a game-changing opportunity to shape the conversation. These principles provide a framework and guidance for decision makers by setting standards and boundaries for decisions. In our last paper on CBDC, *The art of public money*, we concluded with some important questions for policymakers to think through. This paper provides our perspective on how some of those questions can be answered by examining: which of the principles should be considered first; what matters in payment transactions; and, based on our experience operating VisaNet for several decades, what have we learnt that can be applied to CBDC.

Imagining an open
future for payments

Designing for success:
How to build on the G7 foundational principles for retail CBDC

Visa Economic Empowerment Institute

VISA

Acknowledgments

The Visa Economic Empowerment Institute (VEEI) is pleased to publish this paper, which was authored by Charlotte Hogg and Max Malcolm from Visa Europe. The authors wish to thank the following Visa colleagues for their review and input: Sonia Brown, Clinton Chen, Mike Gallaher , Tania Garcia-Millan, Jo Gillespie, Catherine Gu, Chad Harper, Barbara Kotschwar, Jacob Levy, Brian Pringle, Emily Rayment, Bakari Smith, and Rob Walls. For their helpful comments and design contributions, VEEI gratefully thanks Jen Swetzoff from Closeup Content and the design team from 451.

About the Visa Economic Empowerment Institute

The VEEI is a non-partisan center of excellence for research and public-private dialogue established by Visa.

The VEEI's overarching mission is to promote public policies that empower individuals, small businesses, and economies. It produces research and insights that inform long-term policy within the global payments ecosystem. Visa established the VEEI as the next step in its ongoing work to remove barriers to economic empowerment and to create more inclusive, equitable economic opportunities for everyone, everywhere.

Visit: visaeconomicempowermentinstitute.org

Index

Key insights

This paper is intended to support policymaking decisions—decisions which must start with elected officials and be implemented by central bankers. There is a flow that should be respected: Policymakers set decisions to define the goals and vision for CBDC; central bankers define the framework for implementation that meets the goals and vision; and further stakeholders—especially private enterprise—deliver their support within this framework.

By way of reflecting this flow, our paper progresses over three themes: the principles and decision makers; context for implementation; and specific design decisions for CBDC.

The principles and decision makers

The G7 principles for retail CBDC provide a framework to anchor decisions but principles are a starting point. An important aspect of how they are applied is to understand who is making decisions against each principle. The opening section of this document looks at the importance of the principles and who are the most appropriate decision makers in each case, be they policy makers or central bankers

Context for implementation

The broadest context for CBDC is the breadth of our society and the financial systems that form an integral part of it. To help focus the canvas, we have compared cash payments with digital payment flows. This helps understand what matters in any payment, but also helps to understand how payments have changed with the increase in digitisation.

Design decisions for CBDC

Based on our assessment of the decision makers and context, we focus on four of the foundational principles to draw out design decisions. Our key tenets are summarized below and discussed at length in the paper.

Operational resilience and cybersecurity

Visa's belief: Operational resilience and cybersecurity is the most fundamental foundational principle. Adherence to the principle of operational resilience and cybersecurity is not simply a factor for success but the starting point. All parties and services that act in a CBDC are bound by the need to deliver operational resilience and strong cybersecurity.

Competition

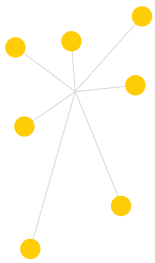
Visa's belief: Competition obliges all parties and providers to bring—and keep bringing—their best possible capabilities to contribute to CBDCs. To enable effective competition, a CBDC must support collaboration through standards and interoperability.

Data privacy and illicit finance

The principles of data privacy and illicit finance are combined in our analysis, because they are linked in terms of the design approach.

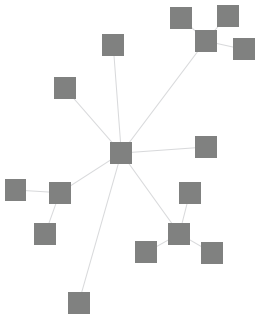
Visa's belief: Data privacy must always be respected, and by default users should be given privacy, along with appropriate choices. No system should be implemented that cannot adhere to legal standards for data use and financial control.

Introduction



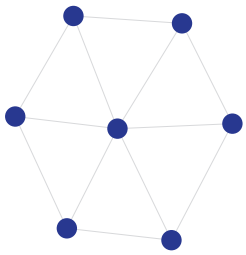
We have seen increasing adoption of digital payment forms, together with the emergence of quasi-currencies—especially stablecoins. It's possible to envision a world without cash and to see consumers engaging with new, stateless forms of money. It's therefore vital to ask questions about what governments and central banks should offer as alternatives.

Against this backdrop, policymakers around the world are working on the concept of central bank digital currencies (CBDCs). A CBDC, especially a retail CBDC, could have unintended consequences for the financial system, especially should consumers hold their accounts at the central bank. It is not just a matter of an operational headache—the consequences for the banking system could be extreme.



The work by the G7 to establish the principles for how to pursue a CBDC is particularly important in this context, and the principles themselves rule out most extreme scenarios. That said (and as is well known by those exploring this topic in central banks), although establishing the 13 principles required hard work, developing and implementing a CBDC is even harder. Technology offers enticing new capabilities, but technology alone cannot be the answer. A CBDC must be the outcome of a wide set of policy and technology choices that could shape society.

The Visa Economic Empowerment Institute's (VEEI's) June 2022 paper, *The art of public money*, posed a set of questions for policymakers to think through in the development of a CBDC. Policymakers are the chefs of CBDC and need to settle the recipe for this new financial dish before cooking with ingredients. They are experienced in building a cash environment when it comes to public money, but a digital payment environment is different. The means of exchange matters deeply.



This paper seeks to offer perspectives on what those plans might include for a retail CBDC; it also aims to address some of the questions raised in VEEI's last paper. We take the foundational principles established by the G7, focusing on those in which our experiences as a private-sector institution running a cross-border digital payment infrastructure for more than 60 years may be relevant. We then provide some thoughts as to the plans or requirements needed to deliver on those principles and the choices that might be open to policymakers.

Implementing a CBDC is hugely complex. We hope this paper will serve to provide some additional thoughts to policymakers, and we welcome continued engagement on this issue.

The G7 principles build a framework to guide CBDC implementations

The *G7 Public Policy Principles for Retail Central Bank Digital Currencies*, published in October 2021, provide a robust starting point for any discussion on the requirements of a CBDC. These principles seek to eliminate some of the tail risks to the financial system of a CBDC and ensure that issues that are core to society—e.g., those involving privacy or competition—are addressed.

We have used these principles as a starting point. For each one, we have considered where we could apply our relevant experience to inform the implementation of that principle, and where we might propose some requirements for a future CBDC.

The principles drive foundational decisions and the scope for opportunities

The G7 principles are classified into two groups: the foundational issues that focus on managing stability and oversight; and the opportunities that focus on establishing capabilities that can improve the current financial infrastructure.

The CBDC's foundational principles are our starting point. They are fundamental to enabling a means of exchange. We believe that trust and credibility are paramount in currencies and in payments. Trust matters deeply.

Opportunities are principles that pertain to use cases. The priorities envisioned in those principles are important, but they seem to be subsequent to, or to be enabled by, the foundational ones. For example, digital economy and innovation (#9) and financial inclusion (#10) could both be delivered through a robust model for competition (#5). In later sections, we will highlight those second-order effects.

G7 foundational principles

1. **Monetary and financial stability**
   Any CBDC should be designed such that it supports the fulfilment of public policy objectives, does not impede the central bank's ability to fulfil its mandate, and "does no harm" to monetary and financial stability.

2. **Legal and governance frameworks**
   G7 values for the international monetary and financial system should guide the design and operation of any CBDC, namely observance of the rule of law, sound economic governance, and appropriate transparency.

3. **Data privacy**
   Rigorous standards of privacy, accountability for the protection of users' data, and transparency on how information will be secured and used is essential for any CBDC to command trust and confidence. The rule of law in each jurisdiction establishes and underpins such considerations.

4. **Operational resilience and cybersecurity**
   To achieve trusted, durable, and adaptable digital payments, any CBDC ecosystem must be secure and resilient to cyber, fraud, and other operational risks.

5. **Competition**
   CBDCs should coexist with existing means of payment and should operate in an open, secure, resilient, transparent, and competitive environment that promotes choice and diversity in payment options.

6. **Illicit finance**
   Any CBDC needs to carefully integrate the need for faster, more accessible, safer, and cheaper payments with a commitment to mitigate their use in facilitating crime.

7. **Spillovers**
   CBDCs should be designed to avoid risks of harm to the international monetary and financial system, including the monetary sovereignty and financial stability of other countries.

8. **Energy and environment**
   The energy usage of any CBDC infrastructure should be as efficient as possible to support the international community's shared commitments to transition to a net-zero economy.

G7 Opportunities

9. **Digital economy and innovation**
   CBDCs should support and be a catalyst for responsible innovation in the digital economy and ensure interoperability with existing and future payments solutions.

10. **Financial inclusion**
    Authorities should consider the role of CBDCs in contributing to financial inclusion. CBDCs should not impede, and where possible should enhance, access to payment services for those excluded from or underserved by the existing financial system, while also complementing the important role that will be played by cash.

11. **Payments to and from the public sector**
    Any CBDC, where used to support payments between authorities and the public, should do so in a fast, inexpensive, transparent, inclusive, and safe manner, both in normal times and in times of crisis.

12. **Cross-border functionality**
    Jurisdictions considering issuing CBDCs should explore how they might enhance cross-border payments, including through central banks and other organisations working openly and collaboratively to consider the international dimensions of CBDC design.

13. **International development**
    Any CBDC deployed for the provision of international development assistance should safeguard key public policies of the issuing and recipient countries, while providing sufficient transparency about the nature of the CBDC's design features.

Assessing who makes decisions for CBDC implementation

It's important to identify the primary decision makers in delivering the requirements stemming from each of those principles. A CBDC can never be a purely technical issue. Technology does drive policy needs and is a key enabler to meet both policy objectives and user needs. How we as societies store value and exchange that value with one another is central to how our societies operate. Governments and citizens need to actively determine how they should do that and what choices should be made. Central bankers also have a key role against the objectives of financial stability and monetary policy that have been set for them.

In the cash world, it's easy to forget that we have made choices for cash to be almost entirely anonymous for payor and payee (except, of course, when it is turned into a digital record at a bank). We've made choices as a society about what people can buy with cash and what they can't, and what size transactions they can make with cash.

Meeting core design principles should not be left to unelected experts and policymakers, because these decisions will touch all citizens. Policymakers try to balance the benefits with the risks—risks of counterfeiting, of money laundering, of a grey economy. In a digital world, we have to make these choices afresh. Reflecting the choices made for cash in CBDC implementations should be open for public discussion and debate. Open consultation would be welcome, but part of the response to that consultation is that the elected officials should focus on these issues.

The private sector should also contribute to and support the implementation of CBDCs—just as logistics and printing companies support the cash world. As a starting point for that contribution, we have outlined which of the principles we can contribute to or advise on, recognising that for some principles it is essential for governments and central banks to be the decision makers.

In the table below, we have identified areas in which the private sector could play a role in establishing requirements for each of the principles. We asked the following non-exhaustive questions:

1. Is this a principle that touches on core societal values? If yes, then governments and citizens will ultimately lead on decision making, and the private sector can advise based on experience.

2. Is this a principle that central banks have a clear set of objectives around? If yes, they will lead on decision making as above.

3. Is this a question on which Visa has relevant experience? If yes, then we will take these principles further to outline potential choices.

Table 1: Assessing roles and responsibilities for CBDC implementation

	Principle	Government decision maker	Central bank decision maker	Private sector/ Visa experience
Foundational	1. Monetary and financial stability	-	Yes	-
	2. Legal and governance frameworks	Yes	-	-
	3. Data privacy	-	Yes	Yes
	4. Operational resilience and cybersecurity	-	Yes	Yes
	5. Competition	-	Yes	Yes
	6. Illicit finance	-	Yes	Yes
	7. Spillovers	-	Yes	-
	8. Energy and environment	Yes	-	-
Opportunities	9. Digital economy and innovation	-	Yes	Yes
	10. Financial inclusion	Yes	Yes	-
	11. Payments to and from the public sector	Yes	Yes	-
	12. Cross-border functionality	-	Yes	Yes
	13. International development	Yes	-	-

Source: Visa analysis

An assessment of cash vs. digital transactions to understand what matters in a payment

Before we turn to requirements, we need to clearly lay out all the steps in a transaction. This provides an important context. If we step back to think of policymakers being the chefs of CBDC, then it is important to make sure the recipe reflects the desires of those who are hungry.

A transaction is an agreement of exchange between parties, so in a payment we are looking at the exchange of a means of value for the receipt of goods or services. This provides a good blanket definition for transaction. However, a transaction can fail and therefore the agreement is not met. In a cash world, a failed transaction is one that goes wrong possibly because the payer has received goods or services that they didn't want, or the terms of the transaction were incorrectly applied (for instance, the payer has received incorrect change). Redressing a failed transaction in these circumstances can be challenging.

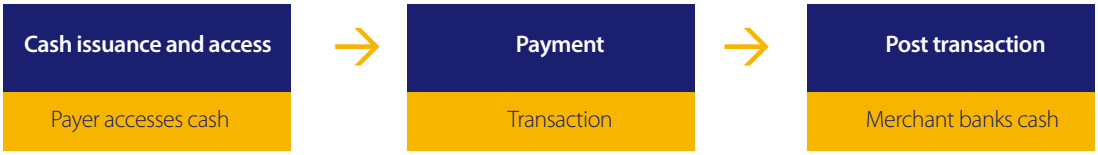
For instance, a customer who is served in a bar and when handed the change insist that they have paid with a larger denomination note than the change they received reflects, is left with their word against the servers. They have the option to wait until the till is counted up at the end of the day, but this is not an ideal position. In the digital space, a failed transaction is logged and the outcome is recorded. So, although a digital transaction can also go wrong, the logging provides a means to manage the failure.

As payments have become increasingly digitised, the features of a payment have changed. There are more steps in a digital transaction, and more players can participate in those steps. The features of both a cash payment and a digital payment, detailed below, demonstrate what matters in a payment and provide a basis that should be applied to the principles.

Cash payments

A cash payment flow is highly familiar to most people and businesses. Many of the rules or customs of a cash transaction are based on human interaction.

Figure 1: The cash transaction flow



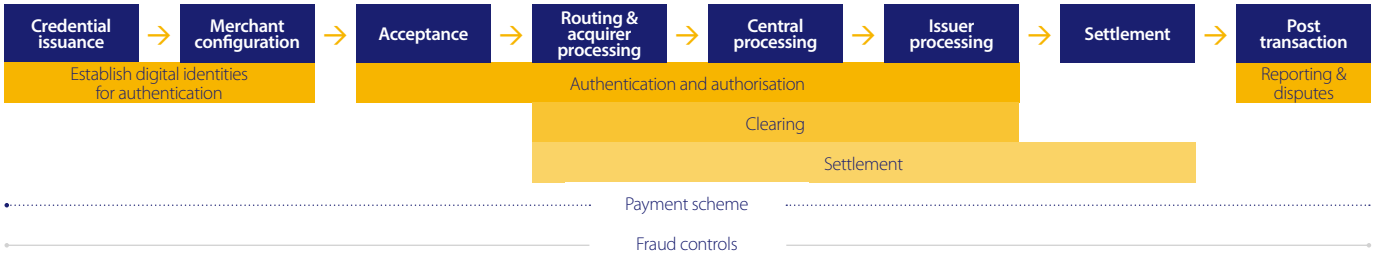
Source: Visa analysis

Although it is simple, this transaction has some specific aspects that can be identified as what matters in a payment. Access to cash is built on the minting of currency, and the coin or note represents the liability of the issuing central bank to honour its value. In effect, the payment scheme is embedded within the note. The primary fraud controls are counterfeit protection in the note and behavioural. The behaviour of either of the parties can trigger concerns in the other, and high-value cash transactions require compliance steps. Post transaction, any dispute management is dependent on the goodwill of the parties involved, and if cash is stolen, it is likely lost forever.

Digital payments

The digital payment flow introduces many more steps and broadens participation to multiple parties. Although these additional steps could be seen as adding complexity, they ultimately provide stronger outcomes and security for the parties engaging in the transactions.

Figure 2: The digital payment



Source: Visa analysis

The diagram above shows a card-based digital payment flow. The use of the term card is, perhaps, an anachronism. This flow is founded on the basis of a card authorisation but, of course, is independent of the card as the form factor. The credential issuance is the key starting point. It is the credential that is the digital identifier of the payer and can be used with a card, with a digital card emulation, a QR code or with a token-based capability for payments.

Key elements in the transaction:

- In a digital payment, a digital identity for each of the transacting parties must be established. This is not necessarily a personal identifier but an identity that allows the role (payer or payee) to be recognised, allows the means to manage routing for transaction messages to be passed between their representative institutions, and is the basis for authentication at the point of sale.
- Authorisation is the request for transactional approval.
- Clearing is the sharing of messages between the financial institutions that log the relative positions as a result of the transaction.
- Settlement is the issuing of instructions and movement of money.

- The reporting and disputes stage provides the mechanisms for transaction logs and the application of dispute management.

- Across the flow is the payment scheme that defines the rules and protocols that govern the transaction—it is the rules of the road. The scheme embodies multiple features of the payment, including the identifiers, acceptance standards, and terms for consumer protection. Scheme oversight also brings the trust to represent the liability of honouring the transactional outcomes, as the coin does in a cash transaction.

- Fraud controls can be applied across the payment transaction flow.

Drawing out design decisions to follow the principles and what matters in a payment

Within the context of what matters in digital payment flows, a clear understanding of the decision makers, and Visa's experience, four principles stand out as key. These are operational resilience and cybersecurity; competition; data privacy; and illicit finance.

These are key principles because they are foundational, and they are the principles for which the central banks are the primary decision makers. Visa's experience in the development of its payment network provides insight to support decisions and plans created to deliver on these principles.

Below, we take a deeper dive into these four principles. We combine data privacy and illicit finance because we believe the tight coupling between those two principles makes it helpful to cover them in combination.

1. Operational resilience and cybersecurity

Visa's belief: Operational resilience and cybersecurity is the most fundamental foundational principle. Adherence to the principle of operational resilience and cybersecurity is not simply a factor for success but the starting point. All parties and services that act in a CBDC are bound by the need to deliver operational resilience and strong cybersecurity.

Resilience and cybersecurity underpins the whole system. It is not enough to design and implement a resilient system—it is also necessary to operate and maintain a resilient and secure system.

The importance of resilience stands out in the context of a digital payment flow, which has the following sequence:

Overall, there is one obvious feature, which is that the extended chain requires resilience across multiple parties. A system's resilience is only as strong as its weakest link, and for a retail payments mechanism, the last mile is not in the direct control of the CBDC operator. Quality of service therefore must be guaranteed not only by technical controls but also by commercial and regulatory controls.

These requirements, especially for third-party connectivity and oversight, need to be defined and clear. A failure by a third party is attributable, in the mind of the user, to the whole system. Without a clear degree of transparency, a third-party failure can undermine trust and confidence in a CBDC.

There are also specific aspects of operational resilience and cybersecurity that are applicable to each step in the transaction, detailed below.

Credential issuance

In the digital landscape today, credential issuance is the point at which the credential is issued for prime beneficiaries of the service: individual consumers. The credential is their unique identifier and provides their secure on-ramp to the digital payments ecosystem. Using the credential requires the trust and confidence of users; thus, the availability and security of the service is paramount.

Merchant configuration

Similar to the credential issuance, the merchant configuration must hold the promise of trust and confidence. In addition to the merchant identifier, this step also includes the first routing decision—to whom a transaction will be passed for processing. This step represents the last leg in terms of connectivity and is furthest from the core of the payment infrastructure. It has the least opportunity for direct operational control, so the design of the service needs to assess the means of service interruption. There are three overall approaches, all of which should be applied with rigor: defining a robust operational standard; providing redundancy in routing choices; and enabling offline transactions.

Acceptance

This step is the point at which a transaction is initiated. The application of fraud controls and secure authentication is essential. This step is also when speed is essential. The authorisation is what both the consumer and the merchant are waiting for; a response that is as close as possible to real time. Paradoxically, real-time account-to-account payments do not demand as fast authorisation response times as card payments. Card payments must be fast because the payer is at the front of a supermarket queue or waiting to get out of a parking lot. The demand for speed means the end-to-end design should avoid bottlenecks and seek to push load sharing farther from the core.

Response time also needs to be scalable. Payment volumes are cyclical and have peaks and troughs. A service needs to be able to meet capacity demands beyond an expected peak—a system that works seamlessly under its most extreme stress should be the goal.

Routing and acquirer processing, central processing, and issuer processing

The next three steps in the process represent the interconnectivity between the participating financial institutions and the processing entity. Quality of service for connectivity holds a better guarantee with a private network than over the internet, although the private connectivity comes at a greater cost and a loss of flexibility. The private network model does provide the opportunity to define a stronger set of protocols for connectivity by parties. A core resilience factor, in terms of maintaining system availability, is the capability for the central processing entity to stand in and act on behalf of the institutions. Stand-in processing provides a powerful redundancy tool, but it does require a mechanism for threshold management. Threshold management are the rules or terms under which the central processing entity can reflect the expected outcomes of the participant.

This, in effect, reflects how much the behaviour of the central processing entity represents the institution it is standing in for. This capability can be vastly enhanced by machine learning models designed to improve transactional outcomes.

Settlement

In the settlement step, the instructions for money movements are posted. In the terms of our definition of a transaction, this is when the exchange is finalised. The parties directly involved in the transaction—the payer and payee—may already be satisfied, but their banking institutions are now responsible for honouring the transaction bound by their participation in the payment scheme.

Moving settlement away from core transaction processing is a proven way to improve response times. This is a design pattern called *separation of concerns*. The concern in the earlier steps of the payment flow is the commitment to honour the transaction which needs to be fast, frictionless, and secure so that payments in a retail environment can flow as users expect. The concern in this later stage is the moving of money (settling the transaction). The separation allows the system flow to process these steps independently.

The benefit of this approach is speed in the initial stages of the transaction when speed really matters. Settlement—the movement of the money—is performed later according to the settlement cycle. The frequency of settlement cycles is a major design decision that must balance participant requirements such as liquidity and liability within the system. It is also key to the payee because their receipt of funds is when they would be able to access and use the money received.

Not all payments are the same, or more appropriately, require the same features. Different payment flows such as account to account payments or card payments reflect different features in the messaging they use—e.g., authorisation response or settlement posting. A CBDC design that maintains independence between the core system and the messaging flows is able to support different payment features and inherently supports a separation of concerns design pattern for operational resilience.

Post transaction

Post transaction, the transactional logs—especially their use to support dispute management—mandate absolute confidence in the data. This step, although it is outside the core transaction flow, provides an opportunity to consider a point of resilience that sits atop each step in the flow. The oversight and rules that define how a transaction is processed and managed provide a non-technical standard for resilience. The governance of these rules sets the standard for the behaviour of all the participants in the flow and is the basis of building trust for users. A major test for the rules is how they are applied to dispute management.

The payment scheme is the basis for the trust and confidence that all users and participants expect from the payment service. Within the CBDC model, there is a direct relationship between the integrity of the central bank and the payment scheme. Therefore, resilience should not just be defined as technology or operational standards, it is also a standard for business performance.

Overall design goals for operational resilience and cybersecurity

Design standards for resilience and capacity management (and scalability) are essential. These standards must reflect:

Technology design

Build for redundancy that ensures there are no single points of failure and operates a model for level of active/active/autonomous failover.

Building redundancy in a system requires that there are no single points of failure. This doesn't simply mean two of everything, but requires a design and build that allows multiple nodes and paths through a system. This leads to an increased need for more components to maintain redundancy through the differing paths of a system. With more components, although the single points of failure are removed, there is added complexity and an increased number of different points of failure. Greater complexity and a larger system footprint risks introducing instability into the system that is being hardened. Building for redundancy therefore requires a challenging design pattern that manages system complexity by cross-routing paths between nodes and managing the flow of system traffic in an efficient and operationally sound manner. This is why the active/active/autonomous (triple A) model is important.

Triple A is a system model that runs with multiple instances of the service actively running in parallel so that if there is a failure in one instance, the system keeps running. The autonomous element enhances the model by enabling the switch over to other instances does not require human intervention. This is important from an operational perspective because human intervention can take longer and is possibly subject to diagnostic interpretation. In the autonomous model, diagnostics is part the automation.

Increasing redundancy in the system increases the cost of the system. Adding system components and complexity is essential for resilience but comes with an increased cost. Increases in cost also apply to the operational model.

Availability

A 99.999 percent (five nines) availability metric is a recognised benchmark for availability. For critical infrastructure such as a CBDC, it is important to consider the scale of numbers in more detail.

An important disclaimer before any numeric analysis though. A five nines availability metric is a system design principle. Every payment is important and system unavailability has real world impacts on the day-to-day life of individuals. Metrics risk failing to recognise the moment someone could be stuck in a car park because they can't pay. There are also fluctuations in payment volumes across a day and peak moments in an annual cycle. Impact analysis of system unavailability based on average transaction rates could also fail to reflect the true impact, which is time centric.

An availability metric defines the design and operational parameters for a system. A benchmark of five nines conversely accepts a potential loss of 0.001 percent of transactions. Thus, a system designed and operated with the expectation of processing 1 billion transactions in a year can, within agreed tolerances, drop 10,000 transactions through downtime.

One billion transactions is an arbitrary number to illustrate the impact of just meeting a five nines availability target. A CBDC platform will be designed with a target volume, but a successful CBDC must be designed to support growth. The higher the transactional volume the greater the number of "acceptably" lost transactions. Given that lost transactions are not acceptable, it is necessary to push towards a higher availability metric.

There is a diminishing return on investment, the challenge and cost to design and operate at a six nines level of availability is far higher than the uplift from four to five nines. The challenge to improve a level of system availability starts within its design but involves a continuous process of extension and hardening of system components. The operational activities of test, rehearsal, and planning for system events overlays a greater overhead than just business as usual. As the target for availability becomes tighter it can even boil down to small procedural changes that must be embedded in the culture of the operational team.

Ultimately, the aspirational target for availability is a trade-off, balancing the diminishing returns of investment to meet availability versus investment to support other system principles.

Recovery

Especially for the highest-priority system components, recovery should be instant. It is necessary to clearly define which system components are the highest priority (these tend to be the components that have a direct impact on transaction and settlement processing performance). The parties responsible for delivering these services must be held accountable to standards for performance and recovery, and visible to those who manage oversight of the system.

Cybersecurity controls must follow a comparable level of standards. Security is a feature required by design. It should be the first consideration, not a test that's applied post build. As cybersecurity becomes an essential feature of any organisational capability, meeting the standards defined by frameworks such as NIST (National Institute of Standards and Technology) or assessments such as the Bank of England's CBEST will be not just an operational overhead but a basis for daily activity. This basis applies to all parties.

It is important to recognise the scope of the security footprint. A new critical financial infrastructure will open a new set of attack vectors, and cybersecurity must cover all layers:

Network security

The entire connected infrastructure that provides all the system capabilities comprises the network. Network security requires controls at all entrance points and throughout the depth of the system.

Ecosystem security

The ecosystem broadens the reach to third-party services interacting with the core and the wider global environment. A domestic CBDC is a node in the global financial infrastructure. Visa's global footprint requires a global cybersecurity operation, and its capabilities enable a local response to international threats before they hit other regions. The same approach must be reflected in a national CBDC service.

Payment security:

Without payment security controls, there will be a huge gap in confidence among users. Although having a large arsenal of anti-fraud tools is desirable, payment tokenization is one of the most important capabilities. Payment tokenization masks much of the data in a transactional flow which reduces data exposure. Also, with a greater degree of abstraction from personal data, the opportunity to apply big data analytics for anti-fraud purposes is possible, without compromising data privacy. Any CBDC should lead with a baseline for payment tokenization in all financial flows.

A final point about cybersecurity is that controls are not just for the prevention and detection of threats, but also must ensure recovery from threats.

Resilience for growth

The operational resilience principle involves ensuring the availability of the system to drive trust and confidence. Over time, the system must be able to scale to support growth, to meet the resilience criteria not only for availability but also for speed of response. Many users of a system are familiar with the frustration of accessing a website grinding to a halt under the pressure of too many users. This is not a scenario that can be accepted for a payment infrastructure.

Designing the system to scale gracefully—such that its growth can be supported by adding system resources rather than re-architecting it—is incredibly important. Broadly speaking, there are two approaches to building scale in a system, horizontally or vertically. Horizontal scaling is an approach where additional copies of system components are added side by side to existing ones—in effect widening the system footprint. Vertical scaling is an approach where additional resources are added to existing system components—in effect making the system taller. The choice of how to scale a system is principally linked to is core architecture. To a certain extent, both approaches are necessary—a high-volume transactional system needs new components and more powerful components.

The requirement to scale a system must be recognised before it is needed. Adding capacity on the fly to address a performance deficit would be challenging and risky. It is essential to maintain a periodic performance review. There are a number of testing strategies to assess the performance of a system; it is the stress test that assesses a system's performance under extreme loads which identifies the critical performance limit. The cyclical nature of payments means that there are expected peak times for volume, such as Black Friday in the United States or Singles Day in China. Stress testing can run in lieu of peak events to ensure capacity is available.

The stress test is a key operational activity. The findings of a stress test, though, should not be to provide a sense of comfort. The findings of a stress test provide a basis to define investment in system scaling as follows:

1. Can the system cope with a peak demand?
   At this first level of assessment, the question asks if the system can continue to operate under duress. This ensures that availability targets are met.

2. Does the system behave how it should?
   The second level of assessment not only asks if the system can remain operational, but also performs without service degradation. Milliseconds count in a payment; a response time measured in seconds would result in increasing queues and frustration for shoppers and merchants

3. Does the system have capacity to exceed expectations?
   Additional capacity provides a buffer to maintain the service should there be an unexpected increase in volume. It is also an essential capability for resilience. As the availability and performance targets for as system are pushed further, planning for the worst-case scenarios is a key next step.

   System scaling needs an investment approach that can support organic growth but also maintain capacity to exceed peak demand when things go wrong. The system therefore needs to be able to operate to the same response times running peak load with the loss of multiple system components. The reason this is an investment decision is that the worst-case scenario, hopefully, will never happen but the infrastructure required to meet it needs to be accessible at all times. The accessibility of this additional capacity is either: "hot", meaning it is running as part of the system; "warm", meaning it is provisioned and ready to go; or "cold", meaning it is accessible but needs to be provisioned.

2. Competition

Visa's belief: Competition obliges all parties and providers to bring—and keep bringing—their best possible capabilities to contribute to CBDCs. To enable effective competition, a CBDC must support collaboration through standards and interoperability.

A CBDC model that leverages the merits of public and private enterprise to deliver CBDC capability is a natural starting point. In order to enable different enterprises to use their strengths, it is important to have a field for competition that is level and not barred by high barriers to entry. The business and commercial model for CBDCs is challenging, and the provision of the core CBDC is not a means of enrichment for a company. The commercial model must focus on the provision and improvement of services for users of CBDCs.

The number of connections or nodes in a network is traditionally considered to produce *the network effect*—in which the greater the number of connections, the greater the value of the service. Interoperability is critical from the outset. A clear catalogue of points of interoperability and associated standards is required to ensure that competitive services can built and provisioned.

However, the network effect should also be considered in terms of the protocols that link nodes. These protocols are not just technical standards or routing mechanisms; they are rules, procedures, and capabilities that shape how and why parties connect across a network, and who or what those parties are.

To look deeper into the connectivity protocols, it is helpful to go back to the digital payment flow:

Once again, the extension of the value chain for a digital transaction brings in more parties and inherently provides opportunities for different services to be offered to users. This naturally creates an arena for competition on two levels: along the transaction flow and into the transaction flow.

Participating parties in the flow should be able to contribute through open standards and clearly published participation protocols. The protocols for participation must define the rules and operational standards that maintain both user confidence and the overall integrity of transactions. The real heart of competition is the acceptance step. Acceptance is the transactional on-ramp for the payment flow and leveraging existing acceptance capabilities is a huge uplift to drive participation and transactional volume. Volume growth becomes a catalyst for adoption.

Acceptance

As stated above, acceptance is the step in which a transaction is initiated. It is the point when the credentials of the payer or payee, or both, are used to generate a request to pay or be paid. Digital payment acceptance covers multiple channels (for example, in-store point of sale and online e-commerce) and different form factors (for example, card and digital token).

The acceptance step is critical in encouraging competition across the transaction flow. Acceptance being the transactional on-ramp, it is the point at which a transaction is initiated. It is where consumer choice really comes into play. Strong acceptance protocols help acceptance feel safe, seamless, and familiar. This drives towards a frictionless payment capability.

A major challenge for the implementation of CBDC is that the use cases are not known. There are existing payment use cases which can be met, and there are emerging use cases that can be driven by CBDC adoption. There are also use cases that have not yet been thought of which can be realised through CBDC. By allowing competition, different use cases can be adopted and developed from the start. Existing, frictionless acceptance capabilities mean that use cases can be established and thrive based on the merit or validity of the use case—not barriers to access the use case.

Strong acceptance drives adoption, which in turn builds scale. The scale and adoption of the service further drives the opportunity for new use cases and innovation, which further still builds scale. This virtuous cycle stems from the accessible on-ramp. Growth reinforces confidence and provides a better commercial opportunity for providers of services to the system. Leveraging existing acceptance capabilities jump-starts adoption and participation.

The opportunity to jump-start adoption also converges to an important aspect of the competition principle. A CBDC implementation must be complementary to and coexist with existing means of payment. Adopting current acceptance means for CBDC will support the user interaction for consumer choice and enable merchants to leverage their existing acceptance services. Leveraging existing acceptance models does not just provide a means to allow the existing means of payment to sit side by side. There is also, at the use case level, the opportunity to cross fertilise the payment flows that are already available. The use of interoperable standards would enable a CBDC platform to integrate and enhance the wider payments ecosystem.

The protocols for acceptance are key to enabling existing acceptance to be applied to CBDC and cover four areas:

- Brand: The brand provides a payment mark that is visible to users and must be associated with trust. Trust is established through maintaining a security posture, standards for availability, capacity to support the busiest periods, terms for engaging with partners, and meeting regulatory standards. Brand-building efforts are not solely a marketing matter. They create trust. Leveraging existing acceptance removes the need to build a new, separate digital brand from scratch and the associated costs that would be required to do this.

- Credential: As described earlier, the credential is the digital identity of a user. This identity is used as a unique identifier and a mechanism for routing transactions. The Visa credential is simply a PAN, a 16-digit number that can be further tokenised to secure its content. Rules for how these credentials can be used, stored, and shared are essential controls to protect users. Importantly, a credential that is a mapping entity rather than a direct personal identifier or a direct link to a bank account have an inherent security feature—if these credentials are compromised, control mechanisms to minimise the liability and enable efficient recovery can be applied. Replacing a token credential is far cheaper and easier than changing a compromised bank account.

- Form factor: The form factor is the medium that stores the user's payment credentials. For years, the form factor was a card. Digital propositions and e-commerce have migrated the credential to different digital domains. Building on this migration, existing acceptance mechanisms can enable all form factors.

- Rules: Rules for Visa acceptance are in place to ensure that when a transaction is initiated, the correct protocols are followed. The protocols detail all aspects of transactional oversight, including adherence to regulatory standards and security standards.

Visa acceptance has taken many years to build and is a globally recognized mark of trust. However, a CBDC implementation should seek to leverage all forms of digital acceptance—existing payment marks and modes—to facilitate a path that reduces friction for CBDC adoption. Bringing the current digital payments infrastructure for fiat currency to the CBDC environment maintains the user experience and vastly reduces the cost of building CBDC acceptance. Creating an entirely new acceptance infrastructure for CBDC would be a major overhead and would delay adoption. Existing payment capabilities already accept multiple different currencies, and their messaging frameworks can be similarly applied to digital currencies and the technical integration should be built to meet the transaction model. The only reason to build afresh would be in response to a market failure. Existing acceptance mechanisms have the technical capability to support CBDC as well as the user base. So it is the commercial model for reuse that must facilitate the competition principle.

A CBDC implementation is a vast and challenging proposition. It needs to be given the best opportunity to get started and subsequently thrive for the benefit of citizens and for the opportunities presented to competing participants. In the mindset of competition, it should build upon a seamless, safe, and familiar user experience in order to catalyse adoption and volume growth.

3. Data privacy and illicit finance

Visa's belief: Data privacy must always be respected, and by default users should be given privacy, along with appropriate choices. No system should be implemented that cannot adhere to legal standards for data use and financial control.

In this discussion of the four key principles, we have singled out operational resilience and cybersecurity, competition, data privacy, and illicit finance. We combine the final two, not because they cover the same area, but because there is a link in terms of cause and effect. Effective controls to address illicit finance are best supported by some access to personal data. The approaches for data privacy and addressing illicit finance are coupled.

We live in a world in which user data are exposed to many organisations in exchange for services. There is a personal choice for individuals who wish to share their data to enjoy the benefits of services and those who don't. This choice becomes more complex with respect to government bodies and their access to user data. The individual and societal position is a personal and political conversation. A CBDC implementation, especially one that is supported by both public and private enterprise, must be reflective of the personal and societal positions rather than divisive. To maintain a balance while adhering to the principles, analysis of the digital payment flow can help to identify data requirements and controls.

In a digital payment flow, multiple organisations act to complete the flow. There are also multiple points of data capture and data use. It is important to assess what data are captured, when, and why. It is also important to understand where the data are used.

By looking at the digital payment flow, we can dig into the details of when, where, and why data are captured:

Credential issuance

Credential issuance is the responsibility of issuing banks or the token provisioning service. This credential provides a mapping to an account at an issuing bank. The issuing bank has the relationship with the customer and has access to that customer's data set. Although we have talked about the credential and focused on the PAN as the identifier, there are additional data associated with a card.

The additional data, controlled by the issuing banks, are, for example, the name and address of the account holder. This association is linked to the credential not as a prerequisite for achieving a transactional outcome—but to improve the outcome.

In this step, a digital identifier has been created and associated with some PII (Personally Identifiable Information) data by the payers' financial institutions. This allows a degree of abstraction between personally identifiable data and the data used in a transaction. Best practice suggests a further degree of abstraction.

Payment tokenisation takes the initially issued credential and creates another new digital credential. These tokens are resolved on use within the core payments infrastructure reducing the need for use of direct personal identifiers. In this model, and with further abstraction from personally identifiable data, the individual's name and address need not be supplied for the transaction, and big data analytics can be leveraged for fraud controls.

Merchant configuration

Configuration for a merchant is comparable to the issuing point with respect to the creation of a digital identifier. In addition to the identifier, more data are captured to cover aspects such as merchant type and location.

More parties may be involved depending on the nature of the merchant and payment channel. The acquiring model sets parameters relating to terminals and e-commerce gateway provision, and these parameters are where multiple parties can be involved: the merchant itself, the acquirer, the terminal provider, and the e-commerce gateway provider.

It is at this step that the digital identifier for the merchant is captured, and also the metadata that describes the merchant type. These data are configured by one or more parties.

Acceptance

The acceptance step is where a transaction is initiated. A transaction requires, at a minimum, the identification of the payer and payee and the transaction amount. However, a digital transaction creates and uses additional data to improve the transaction outcome. An improved transactional outcome is primarily one in which the authentication response is more likely to provide the correct response: a positive authorisation for a genuine transaction, and a negative authorisation for a transaction that can't be fulfilled or that is fraudulent. An additional improved transactional outcome is the capability to service post-transactional requirements such as dispute management.

The transactional outcome is shaped by building a data document for a transaction that can be used in the next step, the processing step. It is hard to describe this document because it is contextual. Its contents are variable according to various circumstances. However, one very important and consistent feature is that it is not simply a list of all the data required for the transaction. It contains some data facts but also references to data stored and controlled by different parties who can be called on to supply results for checks by the processing entity.

The key point is that the identity of the parties required is not based on direct personal identifiers. The identity is token based.

Data fields include:

- core data such as transaction time, transaction amount, and currency;
- party data such as PAN or payment token, merchant ID, and merchant type;
- and contextual data, which depend on circumstance and transaction type (transaction type is a data field to identify e-commerce vs. contactless payments):
    - An in-store transaction will, for instance, have data about the terminal.
    - An e-commerce transaction will have the cardholder's address to support an address verification check.
    - A mobile transaction will include data to identify the phone used, such as the device identifier and operating system, allowing the customer's institution to check the source of the transaction.

There are also data fields used to support network management and space for any data required for local regulatory needs.

Routing & acquirer processing, central processing, and issuer processing

The processing domain step is broadly an exchange among three parties: the acquirer, the central processing entity, and the issuing institution. This is where a transactional outcome is defined, so it should be seen primarily as the point of data usage.

In the simplest form, transaction processing is an activity of resolving the digital identities of the parties and routing the messages to their respective institutions. The primary message intent is to check on whether the payer has available funds and therefore whether the transaction can be authorised.

Checking for available funds is the easy part. The most important action is actually to resolve the identities and ensure that the transaction is genuine.

The transactional outcome is a binary decision of approval or decline. Primarily, the aim is to prevent fraudulent transactions; however, it is still a poor transactional outcome if a genuine payment request is refused. Maximising the frequency of correct outcomes requires a risk assessment and the more detailed the assessment the more accurate the response.

The data and data references collected in the transactional data document provide the basis for the risk assessment. The contextual examples in the preceding section show how this information supports the risk assessment:

- The terminal information for an in-store transaction will confirm PIN entries or a request within the contactless transaction controls.

- The e-commerce transaction will use the cardholder address as part of an AVS (Address Verification Service) to validate the cardholder details.

- The mobile device information can be used as reference against previous transactions. This is a behavioural metric. If the device has been used for previously approved and undisputed transactions it is more likely to be a genuine transaction.

Risk thresholds are not arbitrary; they are defined according to yet more contextual considerations. Transactional value or frequency of transaction requests could increase risk score calculations. Depending on the risk assertion, a transaction could be declined; a request for an additional SCA check could be issued; or the transaction could, under the right circumstances, be approved rather than garner a false decline.

An additional point of improving transactional outcomes is enabling one party to stand in for another. This provides a resilience mechanism should a party fail. It means that the stand-in entity must run a risk score with the information available.

Data relating to the transaction processing and outcomes are logged at this stage and can be used by parties for reconciliation and other post transaction actions.

A challenge at this point of the flow is that there is a fundamental decision point: the transaction decision. The result must be as accurate as possible and leverage data to get the best result. The results also need to be processed and returned with milliseconds.

Post transaction

Post-transactional activities use the logs and records created in the payment flow. This is an inherent value point of the digital payment flow, where records of transactions and the responses derived from the data are captured. Much as with the transaction data document, though, this is not a complete list of all the data associated with the transaction. It is a log of events and core data or data references. Post transactional records are stored by multiple parties, each storing their data that are relevant to the record.

This transaction log allows consumer protections to be acted on. Where there is a dispute, the right information can be called upon to identify what happened and to enable consumer redress.

These records also provide the basis for deeper anti-fraud and illicit finance controls in the shape of analytics and machine learning. Machine learning models that can be trained to analyse behaviours and patterns can be used to understand fraudulent behaviours and be applied to controls within the processing step to enhance the risk assessment.

This analysis is another action in which the referential basis of digital payment data is important. The analytics are not intended to build a picture of a person's behaviour, but they do build an anonymised picture of cardholder payments that can be used to spot anomalies for fraud detection.

There is also a broader macro view that can be, and has been, used to recognise behavioural patterns in one place and lock down activity in order to prevent a wider, systemic challenge. This is well demonstrated in ATM cash-out attacks, in which an institution is hacked and attackers use cloned cards to attempt to withdraw large amounts of cash from ATMs. This behaviour has been spotted by Visa analytics, allowing Visa to isolate the threat and prevent the attack from spreading.

Overall considerations on data privacy and illicit finance

The focus on fraud control in this section highlights the benefit of data capture and data use. By sharing the data load across the transaction space, the parties can meet a general principle of data privacy.

A CBDC implementation needs to be built to understand what minimum data set is required, what data set is required for service enhancement, and what data set should be optional based on user preference. Mandating consumer data sharing from the core will compromise a principle of data privacy if the different levels of data exposure are not recognised.

The need to meet illicit finance controls must also be acted on. To this end, the parties that own relationships with users are the starting point for meeting these standards.

One of the many values of a well-defined payment scheme is that it incentivises all parties to align on their approach and application of the required standards to participate in the scheme. As can be seen in some instances, however, where the scheme does not drive standards alignment, there is a marked increase in payment fraud.

Expectations that a CBDC will reflect the anonymous features of cash do need to be respected. A CBDC is not a migratory replacement of cash, and the two will run in parallel. However, it is important to design with the idea that cash could be replaced. Anonymity is a feature that could be built as a service rather than a design principle. The anonymous service would be a masking/proxy capability. Compliance in meeting illicit finance controls can limit flows that are masked if insufficient data are provided.

This could be a controversial decision point, but our intention in recommending it is to raise the need for balance and understanding.

A CBDC, despite its complexity and potential impact, should be seen as an evolutionary—not revolutionary—step

In trying to provide some considerations for just a subset of foundational principles, it is hard to not go even deeper on specific aspects. We recognise that this is a complex, sometimes nuanced, and certainly important topic for policymakers.

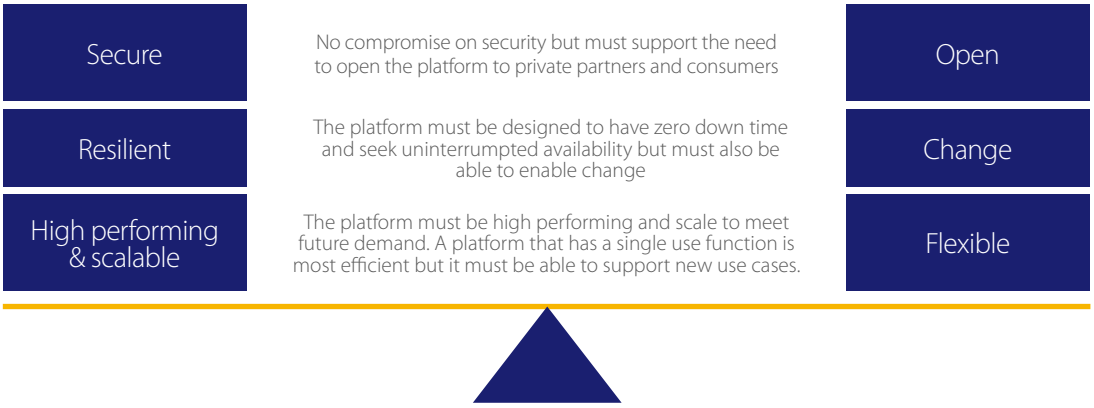
To summarise our thoughts on the key principles:

Operational resilience and cybersecurity	Competition	Data privacy and illicit finance
• The need for resilience and security applies across the entire value chain. • Designing for separation of concerns improves resilience both technically and functionally. • Resilience and cybersecurity must be implemented to prevent loss of service, but also to ensure recovery. • Each step to drive resilience and security requires high investment from the outset.	• Existing acceptance provides the on-ramp for CBDC to drive adoption and use through access to existing infrastructure and opening competition to drive innovation. • Leveraging existing means of acceptance focuses competition on delivering use cases, not access to use cases, driving a virtuous adoption model for CBDC based on its benefits. • All forms of acceptance can be supported to support different means for different needs. • The user experience must be maintained and support user choice.	• Data requirements should be built on the basis of what is needed and what can improve outcomes. • Data privacy should be managed by all parties, but not all parties need access to all data. • Identifiers should be tokenised, with contextual and transactional information driving fraud controls, not PII. • Parties must be incentivised to align to these standards by the payment scheme.

Matters of huge importance—combined with deep complexity—pose some very difficult and challenging questions. A CBDC, which could play an enormous role in society and which requires deep technical and economic understanding, is one of those matters.

The G7 principles are the foundation that decision makers can use to frame their approach, but they are only a starting point. Finding the right balance between the essential foundations of security, resilience, and performance while also enabling innovation and change is hard.

Figure 3: The balance of competing factors



Source: Visa analysis

However, we at Visa have maintained that balance in our network, and we feel that it is essential to continue to do so. A CBDC must also seek to maintain that balance. Foundational principles and leveraging existing capabilities pave the way for innovation in the design and use of CBDC. A CBDC must be a platform for the future that is capable of realising outcomes that have not yet been envisioned.

With this in mind, in an upcoming paper, we will examine the G7 "opportunities" principles (numbers 9-13) and consider how a CBDC platform should drive innovation.

Annex 1: Text descriptions of figures

Figure 1: The cash payment flow. Figure 1 displays simple process flow of the three steps in a cash transaction. The flow starts with cash issuance and access, sets to the payment and ends with the post transaction step. Beneath the flow the figure shows the principal action in each step which are, respectively: the payer accessing cash; the transaction itself; and the merchant banking the cash.

Figure 2: The digital payment flow. Figure 2 displays a digital payment process flow which includes the following steps: credential issuance; merchant configuration; acceptance; routing & acquirer processing; central processing; issuer processing; settlement; and post transaction. Beneath of each of these stages the key activities are identified. These activities cross different stages and are listed as follow: Establish digital identities and means for authentication between the first two steps of credential issuance and merchant configuration; Authentication and authorization below the acceptance, routing & acquirer processing, central processing, and issuer processing steps; Clearing beneath the routing & acquirer processing, central processing, and issuer processing steps; Settlement beneath the routing & acquirer processing, central processing, and issuer processing steps; and final beneath post transaction is the reporting and disputes activity.

Underpinning all steps in the process are two additional functions: the payment scheme; and fraud controls.

Figure 3: The balance of competing factors. Figure 3 displays a representation of a scale balancing the competing factors of security vs. open; resilient vs. change; high performing & scalable vs. flexible. At the fulcrum of each pair is commentary to finding balance as follows: security cannot be compromised but must support opening the platform for partners and consumers; the platform must be designed for zero downtime and uninterrupted availability yet still able to enable change; the platform must be high-performing and scale for change. While a platform that has a single function is most efficient it must be able to support new use cases.

About Visa Inc.

Visa Inc. (NYSE: V) is the world's leader in digital payments. Our mission is to connect the world through the most innovative, reliable, and secure payment network–enabling individuals, businesses, and economies to thrive. Our advanced global processing network, VisaNet, provides secure and reliable payments around the world, and is capable of handling more than 65,000 transaction messages a second. The company's relentless focus on innovation is a catalyst for the rapid growth of digital commerce on any device for everyone, everywhere. As the world moves from analog to digital, Visa is applying our brand, products, people, network, and scale to reshape the future of commerce.

For more information, visit About Visa, visa.com/blog and @VisaNews.

Visa Economic Empowerment Institute