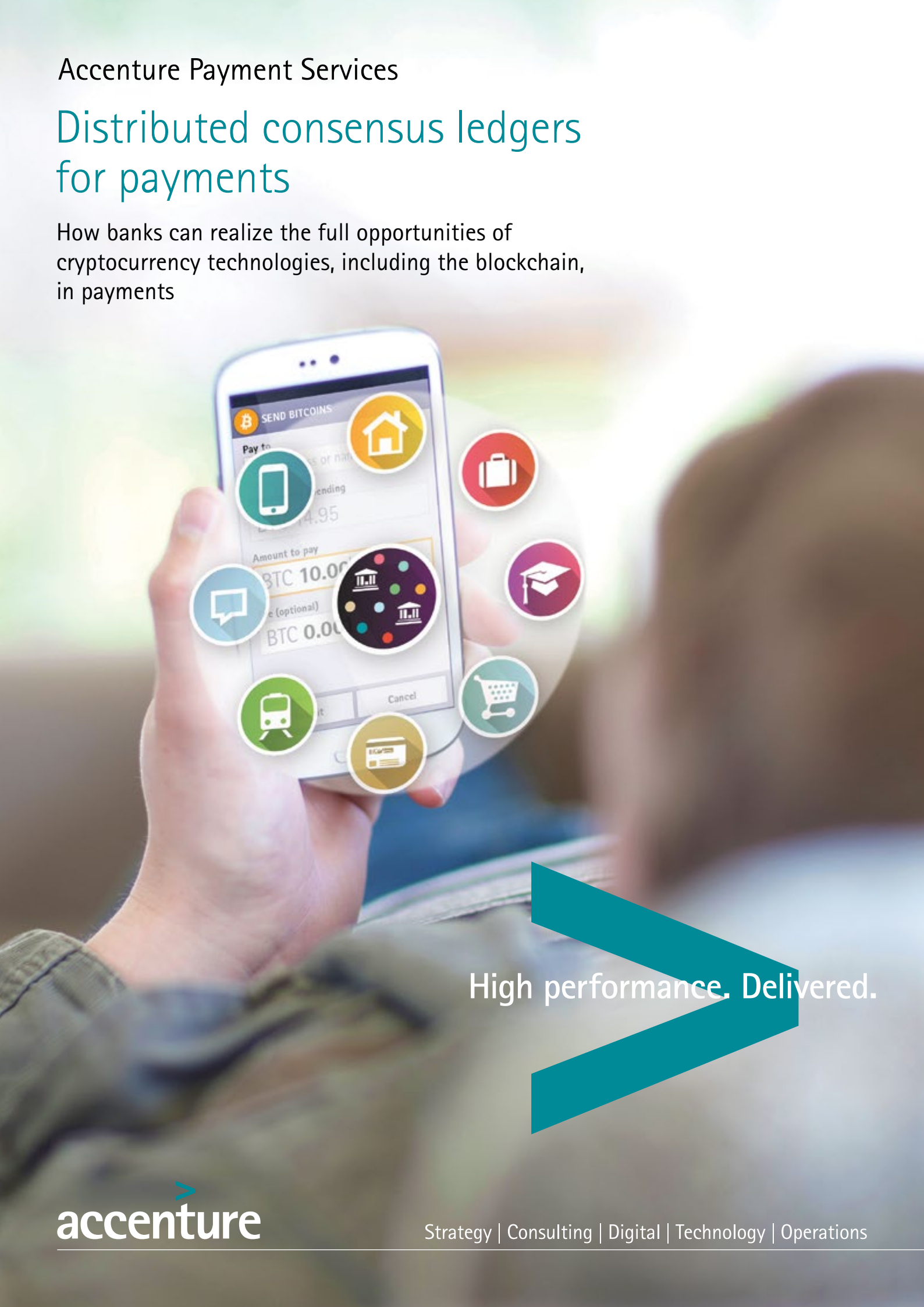
Accenture Payment Services

Distributed consensus ledgers for payments

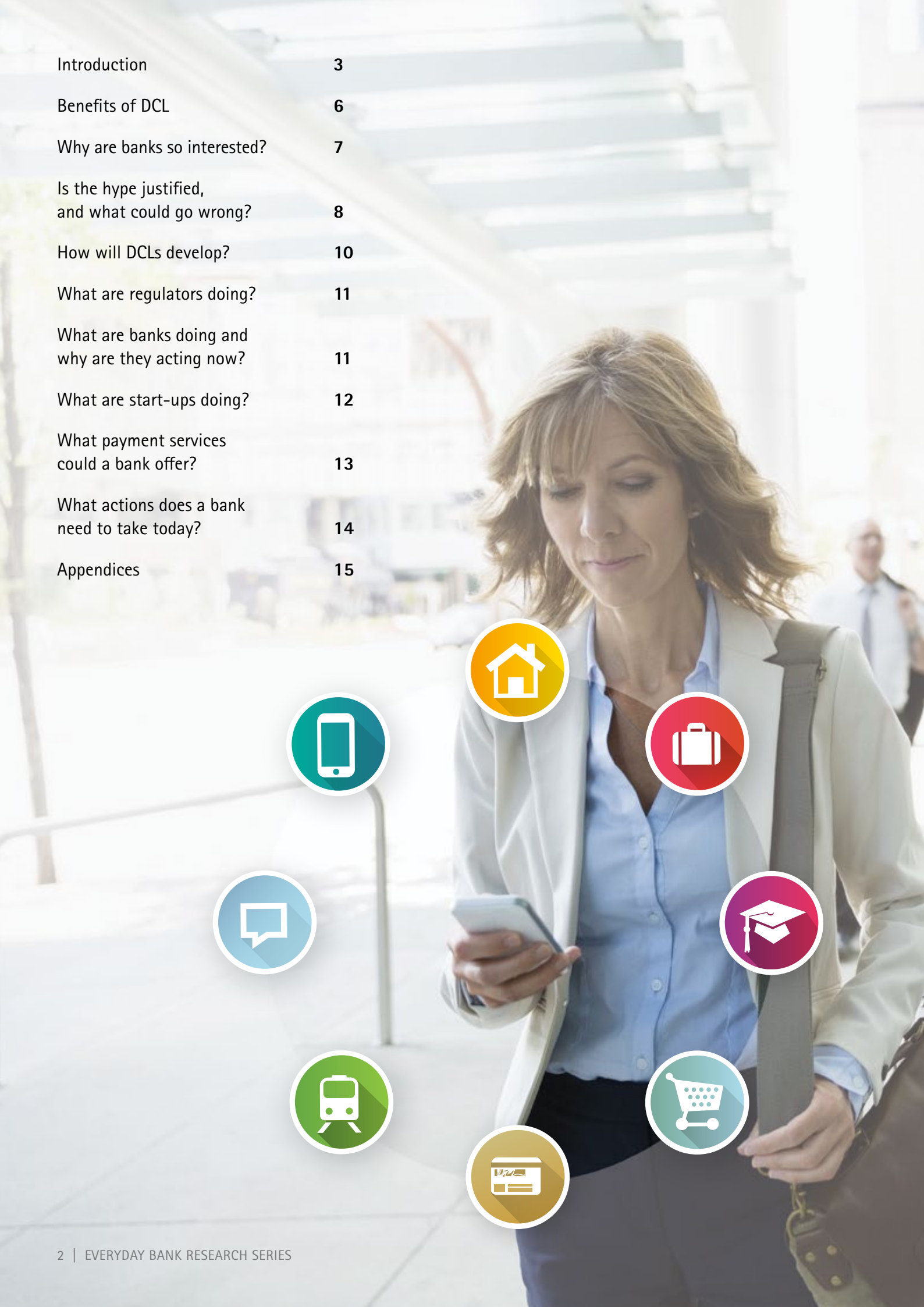
How banks can realize the full opportunities of cryptocurrency technologies, including the blockchain, in payments



High performance. Delivered.

accenture

Strategy | Consulting | Digital | Technology | Operations



Today's evolving DCL landscape

The global rise of Bitcoin has introduced the world to distributed consensus ledgers, blockchains and cryptocurrencies. Usage of Bitcoin itself is growing strongly, with transactions volume now reaching over 200,000 per day and a market capitalization fluctuating between US$3bn and US$4bn.

However, rather than the digital currency itself, many Financial Services executives are more interested in the underlying technology that Bitcoin uses—specifically the 'blockchain', or more generically the distributed consensus ledger (DCL—see panel on page 5 for definitions). Interest focuses particularly on this technology's potential to enhance efficiency, trust, transparency, reach and innovation in the financial markets. And as various players investigate these possible uses, claims are being made about the potential to revolutionize financial services, disrupt long established business models and reduce costs.

Payments is one of the areas where DCL may prove valuable. While there are many other use cases—including in securities and capital markets—the potential use of DCL in payments is the focus of this point-of-view.

Growing interest and investment...

The rising interest in Bitcoin and DCL technology has triggered widespread activity and investment, including the launch of many start-ups—with Coindesk[1] estimating that over US$800m has been invested in Bitcoin companies, and public announcements totaling US$373m in the first half of 2015 alone. At the same time, many banks have set up innovation laboratories and R&D programs focused on blockchain/DCL technologies. Such examples of bank innovation are helping to reshape the future of banking technology.

Accenture is also investing in R&D in this area. In our Technology Labs around the world Accenture is running its own blockchain, smart contract applications and DCL initiatives across a range of industries including financial services, utilities and consumer electronics.

...as banks try to navigate through the hype

However, while innovation around DCL capabilities is under way, there is still a lot of hype—making it difficult for banks to decide exactly where and how to address the opportunity. The DCL sector has seen no breakthrough successes as yet, except for Bitcoin itself. The technology is also relatively immature. Indicators of its immaturity include the limited capacity of the Bitcoin network, and the polarized and fractious debate on how to expand it; the security breaches being suffered on the current generation of digital wallets; and Accenture's own experience of testing and development in our Technology Labs has shown us the technology is not ready for industrialized commercial use.

How does a DCL work?

For a concise overview of what DCL technology is and what it does, please see Appendix 1 on page 19.

As all of this indicates, the industry is in a discovery phase—so while the participants' instincts tell them DCL will be big and transformational, it is not yet clear where and how these impacts will come about. Against this background, many start-ups are focusing on point solutions—wallets, exchanges, security, and so on—with relatively few taking a holistic approach or covering industry solutions. An exception to this rule is Ripple, focused on interbank settlement for cross-border payments and correspondent banking.

Given this situation, the post-hype 'trough of disillusionment' for DCL looks imminent. The ambitious claims about its potential benefits—"savings of US$10s of billions a year"—are hypothetical at this stage, and although are possible, they are not yet founded on proven evidence. At the same time, continuing regulatory uncertainty remains a drag on innovation, and where regulators have taken action, such as in New York (Department of Financial Services Bitlicense regulation), the outcomes risk being expensive and time-consuming, increasing the cost of innovation, particularly for start-ups.

However, it is critical that banks take action now to define their strategy and approach to DCLs. Once the industry starts climbing away from the hype and disillusionment—and these phases won't last long—banks will need to be on the front foot. The impact of DCLs will be pervasive and transformational, and the process to experiment, learn, plan and architect for them needs to begin now.

To dismiss DCLs as irrelevant—or take a "wait-and-see" approach—carries high risks for any bank seeking to keep up with today's fast-changing digital economy and the related advances in banking technology.

Key themes

The goal of this paper is to guide banks seeking to realize the opportunities presented by DCL, help them see through and beyond the hype and disillusionment and position themselves appropriately, starting now (and avoid becoming part of the hype themselves).

To help them do this, we've set out to address a number of key themes, by answering the following questions:

- What benefits can DCL bring beyond existing technology for banks?
- Why are banks so interested—and why is there so much hype?
- Is the hype justified, and what could go wrong?
- How will the public DCL develop?
- What are regulators doing?
- What are banks doing and why are they acting now?
- What are start-ups doing?
- What are the payments use cases that would benefit from the technology?
- What payment services could a bank offer?
- What actions does a bank need to take today?

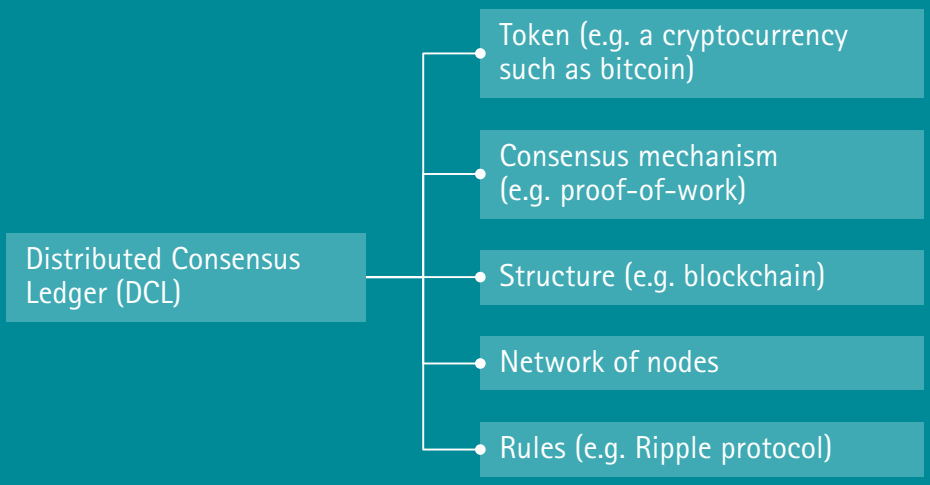
This paper is designed to provide a broad view of the opportunities and status of DCL technologies for payments, and to clarify some of the key DCL terms and concepts, and their applicability to payments. Consequently, it can be used both for insights and as a reference document, and we have covered additional topics in the Appendix:

- How does a distributed consensus ledger (DCL) work?
- What are the differences between a private versus a public DCL?
- What does a DCL architecture look like, and how can a bank start developing it?
- What should be tested in a DCL proof-of-concept?

Terminologies defined

Distributed consensus ledger (DCL) is a more accurate term to describe distributed transaction databases with replicated data integrity maintained by cryptography, than generic use of terms that describe specific features, such as blockchain, or cryptocurrency, as shown in Figure 1.

FIGURE 1. Defining Features of a Distributed Consensus Ledger



Blockchain—The blockchain is the public ledger of all Bitcoin transactions. Transactions are added by miners to the ledger in blocks which are linked sequentially in chronological order. Other ledgers often developed from copies of the Bitcoin software code also use blockchains.

Cryptocurrency—A cryptocurrency is a token on a distributed consensus ledger transaction that represents a medium of exchange and a unit of account. Sometimes referred to as "digital currency" or "virtual currency".

Digital wallet—a digital wallet is an online or mobile account used to initiate ledger transactions (payments), and to access ledger balances and transaction history.

Distributed consensus ledger (DCL)—DCL is a ledger of transactions replicated on multiple nodes on the internet or a virtual private network (VPN). Each transaction is signed uniquely by the user's private key. Transaction integrity and confirmation are enforced through cryptography, agreed through the consensus of DCL nodes. DCLs can be constructed using blockchains, but other structures are possible.

Miner—a miner is a node on a DCL using the blockchain which solves cryptographic algorithms to confirm a transaction, and adds it to the blockchain in consensus with other miners.

Multi-signature (multi-sig)—transactions are those signed by more than one private key.

Node—a server that holds a replicated copy of a DCL and may act as a participant in a cryptographic consensus process.

Public and Private DCLs—a public DCL is permissionless, open to all. Anyone can access it, set up a node and participate in consensus cryptography. A private DCL is a closed group of nodes who set their own rules on consensus, access and participation.

Public and Private Keys—a private key is a secret key held in a digital wallet used to sign transactions, linking them uniquely to the wallet (and its owner). A public key is derived from a private key and is the public address for other wallets to send transactions.

Sidechain—an alternative DCL designed for a specific purpose, that is pegged to another DCL, typically the Bitcoin blockchain, to leverage the liquidity and consensus mechanism of the other DCL. See Appendix 2 for more detail.

What benefits can DCL bring beyond existing technology for banks?

The key characteristic of DCLs is that they enforce a common set of processing and ownership rules across a disparate set of organizations and entities. However, while this means the technology can solve a particular issue, it doesn't mean it is applicable or valuable in every context.

Looking specifically at payments, part of the hype around DCLs is a view that the payments system is fundamentally broken—slow, inefficient, paper-driven—and that DCLs can provide a way to fix it. However, while this may be true of some payments systems at a national level, and for cross-border, it is not the case universally. For example, non-DCL technology (relational database driven) is already in use in the UK and Denmark supporting ubiquitous, high-volume, low cost, real-time payment systems.

A step forward—on several fronts

That said, even a conservative assessment confirms that DCLs can make a difference compared to existing technology. For example, they enable democratic, distributed, evenly-balanced control to be implemented and exercised in situations where it's currently not possible or easy. These include cases where oversight by a central authority is not feasible—such as with international payments—or where a centralized control point, restriction, or intermediary(s) exist that create unnecessary inefficiencies, costs and barriers, for example with correspondent banking payments, card transactions and international remittances.

DCLs also go beyond the capabilities of existing technology by providing transparency where it has previously been impossible, or difficult to achieve. Examples include in anti-money laundering (AML)—an area where DCL's potential is attracting growing interest and investment. For example, the London-based start-up Elliptic has harnessed the underlying technology supporting its visualization of the Bitcoin ecosystem to develop a suite of AML services.

A further point of differentiation for DCLs is that they enable counterparties to transact or share information in a trusted way, where they do not know each other. This means banks across the world can do business with each other securely and directly without an existing relationship.

All of these advantages over existing technologies mean DCLs can enable new business models that would not otherwise be possible or practicable. They highlight why DCLs will have a big impact on the payments industry and why banks need to act now to address them.

What are the payments use cases that would benefit from DCL technology?

No central control—where central control or a central database are not easy or feasible, such as:

- Cross-border interbank settlement
- Cross-border direct debit mandates, letters of credit
- Look-up for cross-border BICs and IBANs to validate counterparties on payment initiation

Intermediaries—where one or more intermediaries in a payments chain can be bypassed:

- International payments (correspondent banking)
- On-us payments across unconnected business units of the same organization
- Card payments—ecommerce and at point-of-sale, particularly cross-border card payments

Access to counterparty information:

- Transparent access to counterparty agreements such as direct debit mandates
- Transparent access to counterparty data for destination validation, AML, sanctions and KYC checks

Transacting at risk, between parties with no regular or previous relationship:

- Trade finance
- International payments
- Interbank settlement

New business models:

- Micropayments
- Internet of things—machine-to-machine payments, smart meter payments
- Fiat currency payments using a DCL
- Bitcoin debit cards
- Loyalty payments

Why are banks so interested—and why is there so much hype?

The rise of Bitcoin has marked a breakthrough in the use of cryptography for financial transactions. And as banks become digital—digitizing their processes, products and services—DCLs have strong potential to provide the technology needed for the digital bank of the future, not just in payments but also in areas such as securities processing.

The venture capital (VC) industry has spotted this potential, and as a result has been investing heavily in the DCL sector. The VC investment has in turn drawn in the banks, catalyzed by their broader focus on FinTech and their internal innovation laboratories working with technologies such as the blockchain. Coincidently, these developments are taking place at the same time as real-time payments is becoming a key dynamic in the payments industry. DCLs have the potential in the medium term to provide near real-time capability for banks (although other more mature technologies are already available and in use), and in the near term to provide a new mechanism for interbank settlement to support real-time payments clearing. See "Real-time Payments for Real-time Banking".

A further consideration is that many of the issues that DCLs are able to address are actually sources of revenue for the banks, so they need to be careful how they harness DCLs, reducing costs and creating new revenue streams to counterbalance any revenue disruption from DCLs: examples include 'float revenue' (from slow clearing), wire fees, card fees, foreign exchange (FX) spreads, and fees for letters of credit. This is particularly the case in correspondent banking, where reciprocal arrangements mean that banks can generate significant business acting as a payments gateway into their local market, and also get low cost access to banking services for their customers in other markets through their correspondents.

Customers are increasingly shopping around outside the banking industry for products and services traditionally provided by banks, such as lending, and payments is no exception. Banks face potential challenges from new entrants using DCL technology—and they need to understand how real these challenges are, and how to seize the related opportunities. Finally, corporate customers may start to use DCLs, or start demanding cryptocurrency products and services. Banks need to work out how to respond, and to identify where new revenue, service and relationship opportunities may exist.

All these points reinforce why DCLs are relevant to the payments industry and why banks need to act now.

Is the hype justified, and what could go wrong?

Recently, the interest in DCLs from banks and VC investors has been contributing to the hype. Bold claims have been made about the potential impacts, typically stating that DCL technology could reduce banks' infrastructure costs by billions of dollars through eliminating central authorities and bypassing slow, expensive payment networks.

However, the reality is that, with the exception of Bitcoin itself, no successful businesses, breakthroughs or market traction—in terms of business results and mass adoption—have as yet emerged with DCLs. Experience of using the technology for commercial purposes is very limited, and much more is required to provide the evidence and compelling analysis required to determine the true potential of DCLs.

The myth of inefficient payments systems...

Furthermore, views of the potential of DCL in payments also vary widely. For example, one of the reasons for the strong advocacy for DCL in the USA is that payments—both domestic and international—are relatively slow and often expensive. A typical refrain is "it's faster and cheaper to send cash by UPS than electronically."

While this may ring true for some aspects of payments in the USA, it isn't the case elsewhere—issues impacting the cost and speed of payments have already been solved. Cross-border payments can now be T+1 (next day), and real-time nostros in correspondent banking are feasible. And many countries already have real-time payments systems—such as the UK, with the Faster Payments scheme—while many more, including the USA, are set to migrate to them over the next few years.

...is compounded by other misconceptions

Misunderstandings around a number of other factors have further added to the hype around DCLs. For example, the notion that centralized payments clearing and settlement is inherently inefficient and costly. This may be true in the securities industry where ownership of assets is transferred through clearing and settlement, a slow process with many intermediaries, but in payments the reverse is often the case. Payments clearing and settlement are often highly efficient and cost effective due to the substantial scale economies, the high percentage of transaction netting and ubiquitous reach they achieve. The UK's Faster Payments system processes more than one billion real-time payments annually, on an efficient, resilient infrastructure that contributes only a small part to the end-to-end transaction costs for the banks that use it.

A further misconception is that centralized clearing and settlement uses a centralized ledger. This is not really the case: accounts are held by the core banking systems operated by individual banks, where cleared transactions are posted; and while settlement does typically use a centralized ledger, it is relatively simple, involving one account for each settling bank, and a few transactions per day between them. Also, while fees for RTGS (wire payments) can be high for customers, the cost to banks is minimal. And in this age of analytics and big data, DCLs are not—as many assume—anonymous, due to their transparency and permanency: witness the FBI's seizure of bitcoins (subsequently auctioned off) when it shut down Silk Road in 2014 and the successful prosecutions that resulted.

...and by high, and often over-optimistic expectations

Finally, there are different constituencies who feed off each other, multiplying the hype. These groups include economists who take the efficiency and transformation claims at face value and apply them holistically to the financial services industry without knowing specifically where the technology is applicable and where it isn't; technologists and start-ups new to payments, who over-simplify how to transform them without understanding the realities of AML, sanctions, liquidity, risk, money transfer, building merchant networks and so on, and who are over-optimistic on how to scale from working prototypes to industrial use; payments experts 'going with the flow' as they enjoy new-found attention and investments; and venture capitalists who sense something big is developing and are placing multiple bets in the hope of finding a 'unicorn'.

Mapping DCL to cost benefits...

If there is a case for genuine DCLs used universally for payments, it would involve the payment account becoming a DCL wallet, and require radically different core banking systems to run customers' current accounts. This approach may indeed have the potential to save costs on a massive scale, since core banking systems are expensive to maintain and run. However the current hype has seen little or no discussion of this concept.

Given the widespread misunderstandings, it's clear that if DCLs are to be used in payments for cost and efficiency reasons, it's important to understand where banks currently incur costs in payments. These essentially arise in five areas:

- Manual processing (resulting in low straight-through-processing, STP), including costly customer investigation and enquiry processes
- Third-party fees in the payments chain
- Fraud losses and anti-fraud, AML, sanctions, and know-your-customer (KYC) processes, and regulatory change
- Complexities of cross-border settlement between banks
- Legacy systems and processes, often with overlapping and duplicate functions, data and processes.

DCLs can address each of these areas, but the key challenge is to identify where and how DCLs can be used in a way that is superior to technology already used widely in financial services (such as standard database and web services technology). Once the industry has a firm grip on this challenge, it can replace the hype with facts and evidence, and start to use DCLs to build the payment systems of the future.

Addressing this challenge is another reason why banks need to focus on DCLs and act now.

How will DCLs develop?

DCLs will develop as both public, permissionless DCLs, which anyone can access, and as private, permissioned DCLs set up within an organization, or between a closed group of organizations who agree on its rules. Judging by their recent media statements, the private model seems to be the one of most interest to banks at the moment. There will also be business models that rely on interactions between public and private DCLs, and on variants known as sidechains (see Appendix 2). One possible scenario is a dominant DCL such as Bitcoin, which is liquid and in widespread use, with a proliferation of sidechains for specific purposes linked to it, leveraging its liquidity and its miners.

Bitcoin, with its blockchain, is by far the largest public DCL, although there are many derivatives or forks of Bitcoin with their own token, or currency, for example Litecoin. Other DCLs built from scratch run on open networks, but are designed for organizations to set up and use as private DCLs, for specific purposes, such as Ripple for international payments or Ethereum for smart contracts.

Looking to the future, all the signs are that Bitcoin will continue to grow: the more it is used, the stronger and more self-sustaining it becomes. If, however, its growth stops or reverses, this would effectively signal the end of Bitcoin. Other DCLs will also grow if use cases are found that benefit directly from the technology. Despite this, it could take at least 10 years for Bitcoin, and other public and private DCLs, to become fully established—which means that even in five years' time DCLs will still be in their infancy.

As a comparator, PayPal is one of very few payment mechanisms that have survived from hundreds that emerged in the dot com boom. It has been growing for 15 years and is clearly a huge success with a bright future, but it still has a long way to go to build market share comparable with card networks.

DCLs will develop both for payments and for other uses. For payments, at least one cryptocurrency such as Bitcoin may develop into a global currency independent of government control (although users will still be subject to their government's financial crime measures). Over time, cryptocurrencies may become an established and useful tool in international trade and payments, working alongside and with fiat currencies rather than replacing them.

A proliferation of DCLs supporting different cryptocurrencies is possible, with each meeting different needs and values—many are already launched (for example Litecoin, Dogecoin), some may endure, while new cryptocurrencies on government-run DCLs, for example "Fedcoin" have been discussed openly by central banks including the US Federal Reserve and the Bank of England. If these variants succeed, it is easy to imagine other cryptocurrencies appearing (in sidechains—see Appendix 2) for specialist needs—"soccercoin", "moviecoin" etc.

In this future environment, fees will become a critical but largely voluntary, market-driven factor in the confirmation and consensus of public DCL transactions. In general, the higher the fee a sender chooses to pay, the faster the speed, the greater the level of security, and the more versatile (or 'smarter') the transaction.

At the same time, wallets will become rich in features, including elements such as support for multiple cryptocurrencies, dynamic transaction fees, advanced sending options, and the ability to prevent transactions from being initiated with unconfirmed funds. KYC on wallets will be robust, and it is possible that a "meta" DCL (perhaps as a sidechain) will be used to register wallet addresses and identity information to facilitate authentication of counterparties for identity, KYC, AML and sanctions checks. Adaptation and improvement will be facilitated by the use of sidechains, with a mechanism for upgrades and protocol evolution through an ongoing democratic process of change consensus.

Over time, as demand and usage grow, the capacity and speed of DCLs will increase. As happened with the internet, where broadband catalyzed mass-adoption and new uses such as social-media, DCLs will need a similar technology breakthrough to bring widespread adoption over the next 10 years. With this, regulators will progressively legitimize the use of Bitcoin and other cryptocurrencies, with banks and non-banks offering services in it. As this evolution continues, a wide range of DCL-enabled use cases will become common, possibly including:

- Fiat payments using cryptocurrency technology
- Correspondent banking/cross-border payments for both fiat and cryptocurrency payments using DCLs
- Distributed interbank settlement for real-time payment clearing systems
- New business models, for example using micro-payments
- Integrated or interoperable private and public DCLs
- Clean (AML, sanctions-checked) transactions
- Cross-border destination-based validation of payment counterparties and their accounts or wallets
- Internet of things—each device on the internet could have its own digital wallet to operate autonomously, initiating and receiving payments
- Seamless back office processing of data, particularly data duplicated across organizations, including transaction data and reference data

Initial market adoption and success of DCLs for payments will be a lot slower than many currently expect. But as DCL adoption takes off, its impact will spread faster and deeper than many realize. Banks must act now or risk being overtaken by events.

What are regulators doing?

Regulators are still wary of DCL technology.

Their position and responses are evolving, but those in countries such as the USA and UK appreciate that it is preferable to regulate it and enable innovation, rather than to try and ban it. Some regulators are also conscious that regulation needs to be proportionate to enable innovation to take place, but this varies, with for example, Europe taking a lighter approach than the USA (where New York has introduced Bitlicenses and California has draft law at an advanced stage).

A key area of focus for regulators is AML. For example, in June 2015 the FATF issued its recommendation to identify and mitigate the money laundering and terrorist financing risks and other crime risks deriving from virtual currencies payments product and services.[2]

The regulatory landscape for cryptocurrencies is fast changing, and to keep pace refer to agencies such as Coindesk that track and report on latest developments.

What are banks doing and why are they acting now?

Various banks around the world are setting up innovation labs focused on exploring potential use cases for DCL/blockchain technology, with some banks focusing mainly on Ripple for international payments, and others on more general use cases requiring smart-contracts, typically focused on Ethereum.

Examples of initiatives to date include Westpac in Australia partnering with Ripple and pilot-testing a proof of concept for low-value cross-border payments with its staff; Barclays running a 90-day accelerator program with Safello, and agreeing a deal with Safello to work on proof of concepts for testing banking services on the blockchain; UBS developing a "utility settlement coin" for interbank settlement; Citi and BNY Mellon creating currencies, respectively called "Citicoins" and "BK Coins" as a corporate recognition program that can be redeemed for rewards; and major banks around the world joining forces with a FinTech company called R3 to agree an underlying DCL architecture for financial markets.

What are start-ups doing?

At the same time, start-ups across the world are developing and rolling out a wide range of solutions that tend to focus on specific points of the payments value chain.

These include:

- **Digital wallets**, for storing and accessing cryptocurrencies and making payments e.g. Armory, Blockchain.info
- **Cryptocurrency ATMs**, for uploading cryptocurrency onto digital wallets at physical locations, purchased by physical cash, and to convert cryptocurrency back into cash e.g. Lamassu, Genesis
- **Cryptocurrency exchanges**, for buying and selling cryptocurrencies electronically with fiat currency e.g. Coinfloor
- **Merchant acquiring**, for providing merchants with capabilities to accept cryptocurrency payments (and convert them into fiat currency if required) e.g. Bitpay
- **Remittances and bill payments** for paying bills or funding bank accounts cross-border e.g. Bitwa.la
- **Debit cards**, for standard card payments in fiat currency funded by an underlying cryptocurrency account e.g Xapo, ItBit
- **Smart contracts**, for registering and managing custody over assets in a DCL e.g. Ethereum (not specific to payments, but could be used to administer conditional payments based on letters of credit and other trade finance instruments)
- **Analytics**, to provide insights on DCL activity, for example for identity and AML e.g. Elliptic (also a Bitcoin custodian)

To date there are few companies focusing on holistic, payment industry solutions—one exception is Ripple (see information panel) for global cross-border payments as an alternative for correspondent banking.

Ripple

Ripple is a federated payments system, using its own distributed consensus ledger, supporting near real-time payments. It is an open system, but payments are made between private groups of nodes (typically banks) on the DCL. Ripple is designed to be integrated with existing bank systems, working with them as an alternative to correspondent banking for cross-border payments. It can also be used between local banks for domestic payments.

Financial institutions acting as market makers provide settlement, liquidity and foreign exchange services, enabled through accounts at the participating banks.

Ripple has its own cryptocurrency, XRP ("ripples"), designed to prevent spam transactions and enable cross-border payments in illiquid currencies. Otherwise, payments are typically processed in fiat currencies.

What payment services could a bank offer?

Banks have two opportunities to use DCLs for payments:

1. Use DCL technology to facilitate payments in fiat currencies, in effect, using the technology to improve existing payment, cash management and trade services (lower cost, faster, greater reach)

2. Use DCL technology to provide payment, cash management and trade services in "naked" cryptocurrencies

For payments in fiat currencies, the services to customers will be similar to existing services, although there is opportunity to provide alternatives to card payments at point-of-sale and in ecommerce, paying directly out of bank accounts. Additionally, there are opportunities to provide new liquidity and interbank settlement services, such as market making services in the Ripple network.

For "naked" cryptocurrency payments, regulatory uncertainty restricts banks in the payment services they can offer, and customer adoption is a big unknown, limiting bank appetite to develop them. However, the regulatory environment is changing and cryptocurrencies are likely to be permitted by regulators when the right AML, KYC and licensing controls are in place. It is also self-evident that a global payments system using a universally accepted, stable, global currency is highly attractive for retail commerce, international payments and remittances, trade and corporate cash management. This means such a system will surely develop (Bitcoin or otherwise) in an appropriate regulatory environment.

Banks should therefore start thinking about the services to provide retail and corporate customers using DCLs and cryptocurrencies, should the market shift in this direction, covering both retail and corporate customers cryptocurrency payment services. These could include:

- **Digital wallet solutions**—banks can issue digital wallets, and in effect become the custodians of the private keys their customers use to sign DCL transactions. These wallets could be used for making payments across all channels including using NFC at point-of-sale
- **Cryptocurrency deposit services**—it is risky for consumers to hold large sums in a digital wallet (in the same way it is risky to hoard cash under a mattress or in a safe), so banks can offer deposit, or custody services for cryptocurrencies for customers to transfer small quantities to their digital wallets as needed
- **Exchange services**—to enable bank customers to freely exchange cryptocurrencies and fiat currencies
- **ATMs**—to allow customers to buy and sell cryptocurrencies using physical cash
- **International payments**—to allow customers to send money cross-borders
- **Corporate cash management**—to support corporates in managing cash, including sweeping and pooling into cryptocurrencies and for near real-time cross-border transfers
- **Analytics**—to provide corporate customers with balance and cashflow information and forecasts
- **API services**—to allow third parties to have access to customer wallets through APIs, embedding them into their own applications and services

What actions does a bank need to take today?

To position itself as a leader in the industry-wide drive to adopt and capitalize on DCL technologies, Accenture believes a bank should take five steps as a matter of urgency.

1. Organize

- Appoint a single DCL lead for the whole enterprise
- Create a cross-business unit/IT team to avoid duplication and siloed innovation across the bank
- Create a R&D function—an innovation lab focused on DCL, covering payments, securities and so on
- Allocate a central budget, funded by individual business units if necessary, but avoiding duplicated/siloed investments and teams
- Implement governance and processes to keep business units (product development, relationship management, operations) engaged with the R&D function, including implementing a qualification process for developing ideas into capabilities that business units support

2. Evolve a strategy and architecture

- Start developing a strategy—but keep it agile and high level, initially focused on developing capability and generating know-how and experience
- Split the payments part of the DCL strategy into using DCL technologies for fiat currency payments, and using it to provide "naked" cryptocurrency services to retail and corporate customers
- Examine the impact of DCL on revenue as well as costs, and formulate an approach for generating revenue using DCL
- Use the R&D experience to regularly inform and guide the strategy
- Define a DCL architecture—identify business processes to change, IT systems to replace, and points of integration (customer, business and IT); align with the enterprise architecture for legacy and non-DCL technology
- Develop an approach to private versus public versus shared DCLs
- Keep the strategy focused on the strengths of DCLs—avoid "re-inventing Bitcoin" or using DCL technology where it doesn't add clear value over existing technologies

3. Build/buy DCL capability

- Educate IT and business staff (including providing hands-on experience, for example installing Bitcoin ATMs in bank buildings and accepting bitcoins in staff restaurants)
- Build capability, in an agile way
- Acquire start-ups and their capabilities such as digital wallets and cryptocurrency exchanges

4. Experiment and develop experience

- Mine cryptocurrency to understand the dynamics of consensus processes
- Develop proof-of-concepts. For further insights into what to test in a proof-of-concept, please see Appendix 4 on page 23
- Develop initial products and services using a DCL and test with customers, focusing first on payments with fiat currencies, before products and services using "naked" cryptocurrency

5. Engage with customers, FinTech and regulators

- Get licensed in jurisdictions relevant to the bank with cryptocurrency regulations e.g. New York
- Focus on DCL companies as a distinct bank corporate customer sector to serve (alongside existing segments for money services businesses and electronic money institutions)
- Keep close to relevant regulators—to inform, guide and educate, especially on R&D findings
- Incubate innovative start-ups building DCL capabilities
- Test and use start-up capabilities—adopt or drop these depending on their relevance, effectiveness and potential
- Engage with customers to test ideas and proof-of-concepts, and to understand their developing requirements and demands

APPENDIX 1: How does a distributed consensus ledger (DCL) work?

A distributed consensus ledger is a ledger of transactions that is replicated on multiple servers, or nodes on the internet. Transactions are initiated and accessed through a digital wallet which uses the user's private key to sign and access the user's transactions. Transactions are typically stored sequentially in blocks that are linked together (hence the term "blockchain", although not all DCLs use this structure).

Taking Bitcoin as an example, the sum of the value of transactions signed by the user's private key equals their total balance of bitcoins. For Bitcoin, the current sum of balances across all private keys is about 15m BTC, the total number of bitcoins in circulation. This number is growing, as miners are rewarded with new bitcoins when they create new blocks in the blockchain. However, the Bitcoin protocol is configured so that the more bitcoins are created, the slower the rate of creation, and the overall total will never exceed 21m BTC.

On a blockchain, transactions are linked in sequence. For example, if a user has received 1 BTC and then pays someone 0.2 BTC, the blockchain will contain the 1 BTC transaction (input) and a 0.2 BTC transaction (output) signed by the beneficiary private key, and a 0.8 BTC transaction (output) signed by the user's private key. The output transactions are linked to the input transaction(s).

Transactions are confirmed as unique and authentic through cryptography. Miners, or nodes on the distributed network, solve cryptographic algorithms, and when a sufficient number agree a transaction is genuine, the transaction is confirmed and irrevocably added to the blockchain.

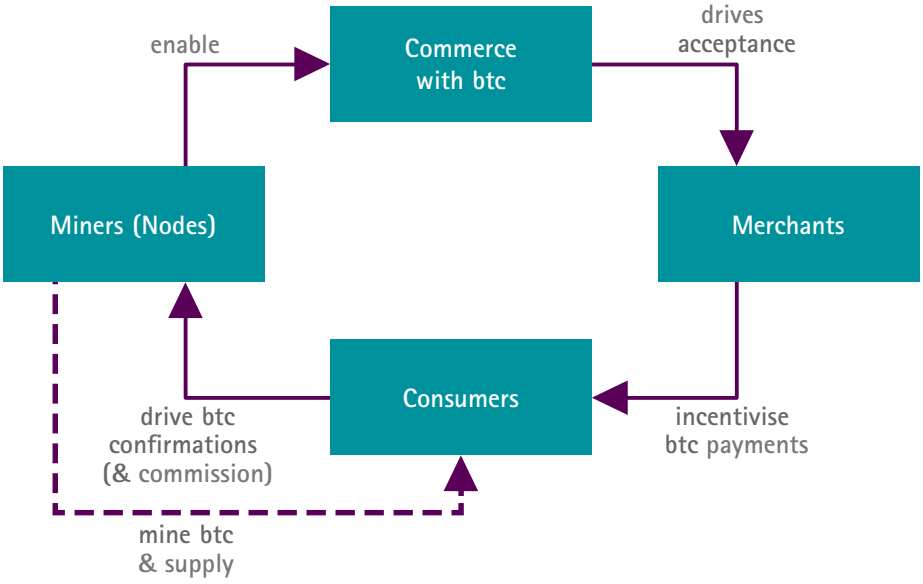
In Bitcoin's case, miners compete to confirm transactions because the first to do so receives a fee (in BTC); miners also received BTC for creating the transaction blocks. This is known as 'proof of work'—miners win the right to participate in this consensus process through proving they have incurred computational cost (electricity). The more computational effort they make, the more blocks they can create, and the more reward in bitcoins they get.

Other cryptographic consensus mechanisms exist in other DCLs, such as 'proof of stake', where miners have the right to participate based on the amount, their stake, of cryptocurrency they own. Typically, the more they own, the more blocks (or equivalent) they can create.

"Proof-of-work" DCLs function because miners are rewarded for creating blocks and confirming transactions. "Proof-of-stake" DCLs function because miners have a stake in the DCL (for example a private DCL), and it is in their self-interest for it to work. However, due to the high computational effort required in "proof-of-work" DCLs, these are typically much slower in confirming transactions than "proof-of-stake" DCLs.

Bitcoin is a self-reinforcing, self-sustaining DCL—the more it is used, the stronger it becomes (see Figure 2). It is truly democratic, as not only are transactions confirmed through consensus, but the whole DCL and changes to it evolve through consensus.

FIGURE 2. Bitcoin's self-sustaining, self-reinforcing ecosystem founded on the value of BTC



DCL ledger networks can be either public or private. Public DCLs, such as Bitcoin, are open to all, meaning anyone can join them and use them to make and receive transactions, and if they so wish, anyone can become a miner. They require the "proof-of-work" mining process to reward miners, since otherwise there is no incentive for any miner to create blocks and confirm transactions, and the DCL would not function.

Private DCLs can be set up internally within an organization, or between a closed group of consenting organizations. These are also known as permissioned DCLs. With these DCLs, the participating organization(s) set the rules, and the validation of transactions can be done without intensive mining, for example through "proof-of-stake". Private DCLs function because it is in the self-interest of the participating organization(s) to make them function to achieve their mutual objectives for the DCL. Participating organizations can have commercial agreements between them, but—in contrast to the "proof-of-work" on public DCLs—they do not need to prove to each other they have consumed excessive computational power in creating blocks and confirming transactions.

The key features of a public DCL can be summarized as follows:

- Replicated ledgers—multiple copies of the DCL on participating nodes
- Resilience (through replication)
- Distributed control
- Owners have full control over their assets (for example bitcoin balances) on the ledger
- Transactions are made on finite or countable resources (for example bitcoins) held on the ledger
- Consensus decisioning
- Transparency—all transactions are visible
- Private keys uniquely identifying the owner of each transaction
- Permissionless innovation—anyone can use the DCL for their own innovations
- Permissionless participation
- Historic transactions are unalterable and permanently available (unless the consensus allows changes)
- Borderless—no national rules, no data residency rules
- However, inefficient use of computing resources, specifically excessive consumption of disk space and computation power

Private DCLs share many of these features. However full control is in the hands of the participating organizations, not widely distributed, and they use computational resources more efficiently.

DCLs can be used for on-ledger or off-ledger purposes. Payment in bitcoin is an example of on-ledger use – bitcoin balances are held on the Bitcoin blockchain, and payment transactions transferring balances between private keys (and digital wallets) can be made. An off-ledger transaction is where an off-ledger asset such as a corporate bond is assigned to a private key on a DCL, using, for example a nominal bitcoin sum (0.00000001 btc). An index reference to the official location record (custody database) of this off-ledger asset is embedded (hashed) into the DCL transaction, meaning the DCL can be used for managing and transferring ownership of assets. This is the subject of smart contracts that can manage this process, and since it is more relevant to capital markets than payments, it is not explored in this paper—although smart contracts may be applicable to trade finance.

APPENDIX 2: Public versus private DCLs

There is much discussion around the pros and cons of public versus private DCL. Using a simple analogy, the public DCL is analogous to the internet, a private DCL to an intranet, and a shared private DCL to an extranet (see Figure 3). The following table summarizes the technical differences:

Public DCL	**Private DCL**
Permissionless ledger—anyone can use it and innovate with it	Permissioned ledger—only a closer group of organizations can participate
'Proof of work' consensus	Custom consensus engine—rules set by the participating organizations
Public nodes	Private nodes (closed group)
Cryptocurrency token	Optional token
Open wallet access/internet	Closed wallet access/VPN
Cost of using it is low	All running costs need to be met by the participating organizations

Private DCLs need to be developed to produce benefits that other centralized technologies cannot already deliver. This is a key challenge: there is a risk that private, walled garden DCLs will reinvent an inferior form of Bitcoin, similar to the walled garden retail computer and email networks in the 1990s which did not survive the rise of the world wide web. It is possible that public and private DCLs will co-exist and interact with each other, although it is too early to forecast how this may develop for payments (and other uses).

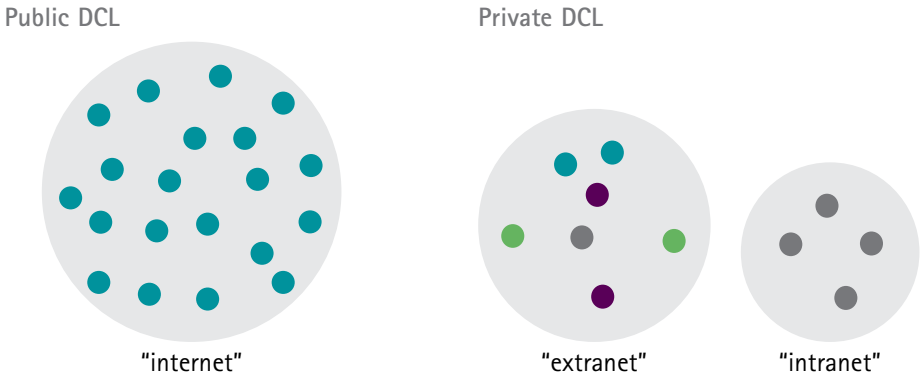
In addition to public and private DCLs, sidechains—a form of off-ledger construct—are a growing consideration.

These are separate DCLs (typically private) set up for a specific purpose. Bitcoins (or other DCL cryptocurrency) are assigned to the sidechain, and locked on the main Bitcoin blockchain. They remain locked until the sidechain has finished with them, meanwhile allowing the sidechain DCL to operate to its own rules and requirements. Example use cases for sidechains include:

- Tracking and management of payments to suppliers on a complex building program
- Managing the allocation, sale and resale of tickets (sporting events, concerts etc), enabling a market in the tickets but preventing them from being resold at excessive prices (for example by ticket touts)
- Managing and monitoring the disbursement of charity donations
- Registering wallet addresses and identity information to facilitate authentication of counterparties for identity, KYC, AML and sanctions checks
- Distributed interbank settlement for real-time payment clearing systems

An analogous example of a sidechain are chips at a casino—exchanged for fiat currency, with a value pegged to the currency, they are used for playing according to the casino rules, and are exchangeable back into fiat currency.

FIGURE 3. Public versus private ledgers



- Permissionless ledger
- "Proof " consensus
- Public nodes
- Cryptocurrency token
- Open wallet access/internet

- Permissioned ledger
- Custom consensus engine
- Private nodes (closed group)
- Optional token
- Closed wallet access/VPN

APPENDIX 3: Banking architectures for DCLs

What does a DCL architecture look like, and how can a bank start developing it?

In developing a banking architecture using DCLs, a bank has to take several important considerations into account. At the highest level, it needs to decide whether to go for a private or public DCL, or a combination, and whether to use DCLs for just fiat currency payments, or to develop "naked" cryptocurrency payment services as well.

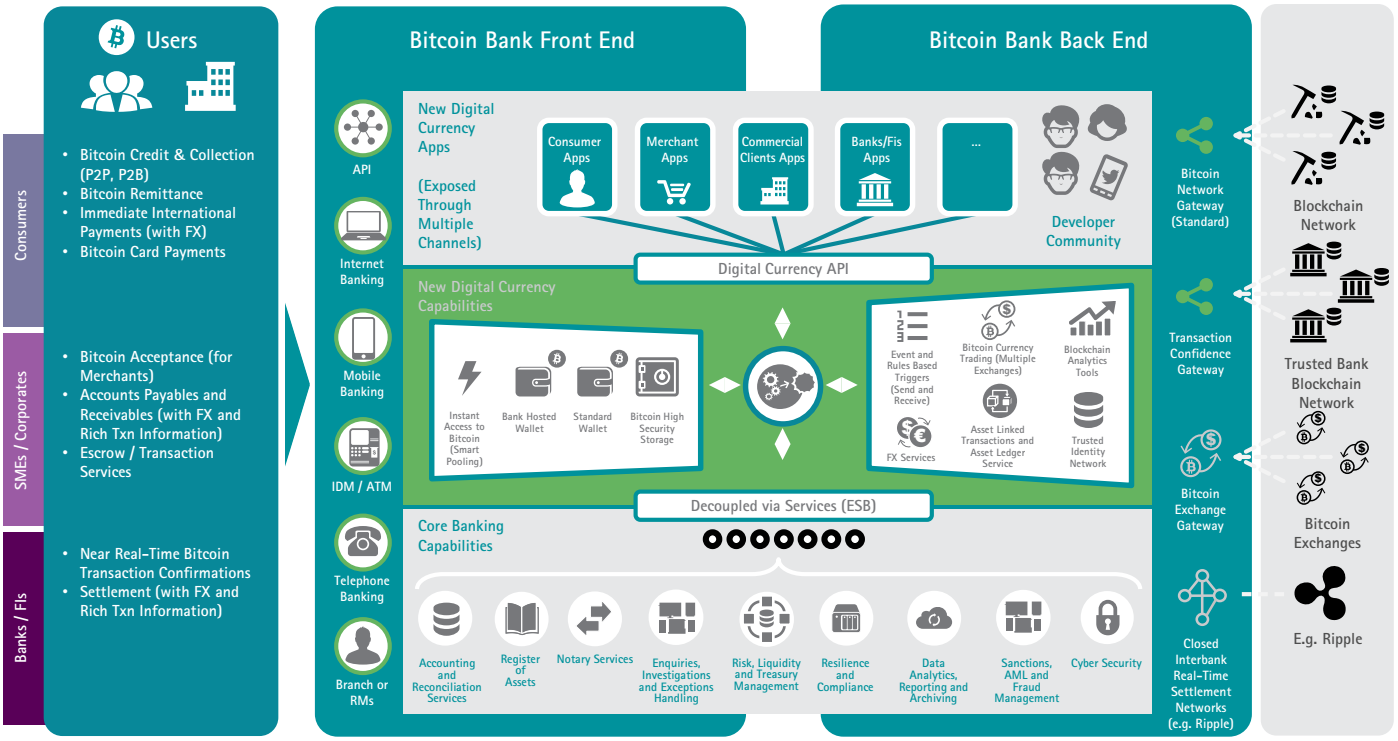
It must also work out the optimal balance between DCL technology and existing, centralized technology—deciding which is more appropriate in which area, and where and how they will coexist and interact. The bank needs to establish how interaction and interfaces with external DCLs will take place, and choose between architecting for crypto-payment services (e.g. Bitcoin wallets) versus architecting to replace technology with a DCL for fiat payment processing. Tokenization and addressing also need to be determined.

These decisions are complicated by the immaturity of DCL technology and the capabilities currently available.

Architectures drafted now need to evolve as understanding and experience of DCLs grows. For example, in the current trend to move to real-time payments, it would be risky to base these on current DCL technology, but within two years DCLs such as Ripple could be gaining traction. This highlights the need for banks to conduct R&D in DCL technology and run proof of concepts using it to develop experience and inform strategies and architectural thinking.

At Accenture we have developed high-level DCL architectures for payments to help guide our clients. Figure 4 is an example, showing a schematic for a Bitcoin Bank Architecture Model to support payment services using Bitcoin.

FIGURE 4. The Accenture Bitcoin bank architecture model



APPENDIX 4: What to test in a proof-of-concept?

With DCL technology in its infancy, one route a bank can take to analyze its potential and participate in the current DCL discovery phase to explore the technology by running a proof-of-concept.

Successful proof-of-concepts need to be grounded in business relevance, and be planned as part of a wider strategy or roadmap initiative. Follow-through plans are important, to build on momentum generated by the outcomes, discoveries and learnings from the proof-of-concept.

Accenture has defined proof-of-concepts for our own clients covering Ripple and blockchain DCLs, and we have a methodology and frameworks in place specific to payments and cash management.

The first step in planning a proof-of-concept is to determine its objectives—for example, "to determine how to use a DCL for cross-border payments, define a revenue model and quantify the risk, settlement, and cost benefits".

The second step is to define the scenarios that the proof-of-concept will test, for example cash pooling, intra-group money movement, inter-branch payments for the same bank operating in different countries.

The third step is to outline the end-to-end payment value chain, from authentication to payment initiation, authorization to clearing, and then settlement, posting and confirmation. For each step of the chain, more detailed events and conditions to explore should be defined, both for existing practices (for example restricting access to customer payments to their branch location) and new ones required by processes required for the DCL.

Finally, the technology-related factors can be determined such as the DCL to use, private or public configuration, the consensus mechanism, whether a sidechain solution is needed, use of smart contracts, integration requirements with internal systems, user interfaces (for example to initiate payments) and sandbox configurations.

The trick is to plan holistically in this way, with participation across business units, operations and IT, with sufficient detail to ensure the proof-of-concept is set up for success. The proof-of-concept should be run as an agile project, where further detail and tests can be elaborated as it progresses.

Contact us

Massimo Proverbio
Senior Managing Director
Accenture Payment Services—Global Lead
massimo.proverbio@accenture.com

David Link
Managing Director
Accenture Payment Services—Asia Pacific
david.c.link@accenture.com

Jeremy Light
Managing Director
Accenture Payment Services—
Europe, Africa and Latin America
jeremy.light@accenture.com

Robert Flynn
Managing Director
Accenture Payment Services—North America
robert.f.flynn@accenture.com

AUTHORS

Sarah Fielder
Manager—Emerging Technologies
Accenture Technology
sarah.l.fielder@accenture.com

Jeremy Light
Managing Director
Accenture Payment Services—
Europe, Africa and Latin America
jeremy.light@accenture.com

FOLLOW US ON TWITTER

@BankingInsights

NOTES

[1] http://www.coindesk.com/state-of-bitcoin-q2-2015-price-gains-amid-euro-crisis/

[2] FATF—Guidance for a Risk-Based Approach—Virtual Currencies

ABOUT ACCENTURE PAYMENT SERVICES

Accenture Payment Services, a business service within Accenture's Financial Services operating group, helps banks improve business strategy, technology and operational efficiency in three key areas: core payments, card payments and digital payments. Accenture Payment Services and its more than 4,500 professionals dedicated to help banks simplify and integrate their payments systems and operations to reduce costs and improve productivity, meet new regulatory requirements, enable new mobile and digital offerings, and maintain payments as a revenue generator. More than 50 clients worldwide have engaged Accenture Payment Services to help them turn their payment operations into high-performing businesses. To learn more, visit www.accenture.com/us-en/banking-payments-services

ABOUT ACCENTURE

Accenture is a global management consulting, technology services and outsourcing company, with more than 358,000 people serving clients in more than 120 countries. Combining unparalleled experience, comprehensive capabilities across all industries and business functions, and extensive research on the world's most successful companies, Accenture collaborates with clients to help them become high-performance businesses and governments. The company generated net revenues of US$31.0 billion for the fiscal year ended Aug. 31, 2015. Its home page is www.accenture.com.

15-3586U/23-5908