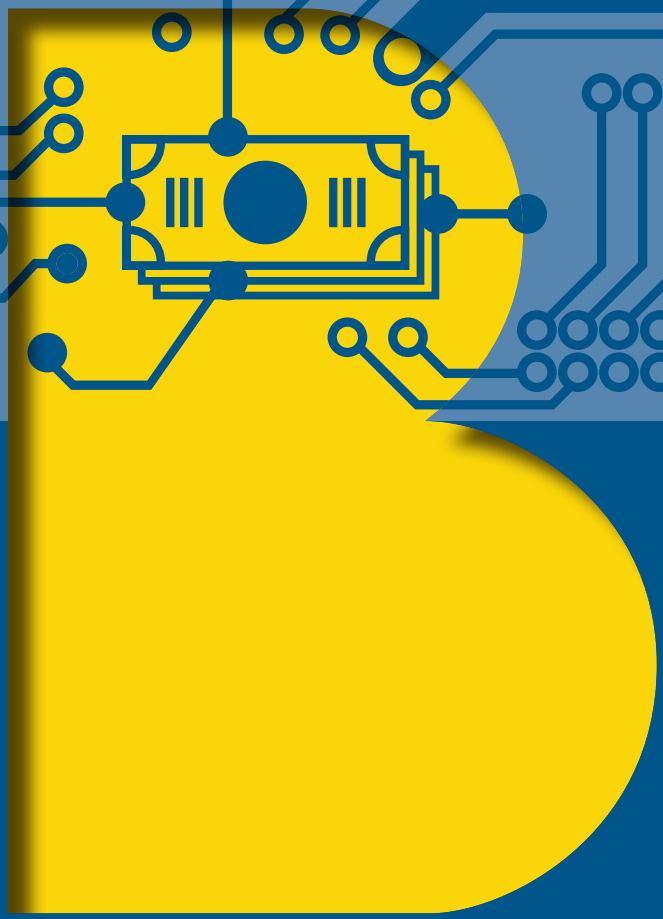
Think:Act

navigating complexity

PART 3



September 2017

Central banking IT of the future

New realities in central banking

Roland Berger

50 years

navigating complexity

THE BIG 3

INTERVIEW WITH JONATHAN DHARMAPALAN ON DIGITAL CURRENCY
→ P. 18

30-40%

of total staff at central banks is likely to be working in IT in 2025.

Page 5

100%

cybersecurity will never be possible for central banks – it is an organizational challenge that goes beyond IT.

Page 6

3

levers to close the gap between the perceived strategic importance of IT and its true future significance.

Page 20

Central banking 2.0

Recent technological developments are changing the mandate of central banks.

The IT functions of central banks have undergone major transformation in recent years. The need to gradually increase capabilities, combined with ever shorter technological cycles, compels banks to be in a state of constant readiness. Indeed, for many central banks in countries around the world, simply keeping up with the rapid pace of change is a challenge.

In the first two parts of this series – New realities in central banking: The organizational challenge and The rise of cryptofinance – we saw how the financial services sector is changing. Innovative FinTech companies are threatening commercial banks' traditional value chains and the danger of disintermediation is forcing incumbents to react. Cryptocurrencies such as Bitcoin are making headlines, and blockchain technology is widely seen as having the same disruptive potential as the internet. Cybersecurity has moved from being a minor headache for IT departments to heading the World Economic Forum's annual risk report.

These new realities affect central banks in a number of ways. The complexity of fulfilling their current mandate has increased dramatically, with almost every field of activity now affected by technological change. At the same time, their mandate has expanded, with new market participants and alternative payment systems needing to be regulated and supervised. Add to that the fact that the pace of technological change is set to increase over the coming years, and it is clear that central banks need to improve their ability to react quickly to the new realities. → A

The IT organizations, systems and infrastructure of many central banks are not yet fit for purpose. While commercial banks, insurance companies and other market participants have made considerable efforts to digitally transform their business models in recent years, often forming partnerships with technology providers and innovative start-ups, central banks have not yet prioritized the digital transformation of their organization. As a result, the level of maturity of their IT departments varies greatly. Some central banks have successfully embarked on the journey to transform their IT departments into proactive business partners with a clear strategic mandate, but many have not yet dedicated the necessary top-management attention and resources to prepare themselves for the road ahead.

A

TECHNOLOGICAL DEVELOPMENTS AFFECT THE MANDATE OF CENTRAL BANKS

Assessment of impact on core tasks of a central bank.

CORE TASK	IMPACT	
Implement monetary policy		Digital currency offers new instruments for implementing monetary policy
Monitor financial stability		Cyber risks are a tremendous threat to financial stability
Manage assets		Trading and portfolio management applications and systems are becoming more sophisticated
Supervise payment systems		Central banks also need to supervise alternative payment systems
Publish statistical data		Big Data creates new opportunities for analyzing statistical data
Issue banknotes and coins		Digital currency will complement physical cash
Supervise financial institutions		Central banks need new capabilities to supervise financial institutions

Source: Roland Berger

A STRATEGIC PERCEPTION GAP

Our ongoing dialog with industry insiders reveals a major gap between the perceived strategic importance of IT within central banks and its true future significance. IT departments at central banks have been growing in size and importance over the last decade and will continue to do so in the future. By 2025, we expect to see 30 to 40 percent of central bank employees working in IT. The gap between the current perceived strategic importance and true future significance puts central banks at substantial risk with regard to their ability to effectively fulfill their future mandates. This is a strategic perception gap that needs to be urgently addressed. → B

The increasing pace of technological development calls for a broader range of IT capabilities and more agile IT organizations in central banks. The rise of game-changing technologies has a different impact on different parts of the organization, from enabling marginal process improvements to causing truly disruptive change. Central banks need to be at the forefront of technological developments, intensifying the dialog with technology providers and exchanging know-how with other public institutions, learning from each other and sharing best practices.

FOUR AREAS OF CONCERN

We interviewed a large number of IT department heads at central banks, industry experts and entrepreneurs and asked them about their major areas of concern with regard to the future of central banks. Their answers all revolved around similiar topic clusters. In particular, they raised the following issues:

1. Cybersecurity: Rapid developments in technology and increased cooperation with third parties have created new threats that central banks need to address proactively

2. Process automation: Central banks can increase their effectiveness and agility by further automating and digitizing core and support processes

3. Cloud solutions: Leveraging cloud solutions reduces central banks' need to build and operate their own datacenters, as well as granting them access to the vast security experience of cloud providers

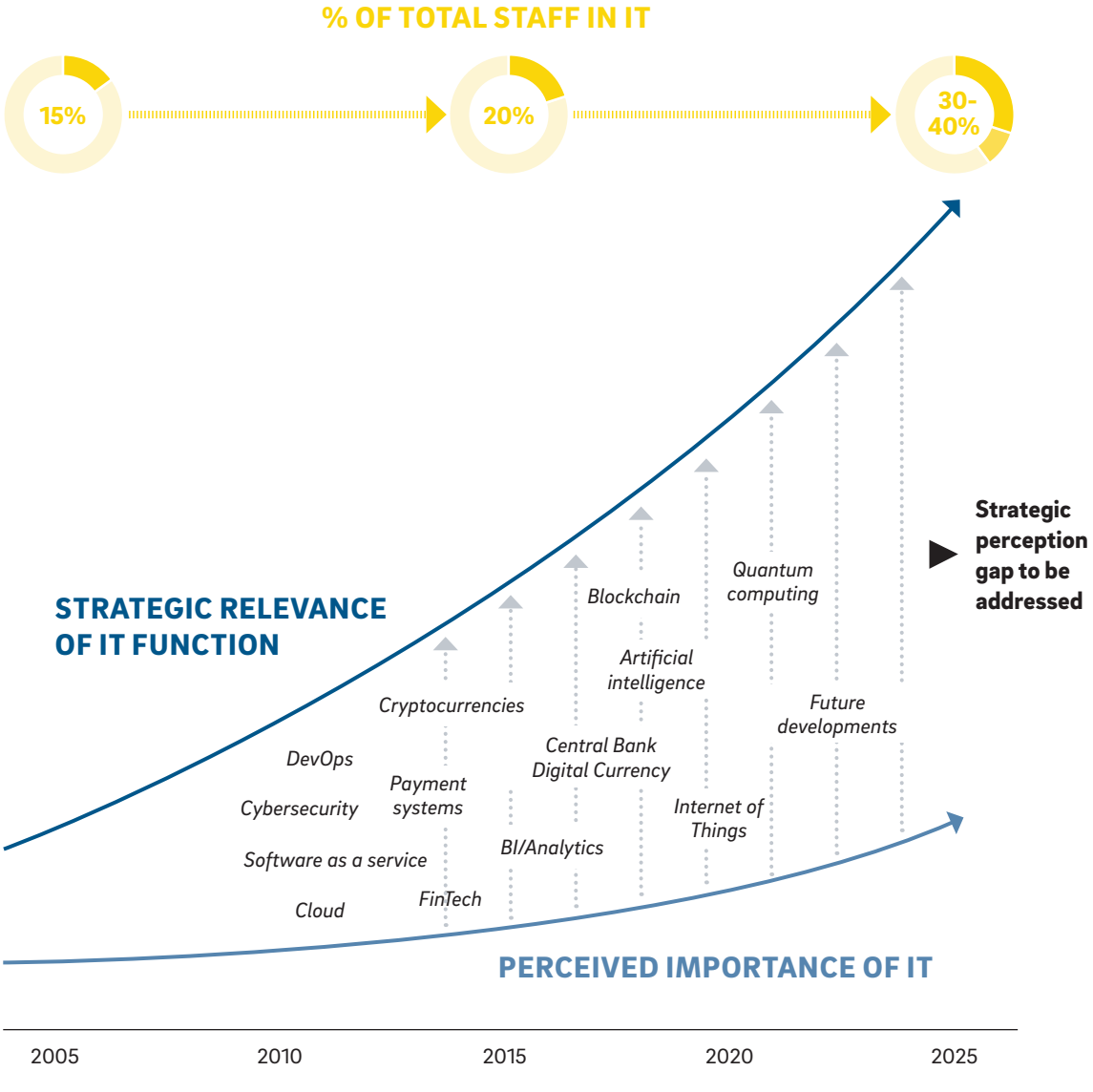
4. Digital currencies: Introducing a digital currency is a complex undertaking and involves a variety of internal and external stakeholders

We scrutinize each of these areas of concern in the following pages.

B

STRATEGIC PERCEPTION GAP EXPECTED TO WIDEN

The strategic relevance of the IT function is expected to grow: a fact that has to be recognized by central banks



Source: Roland Berger

1. Cybersecurity
New technologies open the door to new threats.

Cyberattacks have been making headlines in recent years. They cost businesses between USD 400 and 500 billion a year – and that is just reported cases. They are also part of the new reality for central banks. The last 24 months have seen various attacks by hackers and cyberterrorists aimed at central banks, placing the topic right at the top of the agenda for governors. → C

Most notably, in February 2016 hackers were able to steal USD 81 million from Bangladesh Bank using the SWIFT messaging network. The hackers initiated transfers of almost USD 1 billion from the bank's account at the Federal Reserve Bank of New York. Although a large proportion of these transfers were rejected, USD 81 million was ultimately transferred to bank accounts in the Philippines. This money was then laundered via the local casino industry (see case study).

Cyberattacks can take various forms, the most common of which are distributed denial of service (DDoS) attacks, malware, advanced persistent threats (APTs) and ransomware. As the pace of technological development increases, so does the rate at which new threats emerge. The ability to detect attacks quickly and build resilient systems and structures thus becomes paramount.

Central banks and financial infrastructure providers have taken various steps in the recent past to face these challenges. For example, the Committee on Payments and Market Infrastructure (CPMI) of the Bank for International Settlements has set up a taskforce to strengthen cybersecurity in payment systems. The Bank of Italy has set up a cybersecurity response team in collaboration with the Italian Banking Association. Similarly, the Bank of England is partnering with cybersecurity firm Anomali to collect, integrate and investigate cybersecurity intelligence data. And the Hong Kong Monetary Authority (HKMA) has launched a Cybersecurity Fortification Initiative to develop cybersecurity training and certification programs.

Despite these efforts, the rapid pace of technological change means that 100-percent cybersecurity will never be achievable. As the hackers and attackers build up skills, so must the security experts at central banks. Capabilities and systems need to be upgraded in order for the banks and third-party providers in their extended network not to open themselves up unnecessarily to the risk of attack. → D

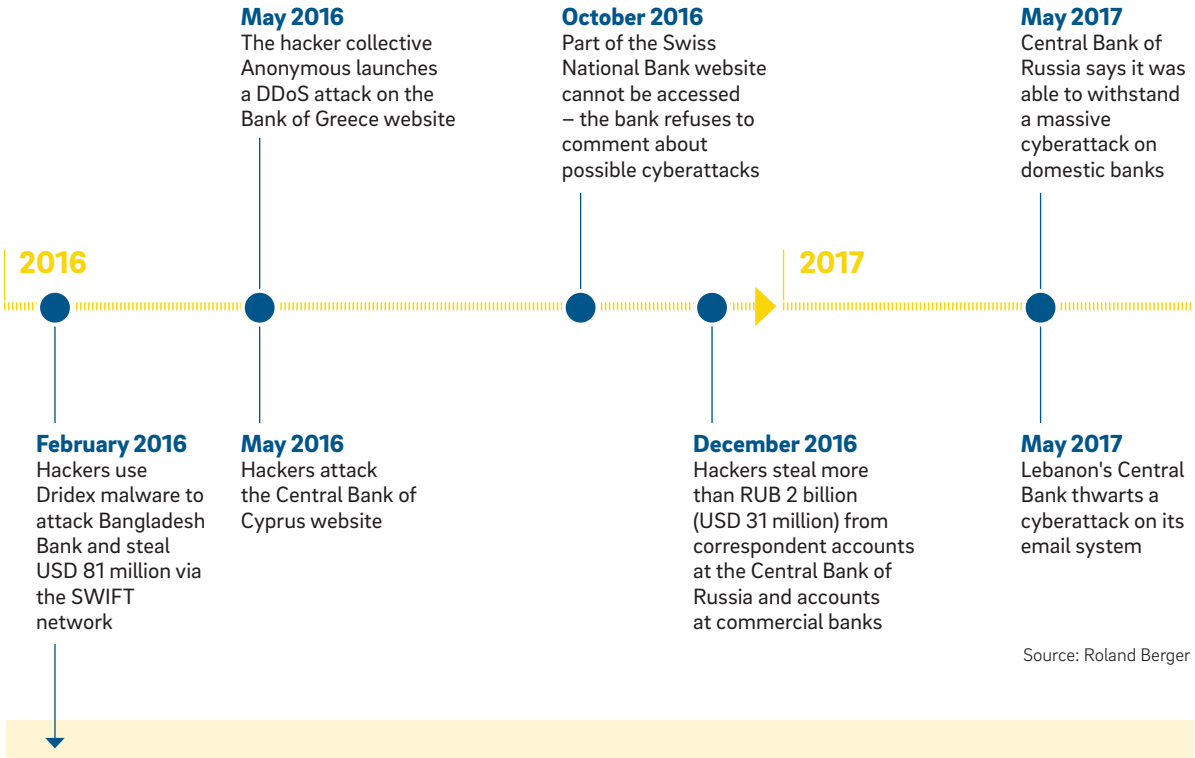
THE ELEPHANT IN THE ROOM: HUMAN ERROR

Systems, processes, policies and tools play a crucial role in strengthening cybersecurity. But cybersecurity is not just a technical problem: the human factor is paramount. A study by IBM reveals that as many as 53 percent of security breaches in financial services in 2016

C

BELIEVE THE HYPE

Central banks have been subject to a wide array of cyberattacks in recent months – attacks are expected to continue and intensify.



Source: Roland Berger

CASE STUDY: **Cyberattacks on the SWIFT network**

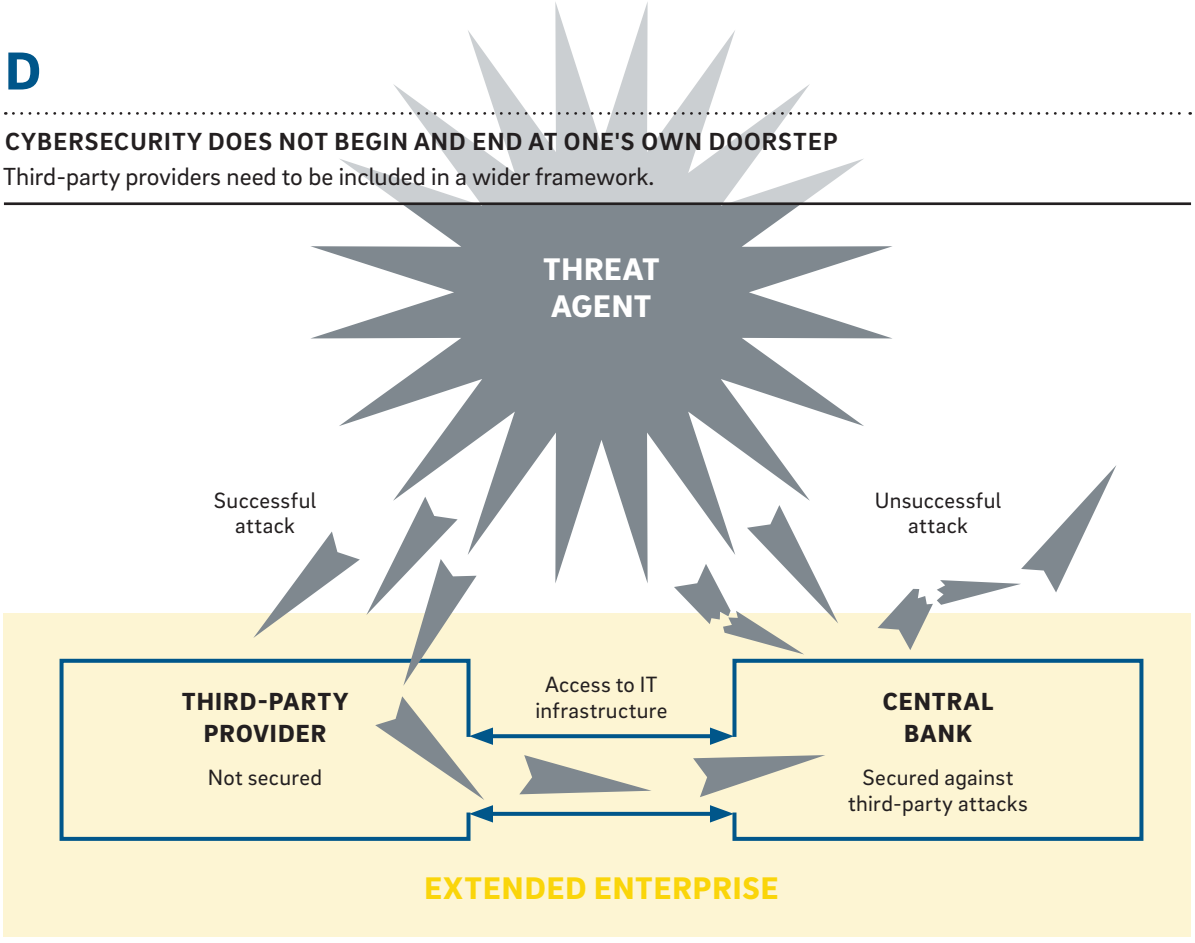
In early 2016, one of the biggest cyberattacks to date took place. Unknown attackers hacked Bangladesh Bank's SWIFT messaging system and instructed the Federal Reserve Bank of New York to transfer funds from the Bangladesh Bank account there to accounts in the Philippines and elsewhere. The attackers attempted to transfer USD 951 million, of which USD 81 million could not be recovered. The attack is significant because it was the first attack on this scale.

The same modus operandi has been used in two other cases, one involving the Sonali Bank of Bangladesh and the other Banco del Austro in Ecuador. The SWIFT messaging network was not compromised in either of these attacks but the customer's environment was breached and credentials were used to send fraudulent messages via the SWIFT network. SWIFT reacted to these cases by launching its Customer Security Programme (CSP), which all participants in the SWIFT network must comply with.

D

CYBERSECURITY DOES NOT BEGIN AND END AT ONE'S OWN DOORSTEP

Third-party providers need to be included in a wider framework.



Source: Roland Berger

"Cyber defense is by no means a trivial matter. In the Middle Ages, it was relatively easy to defend castles by building moats and fortresses. And it was mostly clear from what direction the enemy – often the same enemy – would advance. The reality of IT is a different matter altogether. Enemies are unknown and almost never come out into the open. In some cases, professional hackers hide for months on end within a company's fortress walls."

DR. ANDREAS DOMBRET
Member of the Executive Board of the Deutsche Bundesbank (March 2017)

were due to mistakes made by people within the organization, 42 percent were due to attacks from outside, and 5 percent due to attacks from inside the organization.

Human error includes wrongly addressed emails, stolen devices, leaked passwords, confidential data sent to insecure home systems, and identity theft due to malware or phishing attacks. The best way that central banks can address this is to embed cybersecurity within the organizational DNA, making it a matter of priority for each and every employee within the bank. A study carried out by the Ponemon Institute and IBM shows that employee training has the greatest impact on reducing the cost per cybersecurity breach.

SETTING UP A CYBERSECURITY FRAMEWORK

Strengthening a central bank's "cyber resilience" is a complex task that covers a variety of different aspects. While there is no one-size-fits-all solution, the most relevant aspects to be considered are as follows:

STRATEGY: A cybersecurity strategy should define objectives, priorities and acceptable risk levels (for example, internal emails do not need the same level of security as the website).

ORGANIZATION: Best-practice central banks have a central cybersecurity function within the IT department, its responsibilities clearly separated from those of the IT line function (for example, the central function is responsible for policy-setting and controlling, the IT line function is responsible for policy implementation).

GOVERNANCE: Various governance-related factors must be considered, including top-management visibility, allocation of responsibilities, use of a risk-based approach, availability of critical resources, clearly defined policies, and defined and monitored KPIs.

PROCESSES: The cybersecurity function needs to be involved in projects – almost every project has an IT element and therefore implications for cybersecurity.

CAPABILITIES: Strengthening cybersecurity requires a specific skills set. State-sponsored hackers are continuously developing new kinds of threats. Within organizations the role of the CISO (Chief Information Security Officer) is crucial.

TOOLS: Monitoring tools must display the right balance of complexity and user-friendliness. They should be integrated into the overall architecture to help the CISO monitor and address risks.

CYBER RESILIENCE IS A MAJOR PART OF FINANCIAL STABILITY

Cyberattacks can potentially compromise major participants in a country's financial system and significant market infrastructure. They represent a major threat to the financial stability of a country. Central banks that take on the role of regulator in their jurisdiction therefore need to pay particular attention to building up cybersecurity capabilities. First, central banks need to ensure that their own organization is resilient. Second, in order to supervise and enforce their own cybersecurity regulations they need expert know-how that is up to date with current threats. They should complement this with an effective methodology for conducting assessments and deriving implications with regard to strengthening cybersecurity. One country that has done this effectively is Ireland: the Central Bank of Ireland has its own Banking IT Risk Inspection Team that scrutinizes systems and identifies any cybersecurity risks.

2. Process automation

Digitization and end-to-end optimization makes central banks more efficient and more agile.

In Part 1 of this series – New realities in central banking: The organizational challenge – we saw how, in order to become leaders and shapers in the global financial system, central banks are called upon to become profoundly efficient organizations, able to attract top talent and build up the capabilities necessary to assess the opportunities and threats posed by new technologies. In this third part of the series we focus on how central banks can use IT to achieve the goal of organizational efficiency, speeding up their reaction times and decision-making processes.

Central banks always have, and always will, put the effective implementation of their mandate first. They avoid operational risks at any cost. After all, what is the point of a small gain in efficiency if it has dramatic implications on a systemic level? But while cost awareness can mean cutting certain activities or reducing staff in individual departments, it can also mean focusing on efficient core and support processes.

Central banks often rely on processes that involve many manual steps, making them slow and prone to error. Furthermore, a lack of process automation and digitization frequently leads to overlaps between different processes, which uses up valuable resources. By systematically automating core and support processes, they can increase the efficiency but also raise the quality of their output. This allows them to shift the freed-up resources to other strategic priorities, and in so doing further strengthen and develop the organization. At the same time, employees' job profiles become more interesting, with an increased focus on conceptual and analytical work and less manual work. → E

When it comes to process automation, central banks have a wide range of opportunities, from end-to-end optimization of statistical data processing, incident management, document and access management, employee onboarding and testing of applications, to document management, publication of papers and content automation on the website.

PROCESS AUTOMATION – A SYSTEMATIC APPROACH

Moving from manual to automated processes cannot be an isolated endeavor. In certain cases, it will indeed be advisable to bring in external specialists to teach best practices, introduce tools and train staff, but this is not a sustainable solution.

What central banks need is a state-of-the-art process management system and a dedicated organizational unit to serve as a sparring partner for process owners. The unit should also ensure proper documentation and a standardized approach to mapping processes. Furthermore, it should promote a mindset of continuous improvement and encourage process owners to be innovative and think across departmental boundaries.

By employing a systematic approach to process automation and optimization, central banks can not only increase their operational efficiency but also transform their IT organization into a more agile function that can swiftly respond to changes in the technological environment and cooperate effectively with external partners.

E

TRANSFORMING CENTRAL BANKS INTO AGILE ORGANIZATIONS

Three case studies which show potential implications of process automation.

1. Statistics

Collecting, analyzing and publishing statistical data forms part of the core mandate of central banks. Best-practice central banks systematically optimize the cross-functional process end to end, as a variety of technical departments (such as Application Management) and functional departments (such as Statistics) are involved in the process. Taking this joined-up perspective enables central banks to reduce the number of interfaces, optimize workflows and minimize the number of applications and databases used along the process. An example of a central bank putting this into practice is the Swiss National Bank, who have optimized their statistics processes end-to-end with horizontal process responsibility and a dedicated website with data useful for monitoring developments in the financial sector and monetary policy (see https://data.snb.ch/).

2. Incident management

The traditional role of a service desk in an IT department is to fix incidents submitted by end users via telephone or a ticketing system. While in some instances it is crucial that incidents are escalated and resolved with the help of service desk staff, new technologies and tools allow incidents to be automatically diagnosed, categorized and managed. Our work with clients shows that introducing automated incident management processes reduces manually managed incidents by more than 40 percent.

3. Document and access management

The introduction of Document Management Systems (DMS) and a clear definition of processes is often the first step in digitizing an organization and moving from paper-based processes to fully digitized workflows which are faster and less error-prone. When it comes to access management, central banks can be placed on a continuum from those who operate a "need to know" policy to those with an "open access" policy. Banks with a "need to know" policy only allow access to data when it is absolutely necessary and part of an employee's job description. By contrast, banks with an "open access" policy grant by default all employees access to all internal data that is not classified. The banks define selected data and systems that have increased security risks and allocate access rights for this data. The "open access" principle is embedded in the organizational culture and allows employees to share know-how and think outside the box. Automatically allocating access rights depending on an employee's role creates an efficiency gain and allows the organization to free up resources for higher-priority tasks.

3. Cloud solutions
Introducing central bank as a service.

Cloud computing has been a booming business in recent years. It allows organizations around the world to benefit from flexible, scalable and cost-efficient solutions. Industry leaders such as Amazon and Microsoft have grown and profited from this trend. As financial services companies rely heavily on IT-enabled services, there has been widescale adoption of the cloud. Moreover, the process has been supported by key financial regulators such as the Monetary Authority of Singapore, the UK's Financial Conduct Authority and the Netherlands central bank DNB, which have signaled their approval of the cloud as concerns over data security have receded. The European Commission is also currently heavily promoting the cloud within the European Union: within the Digital Single Market Strategy for Europe, the role of cloud computing is established by the European Cloud Initiative and the initiative on building a European Data Economy. → F

Among the key advantages of cloud solutions is the possibility of storing an ever-increasing amount of data in the cloud without investing in your own server storage. Security is also often better in the cloud: Providers invest enormous amounts in security features, which, when combined with central banks' own network infrastructures, make it possible to meet extremely high security requirements. Central banks can also benefit from these industry best practices without needing to continually upgrade their own infrastructure. Customers, for their part, benefit from the ongoing professionalization. Additional advantages include the availability of data, which enables telecommuting, and cost savings through converting fixed to variable costs and using pay-as-you-go models.

Certain risks remain, of course – reduced availability, lack of control and vendor lock-ins being prime examples. This leads to some hesitation among decision-makers when it comes to shifting to the cloud. As discussed above in relation to cybersecurity at central banks, 100-percent security is not possible. Central banks therefore need to define their own approach when it comes to leveraging cloud solutions and clearly differentiate between strictly confidential data that needs to be stored on their own infrastructure to retain control and less sensitive data that can be stored in the cloud. → F

ADOPTING CLOUD SOLUTIONS IN CENTRAL BANKING

Central banks need to follow a clear roadmap when adopting cloud solutions. This entails choosing an appropriate mix of risk and benefits while remaining within the boundaries of national regulations.

STEP 1 – Define a cloud strategy

First of all, the central bank needs to draw up a cloud strategy based on its overall strategy and risk appetite. All the stakeholders involved need to reach a common understanding, ultimately leading to an agreed strategy and policies.

STEP 2 – Conduct a risk assessment

The central bank should then evaluate which parts of its data and applications can be shifted to the cloud, using predefined, agreed criteria. The data and applications should be categorized in a risk matrix. For example, mission-critical data and applications (such as

trading applications) should remain on the bank's own infrastructure, while less sensitive data and applications (such as statistical data, human-resources data) can potentially be shifted to the cloud.

STEP 3 – Run a business case

The data and applications selected for possible shifting to the cloud should be included in a scenario-based business case. This will enable the bank to evaluate the potential cost savings. For this purpose, initial quotations from suppliers need to be gathered and evaluated.

STEP 4 – Evaluate and select suppliers

The central bank should select one or more suppliers, depending on the vendor strategy. Decisions should be based on a thorough evaluation using the predefined criteria and carrying out negotiations where necessary.

STEP 5 – Pilot, roll out and monitor

Before rolling out the cloud solution, the central bank should run a pilot project with low-risk datasets as a way of validating the operating model. Any lessons learned should then be integrated into the final version for implementation. The implementation itself should be gradual, and followed up with regular risk assessments to ensure that the categorization is up to date and to respond to any changes in the market, technology or risks.

F

PARLEZ-VOUS CLOUD?

Definitions of the most relevant cloud services.

ACRONYM	DEFINITION	EXAMPLE	DESCRIPTION
SaaS	Software as a service	Google Docs	Access to an application that is hosted in the cloud
PaaS	Platform as a service	Microsoft Azure	A platform that allows developers to build and host applications
IaaS	Infrastructure as a service	Amazon EC2	Access to computing, storage and network capacity
BPaaS	Business processes as a service	Payroll processes	Provision of business processes sourced from the cloud
DaaS	Data as a service	Oracle Data Cloud	A platform that gives access to large datasets from anywhere
SECaaS	Security as a service	Firewalls and anti-virus scanners	A business model in which a provider integrates their security services into an IT infrastructure

THERE IS NO ONE-CLOUD-FITS-ALL SOLUTION

Overview of cloud deployment models.

PUBLIC CLOUD	PRIVATE CLOUD	COMMUNITY CLOUD	HYBRID CLOUD
Available to everyone via the internet	Available to trusted users within an organization	Available to trusted users from various organizations	A hybrid of cloud and third-party, public cloud services

Source: Roland Berger

Photo: Marcel Walker / Swisscom

INTERVIEW WITH
MARCEL WALKER

"The main advantage of the cloud is its enhanced flexibility compared to traditional IT setups."

Marcel Walker is Head of Network & Cloud at Swisscom Enterprise Customers. Prior to this role he led Swisscom's Banking operations.

What are the biggest advantages for central banks in leveraging cloud solutions?
In our view the cloud represents first and foremost the complete separation of the infrastructure from the rest of IT management. It does this by creating an opaque layer of services that replaces the traditional combination of hardware- and software. The main advantage of the cloud is its enhanced flexibility compared to traditional IT setups. For central banks this means their technology stacks have faster reflection, adaptation and adoption capabilities, which serve to support the institutions' main missions: price stability, payments management and safeguarding their own operations. These capabilities include concepts like distributed ledger technology, crypto currencies, machine learning analytics and robotic process automation.

How would you address current concerns recarding the security of cloud solutions?
Security enables your business to realize its digitalization strategy. You have to choose the right cloud model, or even take a hybrid approach with your most critical data hosted in your private cloud, as different types of information have different protection requirements. Depending on your needs, you can define a security architecture that features various

technology-independent capabilities to protect information against cyber threats. Be sure to work with a cloud provider who can deliver state-of-the-art solutions for protecting your data and applications. Your strategy should offer continuously improved protection, detection and response capabilities across the whole technology infrastructure, including your cloud providers.

What data/applications can central banks shift to the cloud, and what should remain inhouse?

Because central banks manage heavily by communication and do not cater to private citizens, their data protection needs are different than those of commercial banks. Their main concerns are communication security concerning statements and actions, non-repudiation of data provided as well as integrity of their data stores. This means that central banks theoretically can move almost all data and applications to the cloud, except for the most secure communication infrastructure. To manage their risks on non-repudiation and data integrity, we recommend they keep a shadow master of all crucial applications/data stores at an installation that is under their full control.

How will current and future developments affect cloud solutions?

In the future, we expect the vertical growth of this stack to cover databases, application servers and ultimately the full business application stacks. As use of of cloud infrastructure grow, we expect application providers to align their software solutions and development styles to the cloud solutions available, thus allowing all services types up to and including "Software as a Service" on any available, commercially relevant cloud stack.

4. Digital currencies

Introducing a central bank digital currency is an organization-wide endeavor.

In Part 2 of our series – New realities in central banking: The rise of cryptofinance in central banking – we discussed the topic of digital currencies for central banks and the challenges they present. As recently as 2016 the idea was still a hypothetical one. Now in 2017 we see the topic gaining more traction, with some innovative central banks launching projects and pilot programs to evaluate feasibility and investigate potential technologies that could be used.

In March 2017, for example, Sveriges Riksbank published a multiyear project plan online that outlines concrete steps to evaluate the issuance of the "e-kronor", the electronic currency proposed as a complement to physical cash. Also in 2017, the Monetary Authority of Singapore (MAS) is conducting a proof-of-concept with Ethereum to tokenize the Singapore Dollar. In a similar vein, the Deputy Governor of the Bank of Japan, Hiroshi Nakaso, has commented that the Bank of Japan should try to grasp the possible impact of blockchain and distributed ledger technology on payment and settlement infrastructures, including central bank payment and settlement systems, while a recent working paper from the Bank of Korea confirms the current dominant opinion that digital currency will complement rather than replace physical cash. → G

STAKEHOLDER MANAGEMENT IS KEY

The concept of a digital currency touches upon almost all aspects of the mandate of central banks: It has implications for monetary policy instruments, it requires a payment infrastructure to allow transactions, it affects financial stability and cyber risks, it needs to be issued despite being digital, and so on. What is more, it requires central banks to coordinate a wide range of internal and external stakeholders, from technology providers, regulators, other government authorities and foreign central banks to commercial banks and customers.

How can central banks manage this broad task? They need a dedicated program manager, detached from the day-to-day work of the bank, who can promote the initiative and act as a transformational change agent. The job calls for someone with excellent communication and coordination skills, including the ability to overcome internal resistance to the inevitable paradigm shift.

Central banks need to take a clear stance when it comes to digital currency. But with an issue as important as digital currency, they would be well advised to do some thorough groundwork before reaching any conclusions.

We suggest an approach based on four distinct phases with clearly defined quality gates, go/no-go junctions, and defined deliverables.

PHASE 1 – Pre-study
A small, dynamic team draws up a comprehensive overview of the latest developments and the current state of the debate. The team also interviews key internal and external stakeholders and outlines the scope and ambition of the project.

PHASE 2 – High-level concept
A larger team works on a variety of work streams in parallel, looking at the topic from a holistic perspective. The team carries out a detailed analysis of potential technologies (such as centralized, federated "coopetition" or distributed consensus), legal requirements, policy implications, governance models, roles and responsibilities (such as issuing), and so on. It then draws up a proposal and presents it to the decision-making body of the central bank.

PHASE 3 – Operational concept and implementation planning
After the proposal has been adjusted as necessary, the team adds detail to the operational concept, screens external technology partners and coordinates activities with external stakeholders such as regulators, government authorities and participants in financial markets. It then draws up a detailed implementation plan and presents it to the bank's decision-making body.

PHASE 4 – Implementation
The actual implementation consists of a broad set of interdependent work streams and needs continuous monitoring and reporting to the program management team. Lessons learned and best practices with regard to implementation should be exchanged with other central banks. After implementation, the transformation program is then transferred to the line organization of the central bank, and processes, governance structures and organizational changes are implemented.

G

MORE THAN JUST A NICE TO HAVE
Central bank digital currency has a broad array of potential benefits for central banks.

Reduction of the **COST OF CASH** (e.g. production, transportation, disposal of banknotes) – Currently estimated at 1-2% for developed and 5-7% for developing economies

Broadening the set of **MONETARY POLICY INSTRUMENTS** (e.g. imposing negative interest rates on digital currency or implementing quantitative easing measures by issuing digital currency to e-wallets of households)

Addressing the decline in cash and **IMPROVING FINANCIAL STABILITY** by providing a credit risk free payment system

Eliminating **COUNTERFEITING RISK** by leveraging cryptography-based technology

Improving **OVERSIGHT OF TRANSACTIONS** and increasing effectiveness of AML/CTF monitoring

Proactively addressing the advent of **DECENTRALIZED CRYPTOCURRENCIES** (e.g. Bitcoin)

Increasing **SEIGNIORAGE INCOME**

Expanding **FINANCIAL INCLUSION** by providing alternative access to financial services to underbanked segments of the population (especially relevant in developing economies)

Source: Roland Berger

Photo: Jonathan Dharmapalan / eCurrency Mint

INTERVIEW WITH
JONATHAN DHARMAPALAN

"We can expect that [...] careful examination of evidence and analysis will ultimately lead to a transition to digital fiat currency."

Jonathan Dharmapalan is the founder and CEO of eCurrency Mint, a technology company based in Dublin. eCurrency has pioneered the technology that allows central banks to issue a digital fiat currency (DFC).

Is digital currency just a lot of hype or is it only a matter of time until adoption?

Digital currency is not hype – it is inevitable and it is happening now. We have already digitized information, letters, photographs and commerce. Why not digitized money? Many people already think of account-based money as "digital". People also think that payment systems are digital money. However, we must differentiate between digitized "money" and a digital "currency". Currency, unlike money, is defined by a legal doctrine that renders it legal tender in a country, whereas money is defined as a generally accepted medium of exchange. A currency can exist and perform its function as legal tender only if it obeys the laws that make it legal tender. A true digital currency acts as a sovereign instrument issued by the sole authority of the central bank. That is how it becomes digital fiat currency.

Physical fiat currency, which we use today, is the ultimate instrument of financial inclusion – accessible to all and accepted by all. Its one shortcoming is that it cannot transcend space and time. With the digital revolution taking place, it is inevitable that physical currency too will move into the digital realm. The question being considered by central banks today is not "if" digital fiat currency will be adopted, but "how"?

How does your technology allow central banks to issue digital currency?

eCurrency has solved the question of "how" by mimicking the properties of physical cash. Mirroring the interoperable nature of physical currency, a digital fiat currency is a secure instrument that can be transacted across any payment system and any digital platform. Just as physical banknotes are not tied to the transport mechanism, neither is their digital counterpart. Essentially, we have decoupled the digital currency instrument from the digital wallets in which it is held. Furthermore, we have decoupled the networks on which it is transacted from the digital currency instrument itself.

Returning to our model of physical currency, we have cryptographically mirrored the kind of security elements found on modern banknotes. Just as holographic foils, precision patterns and serial numbers are layered in a physical note, eCurrency has layered and bound together analogous digital security elements to secure the digital currency instrument. Most importantly, we have made sure that this digital currency can originate only from a single authority, namely the central bank, thus ensuring its validity as sovereign, fiat currency.

Where do central banks currently stand when it comes to introducing digital currencies?

Central banks are currently studying the possibility of issuing a digital fiat currency. Many have taken the first steps toward creating a secure, digital stored-value system that will eventually evolve into digital fiat currency.

What are the current hurdles to the adoption of digital currency?

Central banks have been quite proactive in understanding the implications of this upcoming evolution. eCurrency's technical solution is based on requirements set by central banks' understanding of issuance and distribution of a digital fiat currency. Now that eCurrency has overcome the technological hurdles, it is up to the central banks and their respective governments to make the decision to begin the transition to digital currency.

Central banks, as stewards of macroeconomic stability, are conservative organizations by nature; they require time and circumspect study to introduce such an impactful technology. We can expect that their careful examination of evidence and analysis will ultimately lead to the adoption of a digital fiat currency.

What role does blockchain technology play?

Blockchain is one of many building block technologies that underpinned the creation of bitcoin. It is now being adopted for other financial applications. Whether or not central banks can use blockchain remains unclear. Many have already concluded that the nature of blockchain is not suitable for the issuance of currency, as it was not created for this purpose. Quite unlike blockchain, the eCurrency technology was specifically designed and created for the purpose of enabling central banks to issue a sovereign currency instrument in digital form.

What are the benefits of a digital currency for national economies?

Digital fiat currency offers near-term efficiencies and long-term stabilizing benefits for any economy. From a policy perspective, digital fiat currency enables central banks to fully realize their responsibilities as sole issuers of the national currency using simple, clear governance. A digital currency issued by the central bank has the ability to operate under the same governing principles as physical currency. Central banks can govern digital legal tender with simple, existing regulations: only they can create, destroy and declare it legal. While preserving simplicity in oversight, the technology affords governments new insights into near-real-time flows of the money supply. This enhances control over the levers of monetary policy and will enable more efficient and effective policymaking.

From the user's perspective, eCurrency's solution enables more secure and efficient digital transactions. Unlike privately issued digital value, digital fiat currency issued by the central bank works securely across all payment systems, solving the problem of interoperability. Enhanced interoperability improves the utility of digital financial services, benefiting those who have historically been excluded from traditional financial services.

How do banknote printers need to adapt to the ongoing technological developments?

In the short and medium term, banknote printers will continue to provide the physical currency that economies require. The need for physical currency in the form of banknotes and coins may be nominally reduced as central banks replace a portion of their physical cash with digital fiat currency. However, the transition to digital will be gradual and the need for banknotes is not likely to decrease dramatically in the near future.

Mind the gap. Three levers for closing the strategic perception gap of the IT function.

Earlier on in this study we mentioned the worrying gap between the perceived strategic importance of IT within central banks and its real significance, based on our many conversations with industry experts. To close this gap, central banks need to undergo a radical shift in their mindset. We identify three levers that can help address this challenge:

1 **Strengthen the role of IT as a strategic partner at the interface between the business and the IT function.** IT is more than an internal services provider: it should be involved in shaping the agenda, managing the project portfolio and other key tasks.

2 **Make the organization more professional by implementing a plan-build-run organizational model.** Adjust reporting lines and governance structures as necessary.

3 **Build up relevant internal technical capabilities and external supplier-management capabilities.** This will enable you to proactively address technological developments and coordinate an increasingly complex supplier network.

THE ROLE OF THE CHIEF INFORMATION OFFICER

As the IT function grows in importance at central banks, the role of the Chief Information Officer (CIO) also needs to be strengthened. The "new realities" call for an individual with a highly qualified profile and a unique set of technical, interpersonal and leadership skills. Essentially, the CIO needs to have two hearts beating in their chest: a central banker's and a techie's.

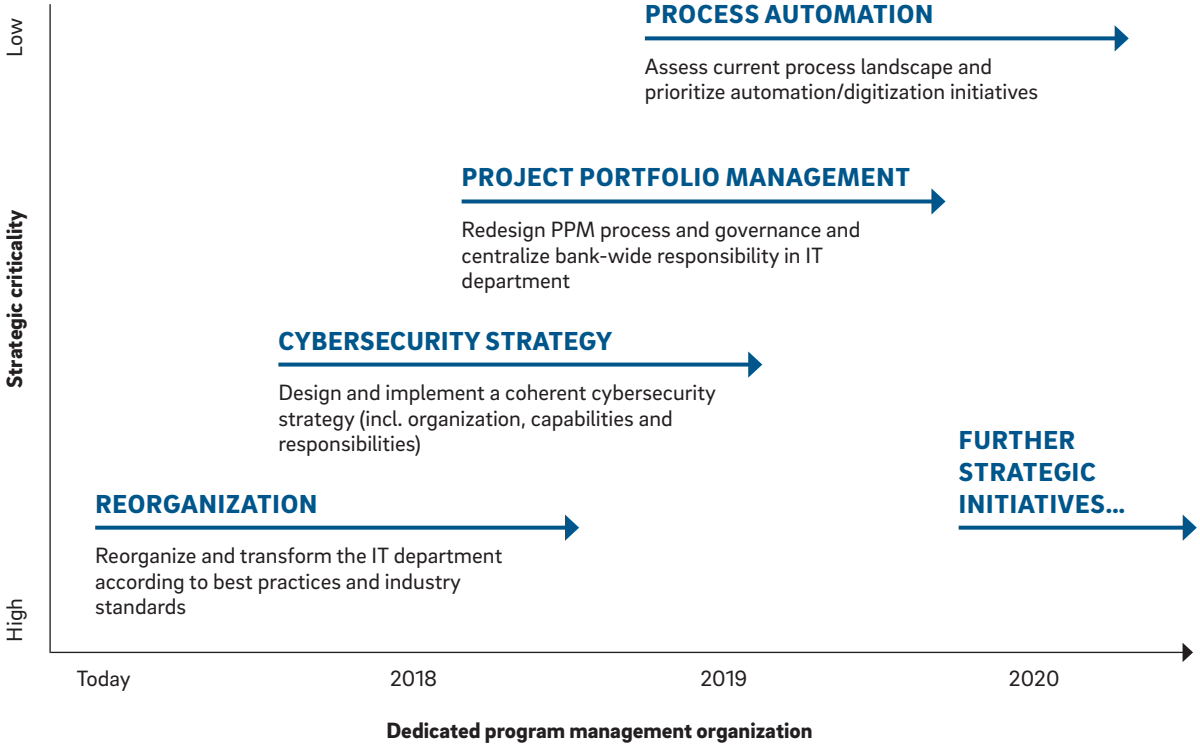
Of course, the CIO must have an in-depth understanding of the entire spectrum of IT functions, from application management to infrastructure and cybersecurity. But they also need to be able to break down the ever-increasing technological complexity and communicate the risks and opportunities to the bank's top management, who are after all mainly economists.

Ensuring your CIO has the right abilities is only the first step. Governance structures must be adjusted so that the CIO is directly involved in decision-making. The CIO also needs management tools such as a "CIO cockpit" so they can lead the strengthened IT function effectively. They also need a clear strategic roadmap for preparing the central bank for the new realities – see the example on page 21. A good starting point for this can be to conduct a 360° review and establish a thorough understanding of the bank's current strengths and weaknesses. → H

H

FROM TRANSFORMATION TO AUTOMATION

A strategic roadmap for Chief Information Officers.



CRITICAL SUCCESS FACTORS

- **Continuous** and **open dialogue** with all stakeholders
- Consistent and effective **change management**
- Excellent **project and program management** capabilities
- **Agile mindset** to react swiftly to technological developments

Source: Roland Berger

In a nutshell: Central banks need to act now. An essential part of their role is to shape the new realities.

Central banks need to take action now. They are facing a range of new, technology-driven challenges that will affect their business in many different ways, many of them difficult to imagine today. They must develop a concise vision that goes beyond bringing their IT systems up to date and actually puts them at the forefront of technological innovation.

Fresh thinking is called for in four key areas: cybersecurity, process automation, cloud solutions and digital currencies. As we have seen, IT departments must become true partners to the business and really live up to this new role. The future will be challenging: Central banks must ensure their resilience and efficiency by becoming high-performance, industry-leading organizations. ◆

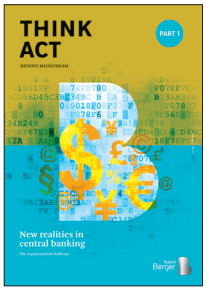
ABOUT US

Roland Berger, founded in 1967, is the only leading global consultancy of German heritage and European origin. With 2,400 employees working from 34 countries, we have successful operations in all major international markets. Our 50 offices are located in the key global business hubs. The consultancy is an independent partnership owned exclusively by 220 Partners.

Navigating Complexity

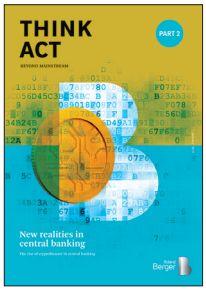
For half a century, Roland Berger has helped its clients manage change. Looking at the next 50 years, we are committed to supporting our clients conquer the next frontier. To us, this means navigating the complexities that define our times. We help our clients draft and implement responsive strategies essential to success that lasts.

FURTHER READING



NEW REALITIES IN CENTRAL BANKING – PART 1
The organizational challenge

Central banks' mandates have expanded over the past few decades. Increasing public scrutiny and a changing operating environment have brought a pressing need for central banks to become high performance organizations. But what kind of structural changes and transformation is necessary and desirable?



NEW REALITIES IN CENTRAL BANKING – PART 2
The rise of cryptofinance in central banking

2017 is heralded as the dawn of digital currencies in the financial services industry. Emerging digital and virtual technologies are lauded as the most disruptive innovations since the advent of the internet. Both hoodies and suits are embracing the arrival of digital currencies. Amidst all the hype, it is important to sift through and identify the key messages relevant in the world of finance in the digital age.

LINKS & LIKES

ORDER AND DOWNLOAD
www.rolandberger.com

STAY TUNED
www.twitter.com/
RolandBerger

LIKE AND SHARE
www.facebook.com/
RolandBergerGmbH

READ WHAT OUR CEO HAS TO SAY ON CYBER-SECURITY
www.rolandberger.com/en/
Blog/Hackers.html

Publisher

ROLAND BERGER GMBH
Sederanger 1
80538 Munich
Germany
+49 89 9230-0

WE WELCOME YOUR QUESTIONS, COMMENTS AND SUGGESTIONS

ADRIAN WEBER
Senior Partner
+41 43 336-8759
adrian.weber@rolandberger.com

KNUT STORHOLM
Senior Partner
+971 4 446-4080
knut.storholm@rolandberger.com

PHILIPPE CHASSAT
Partner
+65 6597-4560
philippe.chassat@rolandberger.com

MICHAEL MÜLLER
Senior Consultant
+41 43 336-8613
michael.mueller@rolandberger.com

Interview partners:

JONATHAN DHARMAPALAN
Founder and CEO of eCurrency
jonathan.d@ecurrency.net

MARCEL WALKER
Head of Network & Cloud at Swisscom
marcel.walker@swisscom.com

TA_17_024