



# **CBDC Innovation in the Caribbean**

The Caribbean Central Bank Digital  
Currency Workshop Summary Report

# Contents

- 3. Foreword | Acknowledgements
- 4. Executive summary
- 11. Case study: Learnings from the ECCB DCash Pilot
- 16. Workshop Summary



# Foreword

Central banks in Latin America and the Caribbean are a few of the most innovative financial regulators worldwide. The Bank of the Republic of Haiti, in particular, is making headlines through its central bank digital currency (CBDC) initiative and driving the regional financial inclusion agenda.

## Acknowledgements

Xiaochen Zhang prepared the Caribbean CBDC Workshop Summary report on CBDC Innovation in the Caribbean. Thank you to Ludmilla Buteau Allien, Leandro Bennaton, Nilesh Dusane, Ella Fitzsimmons, Ligia Lopes, Santiago Lopez, David MacKeith, Layla Mosadegh, Jana Nelson, and Erica Salinas for their support.

The [AWS Institute](#) sponsored this report. Anastasia Raissis provided overall guidance on the event and report. We are especially grateful for the contributions and collaboration that Governor Jean Baden Dubois of Bank of the Republic of Haiti and his team offered in organizing the event.

Thank you to the Eastern Caribbean Central Bank for the rich content provided during the workshop for the case study included in this report. Thank you to all [speakers](#) who contributed to the success of the workshop.

Central banks have a daunting task at hand. They respond to emerging issues quickly, while adapting to advancing technology, new asset classes, and proactively preparing for economic shocks. In their effort to adapt to new technologies, in particular, it is critical to leverage the expertise of those taking the lead. This is why we convened a workshop on CBDCs that led to this report.

The Caribbean Central Bank Digital Currency Workshop brought together 92 participants from twenty central banks and six non-central bank financial regulators to learn from early experiments. Speakers from across the public and private sectors discussed CBDC design choices and the enabling power of cloud technology in supporting CBDC development from discovery through launch. The conversations and learnings were invaluable in developing the collaborations necessary to make CBDCs a success in the region and across the world. We are delighted to have collaborated with Governor Jean Baden Dubois and his team on this regional workshop.

This report summarizes findings from the two-day discussion. You will also find a case study that summarizes the Eastern Caribbean Central Bank's DCash journey. With this report we look forward to further contributing to make the future of money beneficial for all.

### Anastasia Raissis

Director of Global Cybersecurity and Regulatory Policy,  
Worldwide Public Sector at Amazon Web Services

# Executive summary

In July 2020, the Bank of the Republic of Haiti and Amazon Web Services (AWS) convened the Caribbean Central Bank Digital Currency Workshop, during which participants shared their experiences and considerations on Central Bank Digital Currencies (CBDCs).

Over the course of two days, 90 participants joined representatives from over 20 Caribbean, European, and South American central banks, six non-central bank financial regulators, and multiple international organizations such as the International Monetary Fund and the World Bank. AWS and other technology partners were also represented.

Introducing the workshop, Jean Baden Dubois, the Governor for the Bank of the Republic of Haiti, noted that technological innovation is a great catalyst for development and democratization of the Caribbean island states. He observed that the Caribbean is leading the way as more than eighty central banks are studying, exploring, and testing the possibility of integrating CBDCs in their payments ecosystem.

Anastasia Raissis, director of global cybersecurity and regulatory policy, worldwide public sector at AWS, set the tone for the workshop by saying:

**“ If CBDCs are properly designed and wisely adopted, they could become a complementary means of payment that addresses specific market failures, protects citizens from crimes, and bring financial services to many people who are not covered by the current financial system.”**

We ran the rest of the workshop according to the Chatham House rule. Participants spoke candidly about early pilot programs, what they've learned, and the challenges and opportunities involved in implementing CBDCs. We designed the workshop to bring together a variety of perspectives and experiences, and to create an opportunity for participants to connect. Workshops, such as this one, help exchange best practices in the development of CBDCs.

Session topics included what we have learned from early CBDC experiments; how the cloud delivers solutions for CBDCs; the technology considerations for designing CBDCs and the policy; and regulatory ramifications of designing a CBDC. This report summarizes the discussion during the workshop, and a case study of the Eastern Caribbean Central Bank's DCash pilot.



# 1. CBDCs and their potential to drive progress

The pilot programs discussed during the workshop—ECCB’s DCash and Bahamas’s Sand Dollar—showed the potential for CBDCs to drive progress in a number of policy areas.

These include making payments systems faster and more efficient—increasing the resilience of today’s brick and mortar banking systems, including in response to climate change. The systems are also making banking more equitable and inclusive, especially for unbanked or underbanked people.

As one participant said:

**“ CBDCs is a new payment instrument that could bridge the gap in financial inclusion while improving or fostering the modernization of the entire retail payment infrastructure.”**

One presenter drew attention to the benefits of piloting CBDCs in cross-border payments. In this example, the CBDC pilot reduced the speed of transactions from three to four days with conventional payment processes, to three to four seconds.

Another problem with the region’s current payment processes is its high cost. CBDCs tend to be a cheaper alternative for customers. To encourage adoption of CBDCs among customers, one of the pilot projects provided heavily subsidized peer-to-peer transactions. Keeping these costs low—or lower than credit or debit cards—could be an

ongoing attractive feature of CBDCs.

The financial sector in the Caribbean seeks to move away from relying on brick and mortar establishments. Building financial services on top of improved digital banking could be a growth area for innovative banks. Beyond being responsible for stability, with CBDCs central banks will now have a role in encouraging economic growth and innovation. Early adoption of CBDCs in countries of the Caribbean suggest that having a Central Bank that serves as more than just a regulator is a successful approach. It has

resulted in innovation and new banking services becoming increasingly prevalent in those countries. A CBDC pilot program featured two different types of CBDC wallets. One for unbanked people and another for people who have bank accounts. For the banked customer, central banks worked with commercial banks and credit unions to offer CBDC wallets, which gave customers another option for their transactions.

Smartphone adoption is high in many Caribbean nations. Therefore, creating CBDC wallets accessible through smart devices helped these pilot programs meet financial inclusion goals. Wallets created for unbanked



## Efficiency

The CBDC pilot reduced the speed of transactions from three to four days with conventional payment processes, to three to four seconds.

people generally had a low balance but still allowed people to access financial transactions. One way to estimate the median low balance might be to draw on data about average, or minimum, wages in the region. Even though cash itself is not going away, having a secure alternative to an easily stolen wallet, for example, can be an attractive option.

Although much of the focus is on digital, the capability for payments made offline is also considered. Offline CBDCs are at an early stage of their development. And if, or when, they become a feasible proposition, they will require a different technical architecture than their online equivalents.

From both a regulatory and implementation perspective, regulatory sandboxes are a critical part of getting CBDCs right. By running pilot programs and having a regulatory sandbox, policy makers can identify clashes in certain policies as well as what aspects of implementation need tweaking to meet your policy goals. The value of learning by doing, before you commercialize CBDCs, is an important lesson learned from these pilot programs.

## 2. Using CBDC policy objectives to drive technology choices

Another important lesson learned is that the technical architecture of a CBDC depends on implementing government's policy goals. Focusing on financial inclusion, for instance, can require a different architecture than if the focus is on detecting and preventing illegal activities. There is no reason why one architecture cannot do both, but doing so has slightly different technical considerations.

There is no definitive answer for which technology to choose. Central banks choosing to build CBDCs on distributed ledgers can use a variety of distributed ledger technologies: public, private, or a mixture of the two.

In some cases, central banks mint CBDCs. Meanwhile, authorized financial institutions managed relationships with end customers. In this kind of two-tier technical architecture, customers don't have a direct relationship with central banks. Instead, they access CBDCs through intermediary payment providers, such as commercial banks.

In other cases, CBDCs leverage a private permissioned blockchain. In this approach, all the participants in the chain are known to the issuer, as opposed to a public blockchain, where the participants are pseudo-anonymous. *Admittedly, these permissions mean a slightly higher barrier to entry.* Nevertheless, the extra level of control gave people confidence that their

transactions were safe. It also allows for easier law enforcement and anti-money laundering controls where appropriate. Some argue for building CBDCs on top of a centralized database. As commercial banks are already using centralized databases, this makes it easier to integrate CBDCs into established financial solutions. Additionally, such architectures may be less vulnerable to cyberattacks than public distributed ledgers.

Interoperability is at a relatively early stage. Nevertheless, there are three main considerations for central banks: Is the CBDC system interoperable with other ones? Can you integrate it with traditional financial systems? And, could it work with other distributed ledger platforms, such as public blockchains?

Therefore, basing the technical architecture on your policy objectives is a recipe for success.

The implementation of CBDCs is an iterative process. As one of the workshop participants said:

**“ You will not know everything upfront, and the external consultative process helped inform how we go about designing and what features we design now, vis-à-vis what we build later on.”**

### 3. Agile CBDC development with cloud technology

Cloud services support an agile CBDC development. Leveraging new technologies, such as cloud, enables governments to mitigate the large upfront infrastructure investment such a system would necessitate, according to workshop participants.

In order to provide continuous service—a prerequisite for financial stability—a CBDC system has to be scalable, resilient, and secure. Cloud infrastructure, in particular, has a high level of availability and provides features necessary to deploy a resilient IT architecture. Cloud infrastructure is designed to tolerate system or hardware failures with minimal customer impact.



#### Security

Shared concerns about security are one of the reasons why cloud services are especially useful as the basis of launching and maintaining CBDCs.

Cloud services are deliberately designed to be secure, resilient, and scalable. Through their cloud consoles, central banks can deploy cyber hygiene best practices across the services they use. Resistance to counterfeiting, as well as data encryption both in transit and at rest, appropriate access controls and authentication methods are a shared responsibility.



#### Resilience

Cloud infrastructure is resilient to operational failures and other disruptions. Their network consists of servers across several geographic regions, with multiple availability zones within each region, and, in some cases, multiple data centers within each availability zone. This allows for data to easily be replicated and functionality redirected in case of a local system failure. As cloud services have automated data backups and can restore data, this reduces the risk of important information being lost.



#### Scalability

Workshop participants emphasized the need for scalability in CBDC solutions. Payment service providers and customers expect that their transactions will be processed instantly or near instantly. Fortunately, scalability is a particularly strong feature of cloud services. CBDC system providers will pay for what they use, and services scale automatically to meet increased or decreased demand.



#### Confidentiality and control

Beyond the three considerations listed above, workshop participants described a shared belief in the importance of confidentiality. In the cloud, customers own and control their data. This means a few different things in practice. Cloud service providers do not move data without customer consent. Customers decide where data should be stored, and they can download and delete data when they want to. Who can or can't access data is an especially important consideration for sensitive data, such as financial transaction histories. Customers can revoke access to data through eliminating encryption keys. If you revoke a key, it will no longer decrypt the relevant information.

Customers also choose how they want data to be treated. Depending on sensitivity, customers choose whether to encrypt non-sensitive data in transit, and encrypt sensitive data both in transit and at rest.

## 4. Increasing CBDC adoption through stakeholder engagement

The pilot programs reviewed during the workshop showed that adoption of CBDCs is a chicken and the egg problem. Merchants may be hesitant to allow payments with a new type of currency unless it is widely used. Early adopters aside, individuals might not see the point of getting a CBDC wallet. [Beyond marketing campaigns aimed at both consumers and merchants, pilot projects indicate that early adoption of CBDCs by merchants whose goods and services were part of people's everyday lives is important for success.](#)

Participants highlighted the importance of including government institutions as users in CBDC pilots. The government is normally the biggest mover of cash in any economy. The same applies with the CBDC. Without the government as a stakeholder, ensuring that it is actively adopting the currency, it will be difficult to have a wider reach.

Another lesson learned is that piloting smaller international blockchain initiatives prepared the ground for national CBDCs. Even though they acknowledged the costs associated with trialing new forms of payment, they argued this could be offset by the lower cost of running such payment systems once live.

A third lesson learned is that whenever you're trying something new, you need to manage the story around it. CBDCs are no different. Consistent, ongoing messaging is part of building trust in CBDCs. Citizens need to know about the launch and when the pilots are live.

Feedback from the pilot projects suggest that most consumer questions about CBDCs involve security and privacy. Address some of the customer concerns by showing that CBDCs, just like cash, are issued by central banks.

## Some lessons

### [A]

The government is normally the biggest mover of cash in any economy. The same applies with the CBDC. Without the government as a stakeholder, ensuring that it is actively adopting the currency, it will be difficult to have a wider reach.

### [B]

Another lesson learned is that piloting smaller international blockchain initiatives prepared the ground for national CBDCs. Even though they acknowledged the costs associated with trialing new forms of payment, they argued this could be offset by the lower cost of running such payment systems once live.

### [C]

A third lesson learned is that whenever you're trying something new, you need to manage the story around it. CBDCs are no different. Consistent, ongoing messaging is part of building trust in CBDCs. Citizens need to know about the launch and when the pilots are live.



### CBDC objectives

It's also worth sharing with the general public the tangible goals central banks are trying to achieve through issuing a CBDC. These can include security, financial inclusion, and making payment processes reliable, fast, performance efficient, and more cost effective.

Central banks and other financial institutions need to dispel myths about digital currencies giving governments granular insights into people's spending habits. Explaining the difference between privacy and anonymity can be a helpful angle. As one participant said:

**“ We do recognize that there is a strong level of privacy within our CBDC. However, there is not anonymity. We try to make sure that the public is educated about that.”**

It's also worth sharing with the general public the tangible goals central banks are trying to achieve through issuing a CBDC. These can include security, financial inclusion, and making payment processes reliable, fast, performance efficient, and more cost effective. Clarifying that CBDCs are intended as a complement to cash and credit card transactions, not a replacement, can also be helpful.

Retail and commercial banks might be concerned about the implications of central banks dealing directly with customers. However, the CBDC pilot projects demonstrated how closely central banks were working with authorized financial institutions. Central banks would mint, receive and distribute CBDCs wholesale. Onboarding digital currency users, distributing CBDCs, and offering related services in the pilots sat with authorized financial institutions. The financial institutions could also market how and why CBDCs can be valuable to individuals and businesses. Retail banks should also be reassured that by limiting the CBDC transactions individuals can perform monthly, CBDC will not compete with larger scale real time gross settlement (RTGS) payments.

These pilot projects are a good way to show, rather than tell, how CBDCs fit into existing banking relationships. As one speaker said:

**“ Success requires public-private partnerships. We cannot do this on our own. We need partnership. It needs to be the government involved; it needs the financial institutions, the merchants. It requires an all-in effort for it to be successful. It cannot be done just by the central bank.”**



## 5. Removing legal hurdles while maintaining regulatory standards



**61%**

of central banks can only, legally, issue banknotes and coins.



**16%**

of central banks, the law is not clear if the central bank is authorized to issue other financial instruments, beyond banknotes and coins.

Competing policy objectives are a feature of regulatory work. How do you minimize the negative implications of a new instrument while maximizing the positive? Regulators must be clear about the importance of governance and risk management while respecting and acknowledging the excitement about the promises of CBDCs.

Most importantly, introducing CBDCs does not mean waiving regulatory standards. Regulators should examine which existing laws and regulations apply to CBDCs. As one workshop participant put it, “same animal, different cage.”

Data from the International Monetary Fund shows that many countries will need to revise their laws to make CBDCs legal tender. Today, 61 percent of central banks can only, legally, issue banknotes and coins. For the other sixteen percent of central banks, the law is not clear if the central bank is authorized to issue other financial instruments, beyond banknotes and coins.

A risk of any new payment technology is that it can be

abused to support illegal activity, such as money laundering or terrorism. The pilots showed central banks managing these risks in different ways. It was exciting to see know your customer (KYC) modules integrated into pilot platforms. KYC is a mandatory process of identifying and verifying the client's identity when opening an account and periodically over time. Additionally, there is optimism that issuing CBDCs will open up new ways to monitor illicit activity.

Notably, even though distributed ledger technologies were originally associated with decentralization, one presenter said that central banks are likely to keep their roles as organizers and governance bodies.

One of the questions around CBDCs is how they might affect the risk of currency substitution (also called dollarization). Although some speakers expressed uncertainty about this, others considered CBDCs the best bet for central banks trying to avoid national currencies being undermined by public ledger-based digital currencies such as stablecoins.

Most importantly, introducing CBDCs does not mean waiving regulatory standards. Regulators should examine which existing laws and regulations apply to CBDCs.

# Case study: Learnings from the ECCB DCash Pilot

The Eastern Caribbean Central Bank (ECCB) is the monetary authority of the Eastern Caribbean Currency Union (ECCU). A multi-currency union, it encompasses Anguilla, Antigua and Barbuda, Commonwealth of Dominica, Grenada, Montserrat, St Kitts and Nevis, Saint Lucia, and St Vincent and the Grenadines.

The DCash pilot, which began in early 2019, launched in all of the member nations in 2020. In response to the COVID-19 pandemic, the ECCB expanded the original pilot from four countries to include all eight. They also extended the planned timeline for the pilot project from six to twelve months, to gather more data on its implementation.



## CBDCs and their potential to drive progress

One of the ECCB's policy aims for DCash was to create efficiencies in cross-border payments in the ECCU. Beyond addressing the cost, speed, and security of transactions, for the pilot project, scalability and ownership of data infrastructure were also important considerations. Even though the ECCB is not trying to eliminate physical cash, it hopes to see a 50 percent reduction in the use of cash by 2025.

Globally, financial institutions are moving away from brick and mortar establishments. Providing a platform that allows for innovation and competitiveness across the region was a motivating factor behind the DCash pilot.

Financial inclusion was another policy aim for the pilot project. Banking charges across the ECCB tended to be high. An affordable digital payment solution would mean that the ECCB could include people who would have otherwise been excluded. Accessibility is an important aspect of financial inclusion. Based on recent research in the ECCU, smartphone penetration is extremely high (above 100

percent, as some people have several devices). Having DCash available via smartphone therefore meant the ECCB was able to meet their financial inclusion goals for the pilot.

To do that, the ECCB piloted two kinds of digital wallets. One was aimed at people who already have bank accounts. They would onboard through their financial institutions, either a credit union or a commercial financial institution. For these users, DCash became another option for transactions.

The ECCB also developed a type of digital wallet aimed at people who do not currently have a bank account. These DCash wallets have low limits, set according to average wages across the ECCU and are therefore aligned with average spending.

To meet the financial inclusion objective, the KYC requirements were relatively low. To prevent money laundering the ECCB used existing compliance platforms to allow for enhanced fraud protection.

These two types of digital wallet were first rolled out across four countries, with planned launches across the remaining four nations later in 2021.



## Using CBDC policy objectives to drive technology choices

The ECCB decided that the technology used for DCash would be led by the policy objectives above. The ECCB also wanted DCash to be as cash-like as possible, which in turn influenced technical decisions about privacy, resilience, access, and security. Beyond those concerns, the technical architecture also took into account governance, operational arrangements and protocols.

The DCash pilot was built on a robust, private permissioned blockchain infrastructure. Importantly, the ECCB knows who network participants. The presenters from the ECCB argued that, by maintaining this element of control, people using DCash would be confident that their transactions were safe. In that way, DCash would evoke the comfort and trust people have in a sovereign currency.

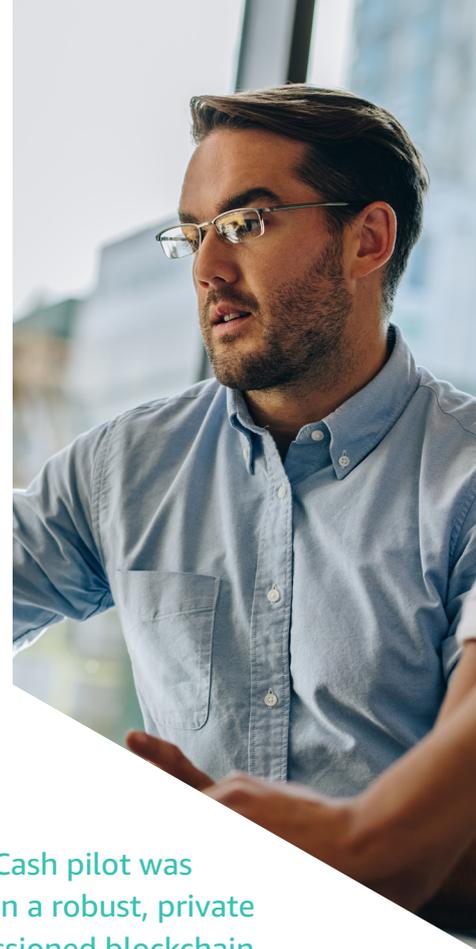
The ECCB designed the pilot architecture to allow authorized third parties to ensure service assurance and fulfillment for merchants and end users. The

ECCB distributes and issues DCash to financial institutions for onward distribution to the public. Financial institutions play a critical role.

Working with existing financial market infrastructures meant figuring out how to work with them to deliver the pilot. The ECCB had to decide what level of interoperability or integration they needed. This included tradeoffs between creating a dedicated independent network while ensuring the integrity of the financial system. This resulted in a DCash pilot network that ran parallel to core banking systems.

Even though multiple entities participated in the permissioned network, the ECCB remained the sole entity able to issue and revoke network access. They operated in a controlled live environment under the strict control and supervision of the central bank. Only approved entities could take part in the pilot project.

DCash also needed to execute frictionless peer-to-peer payments. This system needed to be stable so it could be used alongside cash. This informed the ECCB's decision to not make the DCash pilot interest bearing.



**The DCash pilot was built on a robust, private permissioned blockchain infrastructure. Importantly, the ECCB knows who network participants.**



## Agile CBDC development with cloud technology

The ECCB chose to depend fully on cloud services rather than creating a hybrid physical and cloud infrastructure. This accommodated the need for control, disclosure, cyber resilience, and data privacy. It also allowed the ECCB to manage costs, and helped with DCash adoption across multiple jurisdictions.

All DCash data is encrypted at rest and in transit. The ECCB only has independent data stores when dictated by existing regulatory frameworks.



## Increasing adoption through stakeholder engagement

The pilot showed the importance of having a compelling value proposition for all DCash stakeholders: financial institutions, merchants, end users, and government agencies.

The consultation period gave the ECCB time to develop these propositions and bring stakeholders along with them. Beyond communications, consulting with financial institutions informed the procedures and risk management requirements.

The ECCB worked with financial institutions and payment service providers who use the back-end systems to meet internal requirements. The ECCB also considered the potential for future-proofing the banking systems, ensuring that the new payment infrastructure for the financial system can adapt to technological change.

Education and training were a significant part of the success of the pilot. Financial institutions offered DCash to their staff first so they would be familiar with the technology before offering it to the public.

Public education and awareness were also important. Three points were particularly worth explaining to end-users.

### Firstly,

that people can always update their information. The ECCB underscored that funds are stored on the blockchain; people can recover their funds if they lose their phone. The ECCB also explained to customers that there is a process to recover forgotten passwords.

### Secondly,

the ECCB shared the policy reasons behind why they were running the pilot.

### Thirdly,

it was important to show how using DCash can benefit end users.

Striking a delicate balance between encouraging adoption by merchants first or consumers first, the ECCB chose to target both groups with marketing campaigns.

Including merchants who provide essential services proved to be a successful strategy for the pilot program. The private sector enables transactions: If there's no way to spend Dcash, then customers won't use it.

In particular, merchants who provide essential services like supermarkets, gas stations, pharmacies and bakeries, showed consumers that they could use a CBDC for small payments. This allowed consumers to feel comfortable using CBDCs in the same ways

they would normally use cash. Addressing concerns about the privacy of transactions was another theme of the pilot. Citizens were worried that the central bank would be spying on them. This is not the case, as transactions are encrypted end-to-end. To preserve privacy, the minting system was independent to the rest of the DCash systems, and ran on an offline system. The ECCB requires financial institutions to continue anti-money laundering monitoring; there are certain triggers in place for DCash, but this is already a feature of regular transactions.

The ECCB included a guaranteed conversion of DCash back to cash or account balances. This removed potential concerns that people would be left with DCash that they couldn't use or that they risked losing money if converting back to cash.

The pilot process showed the value of iterative feedback. Throughout its implementation, the ECCB did surveys and held consultations with stakeholders. Through these, the ECCB was able to identify features that needed improvements or needed to be added to improve the overall user experience.



## Removing legal hurdles while maintaining regulatory standards

There were no regulatory waivers for DCash financial products.

Making it explicit that central banks can issue CBDCs as legal tender is an important step for taking digital currencies beyond a pilot stage. The ECCB therefore amended their agreement to explicitly list digital in the definition of currency, making it legal tender.

The ECCB discovered gaps in regulations on data protection and privacy legislation in certain member states. To compensate for these gaps, a design that included data protection was pivotal in the DCash pilot. There is no single repository of customer KYC information for DCash, and it is not stored on a ledger. Instead, each financial institution or agent is responsible for onboarding customers, and they store KYC data on their own databases.

Ease of adoption for financially excluded people was an important goal for the ECCB. As described above, the financial institutions complete the KYC verification process to approve wallets. Even though the onboarding process is not as stringent as for other services, the lower value limits, enhanced anti-money laundering functionalities, and risk assessment of DCash as a new product ensured compliance to existing laws. Additionally, a customer can only have one value-based account.

In support of anti-money laundering efforts, all customers on the DCash network are known by the ECCB and the financial

## Making it explicit that central banks can issue CBDCs as legal tender is an important step for taking digital currencies beyond a pilot stage.

instructions and transactions immutable. This makes both investigation by law enforcement and monitoring identification of suspicious transactions easier. Keeping the cost of compliance low was another objective of the pilot project. DCash therefore has different levels of authorization within financial institutions. These would typically be set up based on the bank's existing protocols. The banks would then conduct product risk assessments to ensure they were compliant with existing KYC and anti-money laundering protocols.

Even if the ECCB stores data associated with DCash, it is encrypted at rest and in-flight. Only financial institutions can access customer information. In cases where the ECCB, regulatory bodies or law enforcement agencies wish to investigate, they have to go through financial institutions (as is the case today).

The principle of no waivers of regulatory standards for DCash applied to the ECCB itself, too. The same multi-factor authorizations required for the minting, issuance, distribution, and destruction of physical notes and coins apply to DCash. Similarly, there were no waivers for international financial reporting standards.

# Next steps for DCash



## Step one

During the COVID-19 pandemic, the ECCB has seen an increased demand for digital payment solutions. They have used this as the impetus to add an ecommerce component to DCash. Merchants who offer online payment services can now have DCash as a payment option or can use APIs to issue invoices.



## Step two

Evidence of the success of the pilot projects, DCash transactions are settled in three to five seconds, as opposed to three to five days for some other payment channels. At times, longer latency can occur, but it is generally the result of connectivity issues.



## Step three

Before going to full commercial implementation, DCash systems will also need to be fully integrated in existing systems. It's not really feasible to ask businesses or financial institutions to run parallel systems in the long term. Therefore, the next stage will include testing what aspect of DCash that the ECCB needs to integrate with other solutions to make it a sustainable part of the payment ecosystem.



## Step four

Bringing along more stakeholders could increase and widen adoption. If governments were to use DCash as a payment method, for example to pay welfare benefits, this would increase adoption.

## Workshop summary

Wrapping up two days of fruitful conversation, Xiaochen Zhang, principle manager, federal financial, worldwide public sector at AWS, emphasized the value of bringing together a host of perspectives and experiences from different countries and regions.

Piloting and launching CBDCs is an exercise in technical innovation, managing risk, and taking an iterative approach to policy making. Regardless of which technology options central banks choose, using cloud services reduces costs and gives access to advanced analytics features.

Learning from others—be it colleagues in different countries or technology partners—is a way to mitigate risks and maximize the chance of success. Several speakers mentioned the effects of the COVID-19 pandemic on the pilots. For instance, some of the face-to-face stakeholder consultations and training sessions, which would normally be part of pilot programs had to either be paused or done remotely.

That said, revamping pilots in the face of changing circumstances can also lead to new insights. These range from clarifying the need for alternatives to cash, or noticing that the scope and timing of a pilot might need to change to test how much friction could be reduced in cross-border payment systems.

Data from other pilot projects will contribute to a better understanding of how CBDC could be designed. They will share important lessons in how central banks could contribute to and support the payment habits and needs of merchants and consumers.

Beyond taking a collaborative approach, the workshop was a testament to the importance of central banks taking a controlled and considered a learning by doing approach to CBDCs. AWS will continue to convene experts from all over the world in supporting central banks' digital transformation journey.

For additional information, see: [AWS Central Bank Digital Currency Whitepaper](#) › [AWS Caribbean CBDC Workshop](#) ›

The AWS federal financial international team enables our public sector financial and multilateral institution customers to achieve their missions of economic development, inclusion, risk oversight, consumer protection and financial and monetary stability. We enable the enablers to harvest green finance, digital currency, and open innovation related opportunities and collaborate with partners to drive for transformational impacts.

For more information, please contact Xiaochen Zhang at: [awsfedfin@amazon.com](mailto:awsfedfin@amazon.com).

