Blockchain: Trust economy
Taking control of digital identity
BLOCKCHAIN, the shared-ledger technology that only a few years ago seemed indelibly linked in the public imagination to cryptocurrencies such as Bitcoin, is assuming a new role: gatekeeper in the emerging “trust economy.”

First, a bit of background. Last year’s Tech Trends report examined how maintaining the procedural, organisational, and technological infrastructure required to create institutionalised trust throughout an increasingly digitised global economy is becoming expensive, time-consuming, and in many cases inefficient.

Moreover, new gauges of trustworthiness are disrupting existing trust protocols such as banking systems, credit rating agencies, and legal instruments that make transactions between parties possible. Ride-sharing apps depend on customers publicly ranking drivers’ performance; an individual opens her home to a paying lodger based on the recommendations of other homeowners who have already hosted this same lodger. These gauges represent the codification of reputation and trustworthiness. We are growing accustomed to the notion that positive comments appearing under an individual’s name means we can trust that person.¹

In a break from the past, the trust economy developing around person-to-person (P2P) transactions does not turn on credit ratings, guaranteed cashier’s checks, or other traditional trust mechanisms. Rather, it relies on each transacting party’s reputation and digital identity—the elements of which may soon be stored and managed in a blockchain. For individuals, these elements may include financial or professional histories, tax information, medical information, or consumer preferences, among many others. Likewise, companies could maintain reputational identities that establish their trustworthiness as a business partner or vendor. In the trust economy, an individual’s or entity’s “identity” confirms membership in a nation or community, ownership of assets, entitlement to benefits or services, and, more fundamentally, that the individual or entity actually exists.

Beyond establishing trust, blockchain makes it possible to share information selectively with
others to exchange assets safely and efficiently and—perhaps most promisingly—to proffer digital contracts. This transforms reputation into a manageable attribute that can be baked into each individual’s or organisation’s interactions with others.

In the next 18 to 24 months, entities across the globe will likely begin exploring blockchain opportunities that involve some aspects of digital reputation. We’re already seeing companies that operate at the vanguard of the trust economy acknowledge blockchain’s potential. When asked during a recent interview about possible blockchain deployment by P2P lodging site Airbnb, company co-founder and CTO Nathan Blecharczyk replied, “I think that, within the context of Airbnb, your reputation is everything, and I can see it being even more so in the future, whereby you might need a certain reputation in order to have access to certain types of homes. But then the question is whether there’s a way to export that and allow access elsewhere to help other sharing economy models really flourish. We’re looking for all different kinds of signals to tell us whether someone is reputable, and I could certainly see some of these more novel types of signals being plugged into our engine.”

The blockchain/trust economy trend represents a remarkable power shift from large, centralised trust agents to the individual. And while its broader implications may not be fully understood for years

---

**Figure 1. Three levels of blockchain**

1. **Storing digital records**
   Blockchain allows unprecedented control of information through secure, auditable, and immutable records of not only transactions but digital representations of physical assets.

2. **Exchanging digital assets**
   Users can issue new assets and transfer ownership in real time without banks, stock exchanges, or payment processors.

3. **Executing smart contracts**
   Self-governing contracts simplify and automate lengthy and inefficient business processes.
   - **Ground rules** Terms and conditions are recorded in the contract’s code.
   - **Implementation** The shared network automatically executes the contract and monitors compliance.
   - **Verification** Outcomes are validated instantaneously without a third party.
to come, it is hardly a death knell for banks, credit agencies, and other transactional intermediaries. It may mean, however, that with blockchain as the gatekeeper of identity and trust, business and government will have to create new ways to engage the individual—and to add value and utility in the rapidly evolving trust economy.

**In blockchain we trust**

Given blockchain’s starring role in the Bitcoin hype cycle, there may be some lingering confusion about what this technology is and the value it can potentially bring to business. Simply put, blockchain is a distributed ledger that provides a way for information to be recorded and shared by a community. In this community, each member maintains his own copy of the information, and all members must validate any updates collectively. The information could represent transactions, contracts, assets, identities, or practically anything else that can be described in digital form. Entries are permanent, transparent, and searchable, which makes it possible for community members to view transaction histories. Each update is a new “block” added to the end of the “chain.” A protocol manages how new edits or entries are initiated, validated, recorded, and distributed. Crucially, privacy can also be selectively enforced, allowing varying degrees of anonymity or protection of sensitive information beyond those who have explicitly been given access. With blockchain, cryptology replaces third-party intermediaries as the keeper of trust, with all blockchain participants running complex algorithms to certify the integrity of the whole.

As the need for portable, manageable digital identities grows, individuals and organisations can use blockchain to:

**Store digital records:** To understand blockchain in the context of the trust economy, think of it as the tech-charged equivalent of the public ledgers that would be used in towns to record everything of importance: the buying and selling of goods; the transfer of property deeds; births, marriages, and deaths; loans; election results; legal rulings; and anything else of note. Instead of a bearded master wielding a long-stemmed stylus to record miniscule but legible entries in an oversized ledger, blockchain uses advanced cryptography and distributed programming to achieve similar results: a secure, transparent, immutable repository of truth—one designed to be highly resistant to outages, manipulation, and unnecessary complexity.

In the trust economy, the individual—not a third party—will determine what digital information is recorded in a blockchain, and how that information will be used. With an eye toward curating a single, versatile digital representation of themselves that can be managed and shared across organisational boundaries, users may record:

- Digitised renderings of traditional identity documents such as driver’s licenses, passports, birth certificates, Social Security/Medicare cards, voter registration, and voting records
- Ownership documents and transactional records for property, vehicles, and other assets of any form
- Financial documents including investments, insurance policies, bank accounts, credit histories, tax filings, and income statements
- Access management codes that provide any identity-restricted location, from website single sign-on to physical buildings, smart vehicles, and ticketed locations such as event venues or airplanes
- A comprehensive view of medical history that includes medical and pharmaceutical records, physician notes, fitness regimens, and medical device usage data

As a repository of valuable data, blockchain can provide individual users with unprecedented control over their digital identities. It can potentially offer businesses an effective way to break down information silos and lower data management costs. For example, in a recent blog post, Bruce Broussard, president and CEO of health insurance provider Humana, shared his vision of a future in which hospitals, clinics, and insurance companies streamline administrative processes, increase security, and achieve significant cost savings by
storing and managing electronic health records on a blockchain.³

**Exchange digital assets without friction:** Using blockchain, parties can exchange ownership of digital assets in real time and, notably, without banks, stock exchanges, or payment processors—all applications requiring trusted digital reputations. Many of blockchain’s earliest use cases for business involved facilitating cross-border payments and intracompany transfers. Applying that same basic transactional model to P2P transactions, blockchain could potentially become a vehicle for certifying and clearing asset exchanges almost instantaneously. What once took T + 3 days to clear now takes T + 3 milliseconds.

Though broad acceptance of P2P asset exchanges via blockchain may still be a few years away, the exploratory steps some companies are currently taking offer insight into where blockchain deployment may be headed. For example, Microsoft and Bank of America Merrill Lynch are jointly developing a cloud-based “blockchain-as-a-service” offering that will execute and streamline asset exchanges between companies and their customers.⁴

**Execute smart contracts:** Smart contracts represent a next step in the progression of blockchain from a financial transaction protocol to an all-purpose utility. They are not contracts in the legal sense, but modular, repeatable scripts that extend blockchains’ utility from simply keeping a record of financial transaction entries to implementing the terms of multiparty agreements automatically. The fact that they are not legally binding makes trust even more important.

Here’s how they work: Using consensus protocols, a computer network develops a sequence of actions from a smart contract’s code. This sequence of actions is a method by which parties can agree upon contract terms that will be executed automatically, with reduced risk of error or manipulation. Before blockchain, this type of smart contract was impossible because parties to an agreement of this sort would maintain separate databases. With a shared database running a blockchain protocol, the smart contracts auto-execute, and all parties validate the outcome instantaneously—and without the involvement of a third-party intermediary.

Though smart contracts may not be appropriate for some legal agreements, they can be a worthwhile option in situations where networks of parties engage frequently, or in agreements where counterparties are performing manual or duplicative tasks for each transaction. For example, they could be deployed for the automated purchase or sale of financial instruments, parametric insurance contracts, and certain automatic market-making activities, as well as for digital payments and IOUs. In each case, the blockchain acts as a shared database to provide a secure, single source of truth, and smart contracts automate approvals, calculations, and other transacting activities that are prone to lag and error.⁵

**Chain of tools**

In the greater context of the trust economy, blockchain is not a cure-all for the challenges of establishing and maintaining trust. As a technology, it is still maturing; standards and best practices do not yet exist. The very features that protect blockchain against theft and fraud could also drive overhead if not correctly implemented—a potential obstacle on the path toward individual deployment of the technology. Finally, legal recognition of contracts and digitally transferred assets is currently limited. The good news is that organisations can take steps now to mitigate if not fully address these challenges.

Some pundits are likening the emergence of blockchain technology to the early days of the World Wide Web, and for good reason. In 1991, the foundations for distributed, open communication were being laid—network infrastructure, protocols, and a variety of enabling technologies from javascript to search engines to browsers. There were also new enterprise software suites that made it possible to take advantage of digital marketing, commerce, and linked supply networks, among countless other opportunities. Hyper-investment chased perceived opportunity, even as specific scenarios describing how the technology would change the world had not yet been defined.
Blockchain may lead to even greater disruption by becoming the new protocol for digital assets, exchanges, contracts, and, perhaps most importantly, identity and trust. With efforts to create a new stack for all facets of blockchain attracting investment, the time is now for enterprises to explore the underlying technology, and to envision how blockchain may be used for more than just the easy use cases of cost savings and efficiency within their own boundaries. Take a hard look at your core business, surrounding ecosystems, and even the long-established mechanics of the way your industry operates, and then direct your experimentation toward a truly innovative path.
Lessons from the Front Lines

Smart play with smart contracts

Delaware, home to more than 60 percent of Fortune 500 firms, is teaming up with Symbiont, a distributed ledger and smart securities vendor, to launch a blockchain-based smart contracts system. Smart contracts are protocols that allow blockchain technology to record, manage, and update encrypted information in a distributed ledger automatically, without intermediaries. The system will enable participants to digitise incorporation procedures such as registering companies, tracking shares, and handling shareholder communications. For companies incorporated in Delaware, this could make registration and follow-up steps in the process faster, less expensive, and more transparent.

At the heart of Symbiont’s solution is an immutable, append-only database, which provides a single, global accounting ledger for system participants. Transaction history is appended and replicated across all network nodes, with access permissions restricted down to the specific organisation or even user level. Each company registering with the state of Delaware signs in with a private key that verifies its identity to other participants. Autonomous recordkeeping will trigger notifications when actions are required, such as new filing requirements when thresholds are met or when documents approach expiration.

Project teams are taking a two-pronged approach to deployment. First, they will rebuild the public archives using a distributed ledger for storage and “smart records” to automate the control and encryption of public and private records. This critical step will make it possible for digital documents to be shared in multiple locations and, importantly, be recovered in the event of system failure. Next, they will place incorporation and other legal documents on a smart contract-enabled blockchain and establish operational procedures for using and maintaining them.

This deployment is part of a larger effort called the Delaware Blockchain Initiative, which will lay the legal and technological groundwork needed to support blockchain-based systems going forward. The governor’s office is currently collaborating with the legislature to build the legal framework required to support blockchain-based incorporation processes and digitally originated securities. “We see companies allocate significant financial resources to correct and validate stock authorisation and issuance errors that could have been correctly and seamlessly handled from the outset,” says Delaware Governor Jack Markell. “Distributed ledger [transactions] hold the promise of immediate clearance, immediate settlement, and bring with them dramatic increases in efficiency and speed in sophisticated commercial transactions.”
SWIFT: From middleman to enabler

Blockchain has the potential to rewire the financial industry and beyond, generating cost savings and new revenue opportunities. Payment rails have been the subject of various blockchain-driven initiatives. Payment transaction firm SWIFT has been testing use cases to demonstrate how its 11,000-plus member financial institutions can optimise the technology’s transparency while maintaining the industry’s privacy requirements in the emerging trust economy.

The organisation’s new R&D arm, SWIFT Innovation Labs, was launched with an eye on eventually providing distributor ledger technology (DLT)-based services that leverage its standards expertise, strong governance, and security track record. DLT, it says, would provide trust in a disseminated system, efficiency in broadcasting information, complete traceability of transactions, simplified reconciliation, and high resiliency.

SWIFT’s team of 10 experts in standards, securities, architecture, and application development built a bond lifecycle application that tracks and manages bonds from issuance to coupon payments to maturity at an ecosystem level rather than by individual company. SWIFT applied its own ISO 20022 methodology to DLT to gauge interoperability with legacy systems in cases where all stakeholders were not on the distributed ledger.

The bond life cycle proof-of-concept was built using an Eris/Tendermint consensus engine to enable smart contracts written in Solidity, a language for the Ethereum blockchain. Monax’s Eris platform was chosen because it is open-source; it enables a permissioned blockchain that can only be viewed and accessed by the parties involved in the transaction; it supports smart contracts; and its consensus algorithm has better performance than Bitcoin’s blockchain.

SWIFT’s lab team set up five blockchain nodes (in its California office, at an account servicer in Virginia, and at investment banks in Brazil, Germany, and Australia) on a simulated network that implemented the ISO 20022 standard, which covers transaction data for banks, securities depositories, and high-value payments. The standard’s layered architecture consists of coded business concepts independent of any automation, which according to SWIFT “seems a good place to look for content that can be shared and re-used” via a distributed ledger.

“SWIFT has been targeted in the press as a legacy incumbent that will be doomed by DLT,” says Damien Vanderveken, head of R&D at SWIFT Innovation Labs. “But we believe SWIFT can leverage its unique set of capabilities to deliver a distinctive DLT platform offer for the [financial] community.” This could translate into cheaper, faster, and more accessible remittance and corporate disbursement services around the globe.
In my role with the MIT Media Lab, I spend my days exploring how radical new approaches to science and technology can transform society in substantial and positive ways. When I look at the current state of blockchain, I’m reminded of the early days of the Internet—filled with promises of disruption, a brand-new stack that needed to be built, unchecked investment, and more than a few crazy dreamers (I was, and remain, one of them). Much as naysayers initially did with the Internet, some consider blockchain, smart contracts, and cryptocurrencies to be fads, but in my opinion, they are not. The potential is real.

In the early 1990s, we knew we were on the cusp of something big. But we were lacking the layers needed to take advantage of the promise: a universal networking protocol (TCP/IP), routers and switches for enterprises to establish and scale communications, a standard for client connectivity and information exchange (HTTP), and many others. The incumbents—cable companies and telcos—were building monolithic, closed systems in order to explore the new frontier. Largely informed by the reference point of their existing businesses, their approach led to set-top boxes, closed communities and online forums, and proprietary systems for search, messaging, and mail. But as we look back, most of the big winners of the era were the native Internet companies that provided each necessary layer that would eventually become the full stack we know today.

Blockchain is like that. There is a layer for transmitting bits and managing the shared ledger. There’s a wallet for organizing and conducting business with one’s assets. There may be a bookkeeping layer for uniformly describing the content and context behind assets on the blockchain. There will be a smart contract layer, and others will likely emerge.

The currency piece of the blockchain is a lot like email was to the Internet. Email may be the most used function on the Internet, and it changed the way businesses work; it was a killer app that pushed the Internet to widespread deployment, after which came Google, Facebook, and Twitter. In the same way, many smart contract layers and other sophisticated use cases will be feasible once blockchain is deployed everywhere.

It remains to be seen whether American institutions will give blockchain the same kind of free rein the Internet enjoyed in its early days. Regardless, there is a need to redraw existing regulatory boundaries. If you diligently deploy a blockchain solution following the existing laws—especially those focused on money laundering—you could twist yourself into knots trying to design your business and products around old statutes. The interplay between technology and public policy played a central role in the Internet’s adoption. Given that the stakes around blockchain are much higher and possibly even more transformative, anything we can do to amplify, accelerate, and advance our collective progress in a prudent but progressive way can transform the world around us to the benefit of society.
I've been in the venture capital business for over 20 years, co-founding six enterprise software companies along the way. I began hearing about Bitcoin in 2011, while serving as chairman of one of the largest social gaming companies in Southeast Asia. In that business, cross-border payments and payment processing quickly became a core competency. As the buzz around Bitcoin grew, I initially discounted this technology as “silly Internet money,” but by 2012, a number of people I trusted told me to take a harder look. So I did what I still tell people to do today: lock your door, turn off your phone, and study this new technology frontier for a day. I realised that this ecosystem will likely have incredibly profound effects on enterprise, government, and society—and is a generational opportunity for entrepreneurs and investors.

I began investing in a wide range of companies across the blockchain ecosystem, including digital wallets, payment processors, exchanges, and miners. This helped me develop a heat-map of the ecosystem, and more importantly, a network of technologists and entrepreneurs who were building the scaffolding for this new industry. It also led to my friendship, and later partnership with Jeff Garzik, with whom I co-founded Bloq.

Enterprise demand for blockchain is real, but there are many questions to be answered. What type of software infrastructure do you need? What can we learn from enterprise adoption patterns of other transformative technology?

To the first question, the emergence of an open source, enterprise-grade blockchain software suite is developing quickly, and we're investing an enormous amount of time and energy helping companies develop an infrastructure that, in many ways, defines the basic anatomy of a blockchain:

- **Blockchain platform** as the base communication and management layer of the network
- **Nodes** to connect to a blockchain network, which behave much like routers
- **Wallets** to securely manage and store digital assets
- **Smart contracts** to automate and streamline business processes
- **Analytics** to drive better decisions and detect network anomalies

The second question revolves around adoption curves. I see a story unfolding that is similar to those of the Internet and cloud computing. Right now, organisations are implementing blockchain technology internally to reduce costs by moving value and data in a more secure, more efficient manner. We are also beginning to see some activity in core operations and business processes that utilise blockchain's encrypted workflow features. These are important stepstones helping drive an architectural step change in blockchain adoption.

Next, companies deploying blockchain networks should consider extending those platforms to their customers, suppliers, and partners. This is where network effects should start to blossom, and will likely lay the foundation for pursuing new economic opportunities—measured in trillions of dollars—think central banks issuing digital currencies, land title registries, a secure digital identity, and more. Yet organisations don't strive just to be better—they want to operate at a different level. With blockchain, moving money should be as easy as email. In 10 years, banks may look more like Apple, Amazon, and Tencent, coupled with access to tons of products and services within those ecosystems. The discussion won't be about whether to use blockchain—it will be about the economics of the platform and how to develop strong network effects.

The blockchain genie is out of the bottle, although the adoption curve remains unclear—will it be three to seven years? A decade, or longer? These networks for money's new railroad will take time to adopt. In the late 1990s, CEOs wondered if they should risk their careers by investing in and innovating with the Internet; today CEOs are in the same boat evaluating blockchain. Like any great technology evolution, the blockchain transformation requires passion and investment, dynamics that drive innovation. Right now, neither appears to be in short supply.
Just as distributed architecture and open standards play spotlight roles in the inevitable architecture trend, they loom large in blockchain and the emerging trust economy. Blockchain is an open infrastructure technology that enables users operating outside of an organisational or network boundary to execute transactions directly with each other. Blockchain’s fundamental value proposition is anchored in this universal availability.

It is also anchored in integrity. When someone adds a block, or executes a blockchain-based smart contract, those additions are immutable. The potential value of the numerous blockchain applications currently being explored—including regulatory compliance, identity management, government interactions with citizens, and medical records management—resides, to a large degree, in the security benefits each offers users. These benefits include, among others:

- The immutable, distributed ledger creates trust in bookkeeping maintained by computers. There is no need for intermediaries to confirm transactions.
- Transactions are recorded with the time, date, participant names, and other information. Each node in the network owns the same copy of the blockchain, thus enhancing security.
- Transactions are authenticated by a network of computer “miners” who complete complex mathematical problems. When miners arrive at the same solution, the transaction is confirmed and recorded on the “block.”

The distribution of miners means that the system cannot be hacked by a single source. If anyone tries to tamper with one ledger, the nodes will disagree on the integrity of that ledger and will refuse to incorporate the transaction into the blockchain.

Though blockchain may feature certain security advantages over more traditional transactional systems that require intermediaries, potential risks and protocol weaknesses that could undermine the integrity of blockchain transactions do exist. For example, it has recently come to light that vulnerabilities may exist in the programming code that some financial services companies are using as they integrate distributed ledger technologies into their operations.

Given that there is no standard in place for blockchain security, other potential cyber issues could emerge. For this reason, users currently rely—arguably too much—on crowdsourced policing. Blockchain is a relatively new technology, and therefore discussion of its potential weaknesses is somewhat academic. Somewhere down the road, an underlying vulnerability in blockchain may emerge—one that would put your systems and data at risk.

Though you should not let fear of scenarios like this prevent your company from exploring blockchain opportunities, as with other leading-edge technologies, it pays to educate yourself and, going forward, let standards of acceptable risk guide your decisions and investments.
Where do you start?

The hype surrounding blockchain is reaching a fever pitch. While this technology’s long-term impact may indeed be formidable, its immediate adoption path will most likely be defined by focused experimentation and a collection of moderately interesting incremental advances. As with any transformative technology, expertise will have to be earned, experience will be invaluable, and the more ambitious deployment scenarios will likely emerge over time. The good news? It’s still early in the game, and numerous opportunities await.

Here are some suggestions for getting started on your blockchain journey:

- **Come all ye faithful**: The financial services industry is currently at the vanguard of blockchain experimentation, and the eventual impact of its pioneering efforts will likely be far-reaching. Yet blockchain’s disruptive potential extends far beyond financial services: Every sector in every geography should be developing a blockchain strategy, complete with immediate tactical opportunities for efficiency gains and cost savings within the organisation. Strategies should include more ambitious scenarios for pushing trust zones to customers, business partners, and other third parties. Finally, sectors should envision ways blockchain could eventually be deployed to challenge core business models and industry dynamics. While it often pays to think big, with blockchain you should probably start small given that the technology’s maturity—like that of the regulations governing blockchain’s use—is still relatively low.

- **Wayfinding**: Start-ups and established players are aggressively pushing product into every level of the blockchain stack. Part of your adoption journey should be understanding the fundamental mechanics of blockchain, what pieces are absolutely necessary for your initial exploration, and the maturity of the offerings needed for the specific scope being considered.

- **The nays have it**: Ask your blockchain gurus to define scenarios and applications that are not a good fit for blockchain. This is not reverse psychology: It’s simply asking advocates to keep a balanced perspective, and thoughtfully casting a light on this emerging technology’s current limitations and implications. Sure, expect challenges and prescribed roadblocks to yield to future advances in the field. But until then, challenge your most enthusiastic blockchain apostles to remain objective about the technology’s potential upside and downside.

- **You gotta have friends**: Blockchain offers little value to individual users. To maximise its potential—particularly for applications and use cases involving digital identity—explore opportunities to develop a consortium or utility for blockchain use.

- **Stay on target**: Far-reaching potential can lead to distracting rhetoric and perpetual prognostication. As you explore blockchain, focus your brainstorming and your efforts on actionable, bounded scenarios with realistic scope that can lead to concrete results and—hopefully—better value. Wild-eyed aspirations are not necessarily bad. But they are best served by grounded progress that leads to hands-on proof and an earned understanding of what is needed to realise the stuff of dreams.

**Bottom line**

In a historic break from the past, the foundational concept of trust is being tailored to meet the demands of the digital age, with blockchain cast in the role of gatekeeper of reputation and identity. While the broader implications of this trend may not be fully understood for years to come, business and government are beginning to explore opportunities to selectively share composite digital identities with others not only to help establish trust but to exchange assets safely and efficiently, and—perhaps most promisingly—to proffer digital contracts.
ENDNOTES


13. Ibid.


15. Ibid.


