CARRYING THE COMMUNICATIONS INDUSTRY FORWARD

Creating Business Value With Blockchain

EMMA MCGUIGAN | ADRIANO POLONI | AMOL PHADKE | RICHARD MESZAROS | EMMANUEL VIALE

Communications service providers (CSPs) are on the brink of a $1 trillion-plus opportunity. The new technology known as blockchain can enable them to leverage their five-billion person aggregated reach – one of the largest on the planet – to unlock new revenue streams, enhance the customer experience, and reinvent themselves as an essential part of users' daily digital routine.

This technology opens up new opportunities across multiple industries. Where the internet enabled low-cost *information* transfer, blockchain enables low-cost *value* transfer. It enables transactions and other forms of data to be consistently shared, traceable, ubiquitous and trusted —qualities that are essential in guaranteeing their value.

With blockchain, CSPs—already trusted purveyors of value—can potentially take a key role in tracking and transferring value across the dozens of billions of devices, sensors and other entities where their Pervasive Network plays a part. Building on blockchain technology, CSPs can play to their strengths, leveraging their valuable heritage of telecoms experience—including customers, billing relationships, networks, understanding of local market regulations, security and trust—to leverage new competitive advantage.

> **Pervasive Network: An environment where the connectivity of devices is embedded in such a way that the connectivity is unobtrusive and always available, and where using the network is simple and ubiquitous.**

WHAT IS BLOCKCHAIN?

At its most basic level, blockchain—a subset of distributed ledger technology (DLT)—is a new type of database system, distributed. It maintains and records data in a way that allows multiple stakeholders to confidently and securely access identical copies of distributed data.

Transactions or data are added and timestamped in a ledger that is distributed among interested parties who participate in an established network of computers. Data consistency is achieved by consensus, and authentication and trust is established without a central authority or auditor, but continuously within the network, through the transparent and auditable flow of information. Figure 1 illustrates the advantages blockchain offers in "flattening" transaction models, while yielding corresponding efficiency gains.

Blockchain offers inherent trust advantages: A new block can be added to the blockchain only if there is consensus among the network participating nodes, and any participants can audit the transaction history, accordingly to pre-agreed rules. Such advantage materializes because there is no need to run a costly and slow inter-organization data reconciliation process, given that with blockchain each participant is certain to access the very same data across the distributed network.

Blockchain is also highly secure and resistant to tampering; if anyone tries to tamper with, duplicate or alter any part of the record, all stakeholders will easily recognize it.

An ecosystem today

The traditional ledger structure between organizations is slow, manual, intensive and error prone. Any exchange of data requires that all of the data stores used by each of the participants must agree and be reconciled, driving significant added effort and inefficiency.
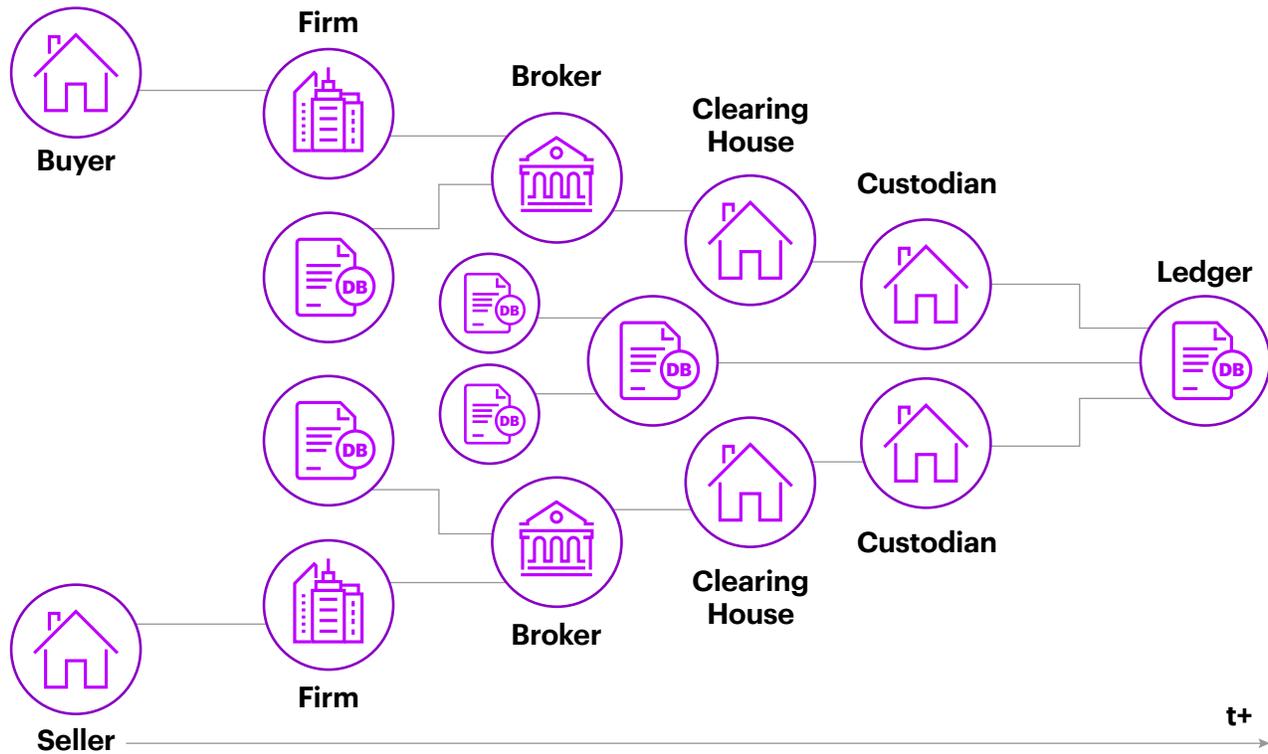
A potential blockchain-based ecosystem tomorrow

A distributed blockchain ledger allows for decentralized, replicated, shared and cryptographically secured operations, which are validated by mass collaboration and apply to many transactions. All market participants work from the same data set, introducing significant efficiency improvements.

HOW COULD BLOCKCHAIN ADD VALUE FOR TELCOS?

CSPs, like companies in other industries, have great potential to benefit by using blockchain technology in their core management systems, where it will provide opportunities for cost reduction through process efficiency gains. Even more exciting is CSPs' special opportunity to obtain new revenue growth, thanks to blockchain enabling CSPs to offer entirely new value propositions.

Consider just a few possibilities: a) Digital Identity Management, b) Internet of Things (IoT) Disintermediation and c) Management of Cross-Carrier Payments. These examples readily illustrate how two of the greatest strengths of a CSP—connectivity and trust—can gain additional power when combined with blockchain's added advantages in security, trust and speed.

Digital Identity Management

Current State. Current approaches to identity and authentication services are inefficient and insecure. Every time a person wants to sign up with a vendor, they need to prove their identity and credentials by using physical or digital documents and providing extensive personal identity information, even though most of that information is not needed by every vendor. Also, signing up online requires either creating many username/password combinations or utilizing the single sign-on functionalities of third-party providers,

such as Google or Facebook. This leads to many challenges, including a lack of convenience and a lack of security due to personal data being shared with third parties. This situation will likely only become more challenging as the Pervasive Network takes hold, with literally billions of devices and sensors taking part and requiring constant validation and authorization.
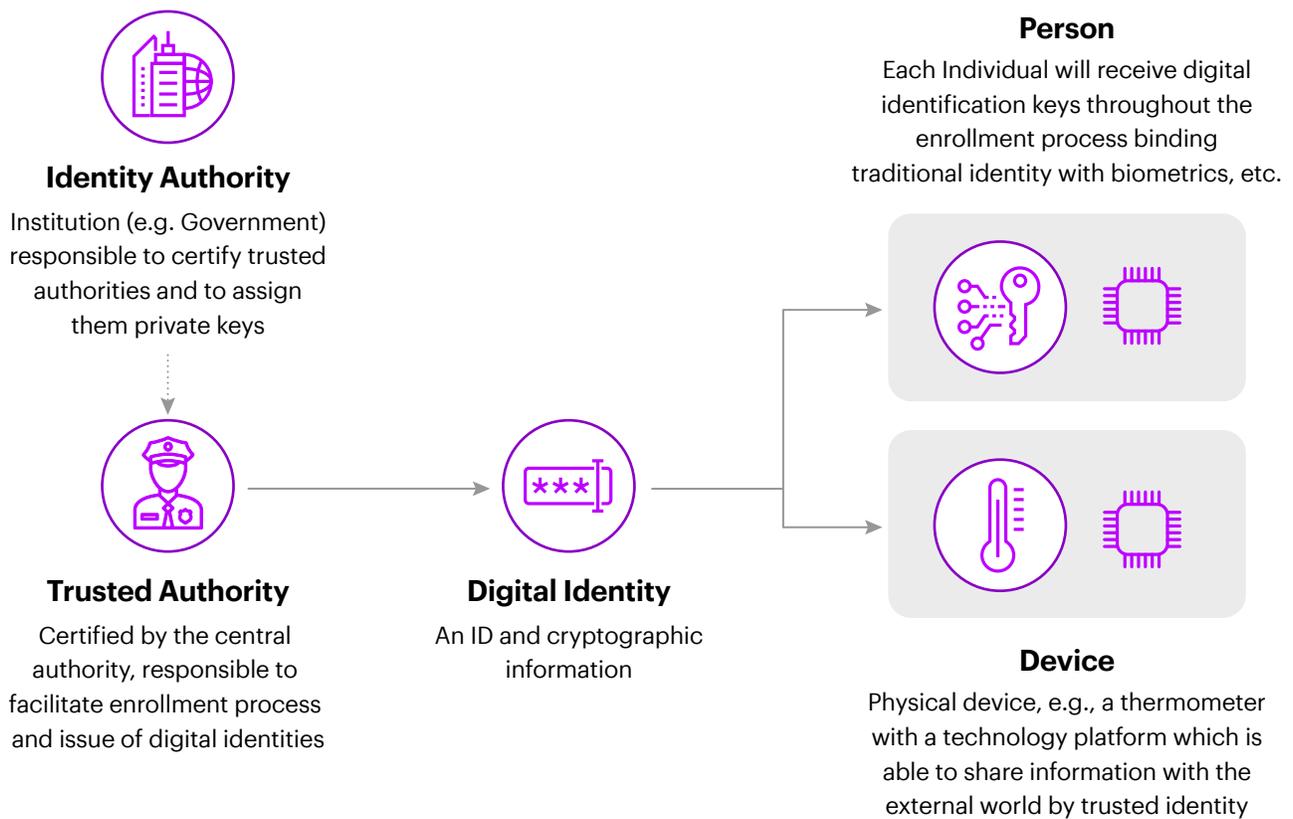
The Blockchain Opportunity. Even though CSPs possess substantial amounts of relevant subscriber data, they currently do not play a significant part in identity and authorization services. Yet using blockchain, CSPs could carve out a meaningful space in the identity value chain by leveraging their current position as a trusted service provider that customers want and expect to know their personal profiles, including their history of devices, services and content purchases. CSPs can leverage the credibility of telcos around trust, security, privacy and proximity.

For example, using a blockchain model, when a subscriber opens an account with a CSP, the CSP could create a digital identity that could be deployed securely and universally. The CSP would add a digital signature using its own private key, with a pointer to this virtual identity, along with necessary descriptors that would then be added to the blockchain. Using this approach, CSPs could position themselves in a new role as trusted issuers and managers of digital identities, opening up new loyalty mechanisms and revenue streams.

Figure 2 illustrates this potential CSP role.

This blockchain-enabled approach would provide decreased costs for implementing identity management, reduction of identity theft, and increased speed and decreased cost for the enrollment process. Establishing a collaborative multi-carrier approach, then leveraging designated identity providers through the use of a distributed and federated blockchain, would provide the potential to reduce traditional identity assurance costs by up to 90%.

Figure 2: Establishment of a CSP as Trusted Authority for Digital Identity Management

Identity Authority

Institution (e.g. Government) responsible to certify trusted authorities and to assign them private keys

Trusted Authority

Certified by the central authority, responsible to facilitate enrollment process and issue of digital identities

Digital Identity

An ID and cryptographic information

Person

Each Individual will receive digital identification keys throughout the enrollment process binding traditional identity with biometrics, etc.

Device

Physical device, e.g., a thermometer with a technology platform which is able to share information with the external world by trusted identity

Roadblocks. Though this new approach is promising, several roadblocks would need to be overcome. Not all players would be equipped to play competitively: commanding a large customer base, having a strong digital presence, and possessing synergies with ongoing businesses on trusted security services (such as mail security) are all factors that would favor new digital players in the game. In addition, for a federated, multi-carrier approach, a new decentralized identity model would be required, where designated, trusted authorities would be responsible for issuing digital identities, as well as for providing fast and effective validation mechanisms that are scalable for large volumes.

Relevant Example. Concrete cases are occurring in the market: for example as part of Italy's Digital Agenda, all citizens are being issued with a "SPID" (public system of digital identities) which will allow access to public and private services. This is supported by four security providers and the incumbent telco operator. Estonia has been an incubator of an advanced digital identity system for the rest of the world: the Estonia ID card is a cryptographically secure digital identity card, powered by a blockchain-like infrastructure on the back end, which allows an Estonian to access public and private services (medical, financial services, etc.), pay taxes, e-vote, and more. Switzerland is also launching initiatives in this space: the City of Zug will soon offer all its citizens a digital identity on the Ethereum blockchain, securing personal information using blockchain technology and associating it with a cryptographic address.[1]

Building on efforts like these, the ID2020 Alliance is a global partnership committed to improving lives through digital identity. An alliance of governments, NGOs and the private sector, ID2020 is using blockchain-based technology with the goal of ensuring that each individual can obtain a digital identity that is 1) personal, that is, unique to each individual alone; 2) persistent, that is, living with that individual from the beginning of life to death; 3) portable, i.e., accessible anywhere that individual happens to be; and 4) private, with only that individual being able to give permission to use or view data.[2]

IoT Disintermediation

Current State. Building on their opportunity in digital identity management, CSPs have a closely related opportunity to facilitate IoT disintermediation. The exponential growth of IoT approaches raises new challenges associated with data authenticity and ownership, security and privacy, and the upfront and ongoing costs of deployment. This growth is also giving rise to increased devices autonomy, shifting focus from a single central authority and monolithic infrastructure to a new, decentralized architectural approach. Recent attacks on IoT devices have demonstrated that unsecure devices/routers can be the vehicle of massive digital denial-of-service (DDoS) outages, with huge societal and economical damage. Security is hence a priority, and will be even more critical as telcos increasingly seek to become more highly valued platform players, with a need to authenticate a connected ecosystem of value-added services offered by players from multiple industries.

The Blockchain Opportunity. CSPs are already engaged in the IoT ecosystem, with home routers for commercial and private usage often serving as gateways for IoT devices, and with many CSPs already offering IoT products and services such as Connected Home and Connected Car. Using blockchain, CSPs would deliver a value-added trust capability through digital identity validations and assuring the integrity of device transactions. They could also displace traditional centralized IoT cloud infrastructures by establishing a peer-to-peer communication model that allows for the lower-cost processing of billions of transactions between IoT devices, positioning themselves as the trusted authority for digital identity.
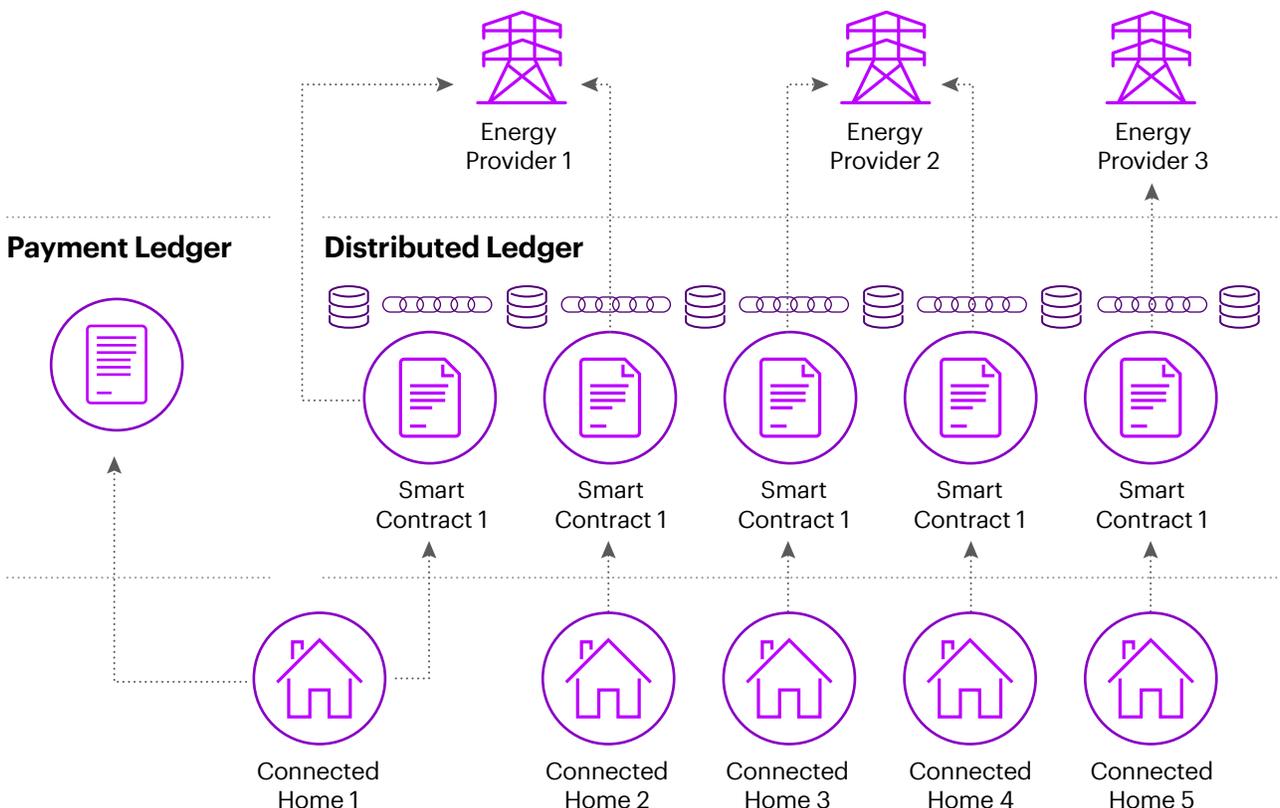
For example, as shown in Figure 3, Blockchain can work together with IoT and the connected home to regulate energy provision between providers and consumers, automating the selection and switching of energy providers to meet customer requirements.

Roadblocks. As with the Digital Identity Management use case, potential roadblocks for CSPs would include several factors favoring new digital players, including command of a large customer base and a strong digital presence.

Relevant Example.
Leading telecommunications provider Telstra is experimenting with a combination of blockchain and biometrics for its IoT

Figure 3: Using Blockchain to Automate Customers' Selection of Energy Provider

Energy Provider 1

Energy Provider 2

Energy Provider 3

Payment Ledger

Distributed Ledger

Smart Contract 1

Smart Contract 1

Smart Contract 1

Smart Contract 1

Smart Contract 1

Connected Home 1

Connected Home 2

Connected Home 3

Connected Home 4

Connected Home 5

smart home offerings. Facial and voice recognition is tied to the blockchain to verify the identity of the persons interacting with the devices, with the goal of providing real-time tamper detection and tamper resistance capabilities in the home environment, while also improving security across the IoT devices.

Telstra is also experimenting with using distributed ledgers for legal interception, agriculture, network operations, environmental sensor monitoring, car safety, fraud, compliance and audit, and e-voting.[3]

Management of Cross-Carrier Payments

Current State. What customers desire is real-time, rapidly delivered, secure transactions of specific, often small, amounts. Meeting those demands is cost-prohibitive for telcos in today's world.

Financial transactions among CSPs, such as mobile payments, require an underlying fund transfer mechanism, either credit cards or bank transfers; and the means by which these payments move across borders is through traditional banking processes.

The Blockchain Opportunity.
Let's consider the CSPs' opportunity with businesses who can benefit from reaching telcos' aggregated user base of 5 billion. As Figure 4 illustrates, blockchain offers telcos the opportunity to eliminate the necessity for centralized authorities to validate many types of transactions.

Thanks to its distributed ledger technology, blockchain offers telcos the opportunity for immediate reconciliation, enabling them to facilitate rapid, secure, variable-sized payments between users. Once blockchain technologies are realized, other cross-carrier, cross-border use cases can be considered, including global remittance, international travel and international airtime top-ups.

Figure 4: Immediate Validation of Transactions

Centralized approach

Blockchain approach
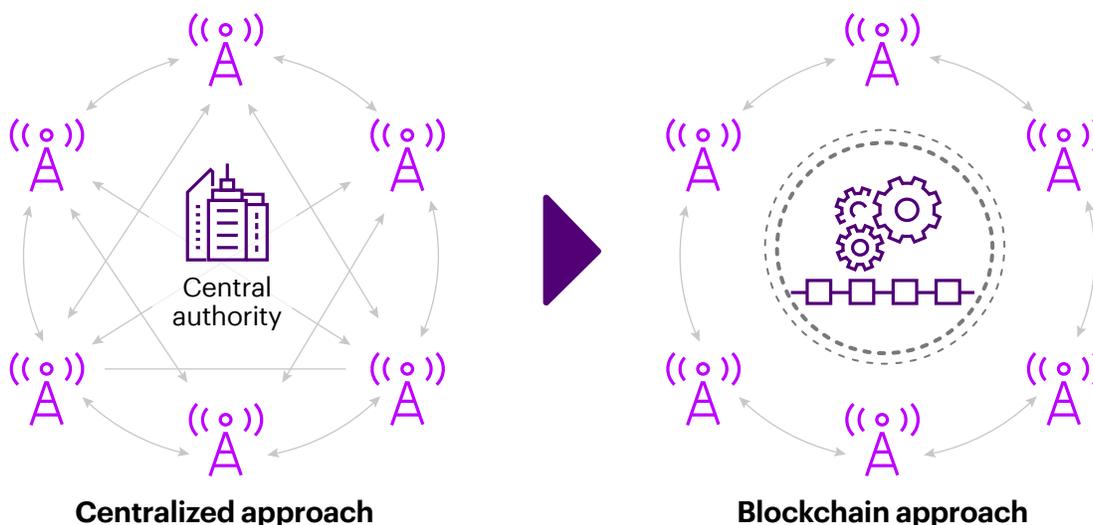
The largest single opportunity may be creation of a universal, integrated solution for all users, connecting the unbanked population, which currently represents untapped value in the economic system.

Roadblocks. While these and many other potential use cases exist, developing them as an independent carrier will be very expensive and difficult.

Relevant Example. For CSPs, the opportunity to realize the full benefit of blockchain in this area will be greatly facilitated by the establishment of a telco consortium, which would spread the risk and cost of development. SoftBank, Sprint and TBCASoft have demonstrated a cross-carrier payment platform system, which is designed to be operated 24/7 at low cost and to complement existing

trust by providing the missing inter-carrier clearing component. The group intends to help define the next-generation business platform leveraging state-of-the-art technologies, and to bring new and disruptive business models to life by influencing regulations and standardization.

> **The record-keeping aspect of blockchain can also help CSPs manage network appliances, including switches, routers and gateways. Network equipment providers are seeking to use blockchain to maximize efficiency from their current operations. Complex pieces of hardware can be more effectively managed through a blockchain-based controller, providing a secure record that can help alleviate network outages and maximize efficiency.**

PLAYING TO CSPS' STRENGTHS

As these use cases illustrate, CSPs have a number of significant opportunities to benefit from the application of blockchain technology. Beyond these examples, CSPs also enjoy a number of significant general advantages. Because of their broad-scale connectivity and high levels of quality, security and fidelity, CSPs' networks are well positioned to participate in the certification of value that is the essence of blockchain. A high proportion of their customers are already familiar with the use of communications devices to participate in transactions, demonstrating a clear roadmap for expanding such use into unbanked populations using

blockchain. And because of their history of strong customer relationships, CSPs are already trusted as purveyors of value, which is highly relevant to their potential opportunities as digital identity managers and as facilitators and validators for blockchain-enabled transactions.

CSPs also have a strong history of collaboration within the industry; and this, along with their deep knowledge of the intricacies of policy and regulatory matters, positions them to be leaders in operationalizing blockchain technologies across a spectrum of use cases and geographies.

HOW TO GET STARTED

In summary, there is a clear opportunity for CSPs to start understanding how blockchain can drive new opportunities for individual carriers and for the industry as a whole.

Their general path is clear:

1 Identify and prioritize relevant use cases: those that either add value and solve real problems, or address innovative market opportunities.

2 Use design thinking to explore a few high-priority use cases, defining the role of blockchain, its impacts on the business model, and value drivers.

3 Create a prototype/proof of concept to understand a specific use case, including clear definition of the issue at hand and the solution the technology provides.

4 Launch pilots to gain real-world feedback and understand implementation.

5 Launch successful projects into the production environment; roll them out to target customer segments; and scale, manage and optimize them as an enterprise capability.

When value transfer becomes the new paradigm, customers and end users will demand connectivity, security, fidelity and trust. Blockchains built on networks optimized for data transfer alone will encounter tremendous headwinds as they labor to bring their networks to the requisite level...one that telcos already enjoy today. CSPs owe it to themselves to take advantage of their inherent strengths...and to investigate these opportunities.

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions – underpinned by the world's largest delivery network – Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 442,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

To explore more, please visit www.accenture.com/blockchain

CONTACT THE AUTHORS

Emma McGuigan
London, UK
emma.t.mcguigan@accenture.com

Adriano Poloni
Milan, Italy
adriano.poloni@accenture.com

Amol Phadke
London, UK
amol.phadke@accenture.com

Richard Meszaros
Dallas, Texas, USA
richard.t.meszaros@accenture.com

Emmanuel Viale
Sophia Antipolis, France
emmanuel.viale@accenture.com

1 https://blogs.thomsonreuters.com/answerson/e-estonia-power-potential-digital
   -identity/; https://e-estonia.com/solutions/; http://www.id.ee/?lang=en&id=36881;
   https://bitcoinmagazine.com/articles/swiss-crypto-valley-create-digital-identities-its
   -citizens-ethereum-blockchain/?utm_content=buffere6b1e&utm_medium=social&utm_
   source=twitter.com&utm_campaign=buffer

   https://newsroom.accenture.com/news/accenture-microsoft-create-blockchain
   -solution-to-support-id2020.htm

   http://id2020.org/

   https://www.agendadigitale.eu/cittadinanza-digitale/a-che-punto-e-il-sistema-
   pubblico-dell-identita-digitale-e-a-che-serve/

   http://www.latimes.com/world/la-fg-india-database-2017-story.html

   http://securekey.com/wp-content/uploads/2016/06/ECONOMICS-OF-IDENTITY.pdf

   http://id-use.blogspot.it/2015/11/no-business-case-for-identity-providers.html

2 https://id2020.org/partnership/

3 https://www.zdnet.com/article/telstra-explores-blockchain-biometrics-to-secure-smart-
   home-iot-devices/