Project on

Blockchain based Health Informatics for Pandemic Management

Submitted By:

Vikas Vashista

(2K18/EMBA/540)

Under the Guidance of:

Mr. Yashdeep Singh

Assistant Professor

DELHI SCHOOL OF MANAGEMENT

Delhi Technological University

Bawana Road Delhi 110042

CERTIFICATE

This is to certify that the minor report titled "**Blockchain based Health Informatics for Pandemic Management**" is a bonafide work carried out by **Mr. Vikas Vashista** of **EMBA 2018-20** and submitted to Delhi School of Management, Delhi Technological University, Bawana Road, Delhi-42 in partial fulfilment of the requirement for the award of the Degree of Executive Masters of Business Administration.

Signature of Guide
(Yashdeep Singh)
Assistant Professor, DSM

Signature of Head (DSM)

Seal of Head

Place:

Date:

DECLARATION

I, **Vikas Vashista**, student of **EMBA 2018-20** of Delhi School of Management, Delhi Technological University, Bawana Road, Delhi – 42, hereby declare that the dissertation report **"Blockchain based Health Informatics for Pandemic Management"** submitted in partial fulfilment of Degree of Executive Masters of Business Administration is the original work conducted by me.

The information and data given in the report is authentic to the best of my knowledge.

This report is not being submitted to any other University, for award of any other Degree, Diploma or Fellowship.

Place: **(Vikas Vashista)**

Date:

ACKNOWLEDGEMENT

I would like to express my sincere gratitude towards my Guide, **Mr. Yashdeep Singh** (Assistant Professor, Delhi School of Management, DTU) for his support and valuable guidance throughout the duration of the project. In the journey of this project from my bottom of hearth I want to thank to him, for his patience for providing me with a goal-oriented approach towards this project and for the constant encouragement & support at every stage.

My sincere gratitude goes out to my all the professors of DSM, whose teaching gave many valuable inputs for completion of this project.

Vikas Vashista

(2K18/EMBA/540)

Table of Contents

Table of Figures

Abstract

The economic costs of COVID-19 are devastating, on a scale perhaps never seen in modern times. At this stage, the human costs are unfathomable. This is one of those rare turning points in history. The COVID-19 pandemic will profoundly change our economy, our behaviour, and society. Some leaders who failed the test will lose their jobs. Some governments that failed their people will lose their power. Many institutions will come under scrutiny and, we hope, change for the better. This is new promise of the digital economy. It's a new promise because we're in a new second era of the digital age, where technologies like artificial intelligence (AI), the Internet of Things (IoT), augmented and virtual reality (AR/ VR), biotech, and above all, blockchain are providing leaders with an unprecedented set of opportunities. These technologies have not stormed the world; rather, they've developed slowly in an uneven and combined or complementary manner. These technologies are now relevant as never before, not just to business and the economy but the future of public health and the safety of global populations. Traditional systems have failed and it's time for a new paradigm. To build on Victor Hugo, Nothing is more powerful than an idea that has become a necessity.

Recently, there have been increasing calls for healthcare providers to provide controls for patients over their personal health records. Nevertheless, security issues concerning how different healthcare providers exchange healthcare information have caused a flop in the deployment of such systems. The ability to exchange data securely is important so that new borderless integrated healthcare services can be provided to patients. Due to its decentralized nature, blockchain technology is a suitable driver for the much-needed shift towards integrated healthcare, providing new insights and addressing some of the main challenges of many healthcare areas. Blockchain allows healthcare providers to record and manage peer-to-peer transactions through a network without central authority. In this report I also discussed the concept of blockchain technology and hurdles in their adoption in the healthcare domain.

This project report focuses on following three areas— Self-sovereign identity and data governance, supply chain (Pharmacy) and healthcare informatics management.

Self-sovereign identity, health records, and shared data is the most important asset in fighting pandemics. Without it, we can't answer critical questions: Who are infected? Where have they travelled? If any useful data exists now, it sits in institutional silos, inaccessible to individuals and other stakeholders. We need better access to the data of entire populations and a speedy consent-based data sharing system. The trade-off between privacy and public safety need not be so stark. Through self-sovereign identities where individuals own their health records and can freely volunteer it to governments, clinicians, drug companies and others, we can achieve both.

Supply chains are critical infrastructure for our globally connected economy, and COVID-19 has put them under tremendous strain, exposing potential weaknesses in their design. We must build supply chains that are transparent, where information can be accessed quickly, and where participants can trust that information about goods are accurate. Blockchain serves as a state machine that allows us to know the state of not only our suppliers but also the assets themselves.

Front-line medical professionals are the heroes and our last line of defence. Yet hospitals can't onboard people fast enough. This is not for lack of talent; it's the inability to find them. This talent management paradox, where organizations continuously struggle to tap into the pool of skilled people looking for work. How does blockchain solve this? By streamlining coordination among different geographies, departments, and certification bodies so that process becomes more efficient and transparent. Convoluted criteria checks, redundancies in the certification process, and the processing of documents all slow down (re)licensing. If, as part of a self-sovereign identity, every professional had verifiable and trusted professional information, then we could resolve this talent management paradox and get people to where we needed them, saving lives and starting jobs in the process.

People respond to incentives. That's the consensus among behavioural economists and a theme of much public policy: How do we improve individual and business accountability during a crisis? What kinds of incentives do we need to manifest behaviours that will prevent viral outbreaks from rocketing into pandemics or mitigate the damage that pandemics cause—without compromising privacy or liberty? Government must be aligned, too. How do we encourage policymakers, governments, businesses, and other institutions to prepare for the inevitable by keeping supplies on hand, designing a strategy for handling public health crises, or reserving funds for swift response? Crypto economics can help with alignment. Blockchain serves as a mechanism to synch up the incentives of stakeholder groups around issues and activities, changing patterns of behaviour in the process.

Governments must wake up to the blockchain opportunity. Every national government should create an emergency task force on medical data to start planning and implementing blockchain initiatives. They can stimulate the development of technology firms working on the solutions described here. They can act as a model user of these important platforms and applications. They must focus on the supply side of the market for data, not just the demand side. That means passing legislation to mobilize stakeholders around creating self-sovereign identities and citizen-owned health records. They should pilot blockchain incentive systems for motivating people to behave responsibly. They should partner with medical professional associations and other players to implement blockchain credential systems. Governments have the world's largest supply chains, many involved in producing critical medical provisions. They should rapidly pilot asset chains as described herein. Central banks should move swiftly to create a fiat digital currency in their country and the International Monetary Fund should provide leadership in rolling these into a global, hegemonic, synthetic digital currency.

The project report also provides recommendations for the private sector and civil society.

Chapter 1: Introduction

"The next outbreak? We're not ready," said Bill Gates in his prophetic TED talk of March 2015.

The talk has soared from 18 million to over 25 million views in the last week. Of course, Gates was right to say that a pandemic of this size was inevitable, and he wasn't the only one. Since Gates' talk, experts have pointed to research that warned of the danger much earlier and produced scores of new works to sound the alarm. But the world was oblivious, some nations and leaders more than others, and now we're paying the price.

As, I have been drafted this project report, the number of new cases and deaths is exploding. The spread of the virus has a lot to do with data. Rather, the lack of it. Clinicians, epidemiologists, and government authorities have been working in the dark. Most Western countries had virtually no testing in the early weeks of the outbreak. As Ed Yong wrote in The Atlantic: The testing fiasco was the original sin of America's pandemic failure, the single flaw that undermined every other countermeasure. If the country could have accurately tracked the spread of the virus, hospitals could have executed their pandemic plans, girding themselves by allocating treatment rooms, ordering extra supplies, tagging in personnel, or assigning specific facilities to deal with COVID-19 cases.3 The pandemic revealed deep structural inadequacies in our health systems but also in our supply chains. Everywhere systems based on decades-old technologies caused severe shortages in protective equipment from masks and gloves to ventilators. Driven by fear and lack of transparency in supply chains, consumers panicked, emptying shelves of staples. With some consumers hoarding years' worth of toilet paper, surely at least one wealthy person said, Let them use bidets. The bidet market soared, only to be hit by shortages, too. While exposing a failure of institutions and leadership, the pandemic revealed serious deficiencies in our systems for innovation, commerce, data governance, and technology infrastructure.

Now's as good a time as any to understand these, not just to help avoid pandemics in the future but to help us move through this crisis, which surely will continue for some time.

How do we get better data about an outbreak and our responsiveness to it?

How can we increase the reliability of our supply chains and our logistics, transport, and payment systems?

How can we better ensure the authenticity and provenance of medical products and medications as well as the credentials and readiness of medical personnel?

How can we build better transparency into systems to help rebuild consumer and citizen trust?

How can we track citizens who have tested positive without undermining their rights?

How can we make retail commerce safer?

How do we better incentivize citizens to behave more responsibly?

Can we move to a new paradigm in health records that are both private and owned by citizens but also provide the critical data that experts and authorities need to manage a crisis?

How do we build better sanitation infrastructure and encourage citizens to care more about their wellness?

Is now the time to eliminate that germ-loaded vestige of the preindustrial economy— cash?

It turns out that a next generation of technology that includes *AI* and *IoT* and centers on **blockchain** could help leaders to usher in a new era of public health and responsiveness to the communicable medical crises that will increasingly plague us on this ever-shrinking planet.

Chapter 2. Literature review

The research gaps that I seek to address in this research are related to three key research streams namely : Information Technology in healthcare and its adoption and privacy concerns and trust. Now I present the relevant and recent literature for these streams.

Information technology has transformed ways in which health information are obtained and utilized. Based on respective health technology assessments, countries prioritize healthcare delivery in order to create sustainable health systems (Littlejohns et al., 2018). Exclusively designed technologies for healthcare services have contributed to the digital health phenomenon (Lupton, 2014). Researchers have studied impact of information technology on quality, efficiency and cost of healthcare services (Chaudhry et al., 2006). Most of the studies show positive effect of IT on healthcare services with some studies reporting mixed findings (Buntin et al., 2011). For example, positive outcomes such as reduced healthcare costs for both service providers and consumers were reported by Li and Benton, (2006) and increased service satisfaction by Queenan et al., (2011). Devaraja et al. (2013) surveyed hospitals in US and substantiated using Theory of Swift Even flow (TSEF), the finding that adoption of IT results in improved revenue. Piccinini et al., (2013) reported reduced costs associated with management of healthcare due to centralization of healthcare service using IT. Lahiri and Seidmann, (2012) reported reduced flexibility as an undesired outcome of technology adoption in healthcare service delivery. Sharma et al. (2016) suggested complementarities between clinical health information technologies (primarily used for patient data collection, diagnosis and treatment) and augmented clinical health information technology (used for integrating information for augmented decision making) with respect to process quality.

Emerging technologies such as big data, cloud computing, blockchain and health sensing are revolutionizing healthcare operations and delivery (Yang et al., 2015, Wan et al., 2019 and Gan et al., 2020). Wang et al., (2016) enumerated a number of capabilities of big data analytics in healthcare sector, particularly for decision support capability, analytical capability for pattern of care, predictive capability, unstructured data analysis capability and traceability. Zhong et al., (2016) proposed application of big data analytics for raising adoption of digitized health records. Cloud computing as an enabler for cost effective solution for patient information, sensor-based health data collection and delivery has been proposed in many studies (Binczewski et al., 2011; Patra et al., 2012; Rolim et al., 2010).

Available literature on adoption of technology in healthcare can be broadly categorized in two streams. *First*, studies concerned with extent of IT related adoption in healthcare by analyzing pervasiveness, scope and scale. *Second*, studies examining enablers and barriers in adoption of IT (Agarwal et al., 2010).

Studies belonging to *first stream have explored various characteristics of healthcare service providers, such as size, location, competition, ownership status, etc., that have adopted IT* (Cutler et al., 2005; Jha et al., 2009; Kazley and Ozcan, 2007; McCullough, 2008).

Major barriers in adoption of IT as enumerated by second stream of studies include *financial, functional, environmental and individuals including service providers and service users* (Bhattacharjee et al., 2006; DesRoches et al., 2008; Jha et al., 2009; Tang et al., 2006).

One key challenge with adoption of IT in healthcare is that the systems are typically not designed for multi-institutional lifetime records. Ethically managing health data, guarantee of security, auditability of records, and interoperability and immutability are few concerns that need to be addressed (Ekblaw et al., 2016). Qadri et al., (2020) in their study of emerging technologies for healthcare delivery advocated for IoT (Internet of things) and AI (artificial intelligence) oriented healthcare delivery system. Further, this study conceptualized the tenets of H-IoT (healthcare internet of things). The arguments for adoption of H-IoT was also supported by Porambage et al., (2016). Meng et al., (2018) in their surveyed stakeholders belonging to 12 different healthcare organizations developed a trust-based approach to figure out malicious devices in a healthcare environment. Yan et al., (2015) proposed trust based framework for virtualized networks and software defined networking. The study in particular argued for adoption of cloud computing to securely deploy various trustworthy security services over the virtualized networks. Ahmed et al., (2017) explored the recent advances in big data analytics for IoT systems as well as the key requirements for managing big data and for enabling analytics in an IoT environment. Lin et al., (2018) presented a blockchain-based system for secure mutual authentication to enforce fine-grained access control polices. Yan et al., (2016) proposed two trust evaluation algorithms to support different application cases. Specifically, these algorithms can overcome attacks raised by internal malicious evidence providers. Perera et al., (2017) argued for adoption of FOG (edge) computing based approach for solving analytical and computational problems for diverse problems including those related to medical industry and smart cities. Wazid et al., (2017) devised a novel authentication framework for medicine anticounterfeiting system considering the IOT environment aimed at ascertaining the authenticity of pharmaceutical products. The key benefit of the proposed scheme was in terms of its lower communication and computation cost over other similar authentication schemes. Wazid et al. (2018) proposed a new secure remote user authentication scheme for implantable medical devices communication environment to overcome security and privacy issues associated with existing schemes.

In order to study technology acceptance in healthcare with respect to trust, we need to appreciate distinctions of healthcare services from other services. People commonly demand healthcare services under distress in that either they are sick or at risk thus relinquishing privacy. There is risk of loss of privacy associated with providing personal information (Culnan and Armstrong, 1999). If the service provider cannot be trusted, there is no reason why consumers should expect to gain from using the particular service (Paulov, 2003). Number of public opinion polls establish that individuals are quite concerned about threats to their personal information (Xu et al., 2008). However, partial mediation of trust and privacy concern reduce the perception of risk (Andrews et al., 2014). Once consumers trust the service provider, the service provider seeks more health-related information (Miller and Bell, 2012). Bansal et al., (2010) established that personal disposition indirectly impacts trust through information sensitivity and privacy concern. Platt et al. (2019) found that expectations of benefits and positive views of health information sharing are associated with system trust. Steininger et al., (2015) in their study

pertaining to acceptance of *electronic health record (EHR)* demonstrated that privacy concerns impact perceived usefulness of EHRs negatively. He et al., (2012) identified the security challenges facing a sensor network for wireless medical monitoring and suggested that the network should follow a two-tier architecture. Based on such an architecture, the study also devised an attack-resistant and lightweight trust management scheme termed as ReTrust. Zhou et al., (2013) described the goals and tactics, and presented a distributed architecture of *m-healthcare social network* A critical review of extant literature reveals crucial research gaps that we seek to address in this research. Majority of studies exploring influence of information technology in healthcare are limited to analyzing impact on quality, cost effectiveness and efficiency of the service. Likewise, researchers have extensively explored behavioral constructs namely, trust and privacy concern, their enablers and their influence on technology acceptance independently in online transactions and e-commerce applications. However, studies on effect of behavioral aspects of patients on acceptance of IT in healthcare are lacking. Because of various distinct characteristics of healthcare service, it would be fruitless to apply canonical approaches for assessing users' response by espousing inferences from studies carried out in other service setups.

Chapter 3 – Blockchain

3.1. Disrupting the business of trust – the emergence of blockchain technology

For centuries, businesses and in some cases entire industries have been built on the simple principle of trust between multiple parties. However, this business of trust is about to be disrupted and transformed with the advent of blockchain technology. Blockchain can be defined as a distributed ledger technology that can record transactions between parties in a secure and permanent way. By 'sharing' databases between multiple parties, blockchain essentially removes the need for intermediaries who were previously required to act as trusted third parties to verify, record and coordinate transactions. By facilitating the move from a centralized to a decentralized and distributed system, blockchain effectively liberates data that was previously kept in safeguarded silos.

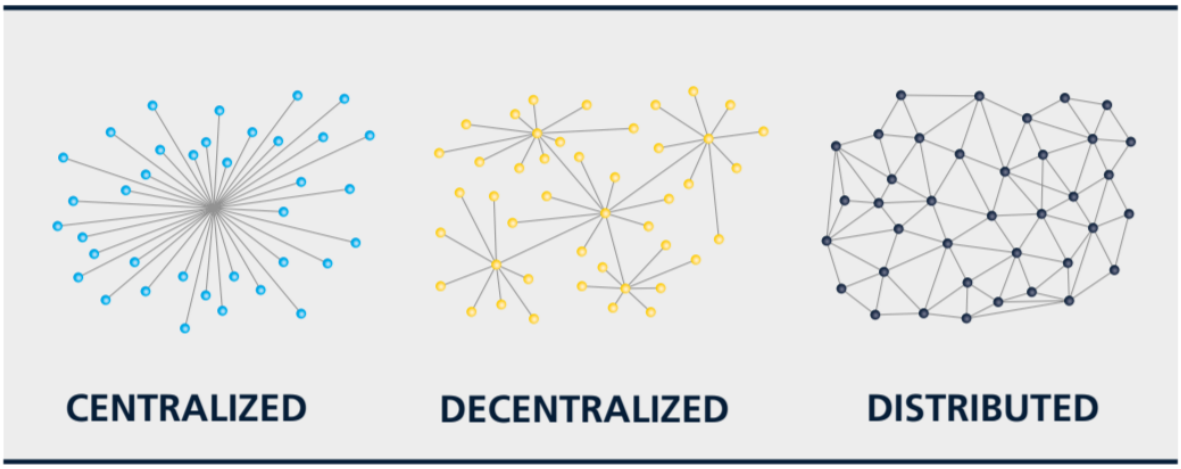


Figure 1: Going from a centralized to a decentralized, distributed database using blockchain (Source: DHL)

What kind of impact could this have on everyday life? Imagine in healthcare, sensitive data from all stakeholders – ranging from patients to medical companies – could be shared using the highest levels of encryption and data protection to greatly improve service efficiency and quality. Or in finance, companies and customers could potentially adopt a common digital currency as an alternative to traditional money, reducing the cost of transfers and enabling micro transactions. And in logistics, data sharing across the supply chain could enable higher levels of transparency, empowering consumers to make better choices about the products they buy. These are just some of the many opportunities that blockchain presents. Despite its brief history (see figure 2), blockchain is currently enjoying a rapid rise to prominence in corporate agendas as well as in the media.

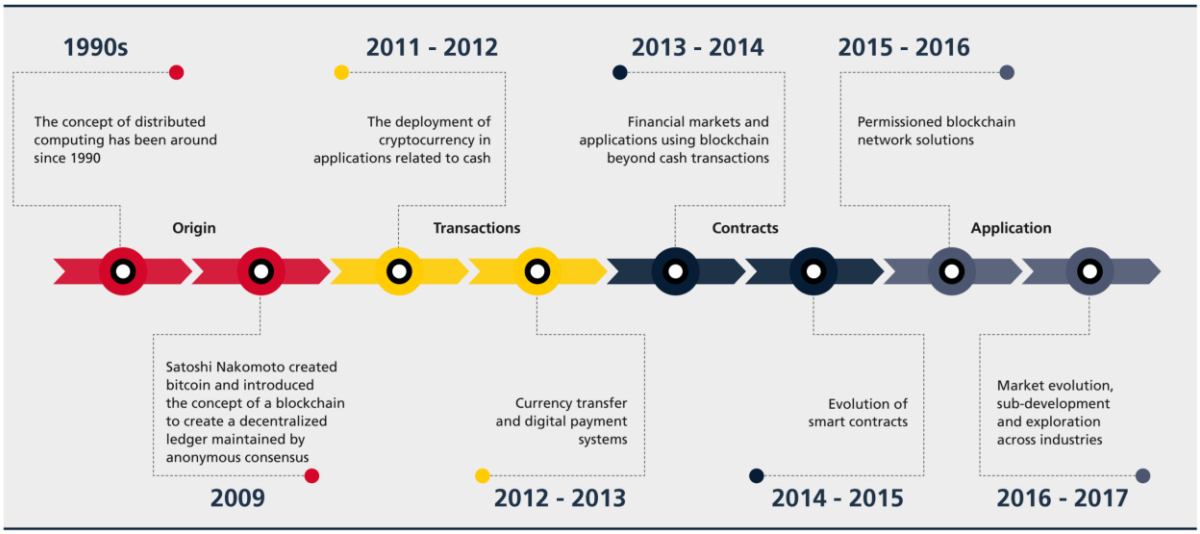


Figure 2: A history of blockchain technology (Source: Accenture)

Mainstream awareness can be largely attributed to its original application as the underlying technology of digital currencies, in particular bitcoin. Besides the adoption of this technology in powering cryptocurrency networks, there are open questions about where blockchain is headed, when it will yield positive results, and who will benefit most from it. What's clear at this point is that blockchain applications may have one of the most profound impacts on the logistics industry, especially the supply chain. Vipul Goyal, an associate professor at Carnegie Mellon University, states a lot of companies are interested in blockchain for creating more efficient workflows, but supply chain management is one of the big killer apps .

This is because global supply chains are highly complex, with diverse stakeholders, varying interests, and many third-party intermediaries – challenges that blockchain is well suited to address. In the logistics industry, blockchain can be harnessed in two key ways, namely, to drive efficiency and enable new business models:

Drive efficiency: Blockchain can potentially improve efficiency in global trade by greatly reducing bureaucracy and paperwork. For example, a multi-stakeholder process with a lengthy paper trail could be replaced with an automated process storing information in a tamper-evident digital format.

Another example is the automation of services that currently require an intermediary such as insurance, legal, brokerage, and settlement services. Blockchain could be used to track a product's lifecycle and ownership transfer from origin to store shelf, even as it changes hands between the manufacturer, logistics service provider, wholesaler, retailer and consumer. It would facilitate and automate each business transaction, enabling a more direct relationship between each participant (e.g., automating payments and transferring legal ownership between parties).

Enable new business models: Micro payments, digital identities, certificates, tamper-proof documents and much more can be introduced and radically improved using blockchain-based services. For example, driver training organizations could replace easy-to-fake paper-based certificates with tamper-proof digital versions that can then lead to new identity-related services. Just as the Internet

began a revolution of communication, blockchain technology could disrupt current business practices and models.

With significant benefits in sight, the overall market for blockchain is expected to boom with some estimates projecting growth of blockchain technology from USD $411.5 million in 2017 to $7.68 billion by 2022.2 Reasons for this rapid growth are the rise in banking, financial services and insurance applications including digital currencies and identities, as well as the continuing development of this technology and growth from major vendors. And while blockchain is not yet fully mature, its huge potential suggests this is the right time to learn more. Companies need to understand how blockchain technology can empower ground-breaking innovations, what obstacles must be overcome, and the likely value and tangible rewards it can deliver, especially in logistics.

What is bitcoin and how does it relate to blockchain technology?

- Bitcoin is a leading digital currency stored on a global, decentralized peer-to-peer blockchain
- Bitcoins are digital assets or cryptocurrency, meaning they are designed to be used as a medium of exchange
- Blockchain is the underlying technology which enables transactions to take place in a secure and trusted manner between pseudo-anonymous parties
- Anyone can participate in the bitcoin blockchain and ownership can be digitally transferred without the need for an intermediary
- Other digital currencies are available, including ether on the blockchain-based ethereum platform
- Bitcoin's price volatility, high liquidity as well as its role in enabling transactions to bypass trusted banks and financial institutions has led to criticism
- The creation or 'mining' of bitcoins is done through computers solving complex equations. Currently, it is heavily energy-intensive, requiring improvements in energy efficiency
- Whether bitcoin will be sustainable as a digital currency is yet to be known

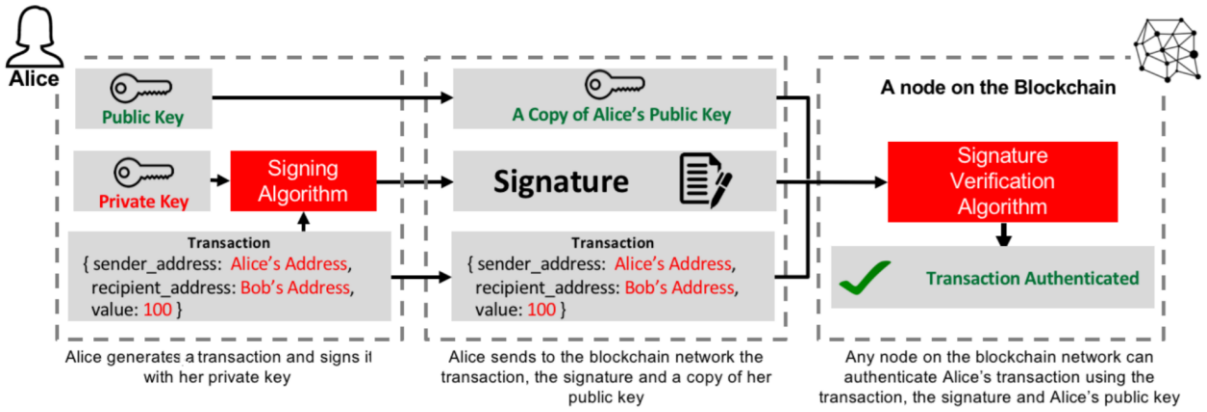


Figure 3: Bitcoin Transaction Authentication Process example (Source: Adil Moujahid, 2018)

3.2. How Blockchain Technology Works – An Overview of Key Features

Blockchain is a digital-ledger-based technology developed to change the perspective of the digital transactions, or specifically, to replace them. Blockchain is defined as a distinct, decentralized distributed ledger that includes all transactions records related to participating members. Blockchain transactions are created and stored in chronological order, allowing digital assets (such as digital currency and digital data) to be tracked by participants without central record-keeping. One of the key features in blockchain is that participating nodes in the network will hold a copy of the full blockchain. All transactions on the blockchain must be approved because transactions are only valid under the consensus agreement of the participating members. In addition, all transactions are trackable, making fraudulent transactions impossible to bypass.

Blockchain technology does not introduce an entirely new paradigm. Rather, it builds on the old template of a ledger – something that is used to log transactions over a period of time (see figure 4). Traditional ledgers are owned by one entity (such as a business, organization or group) and controlled by a designated administrator (for example, an accountant).

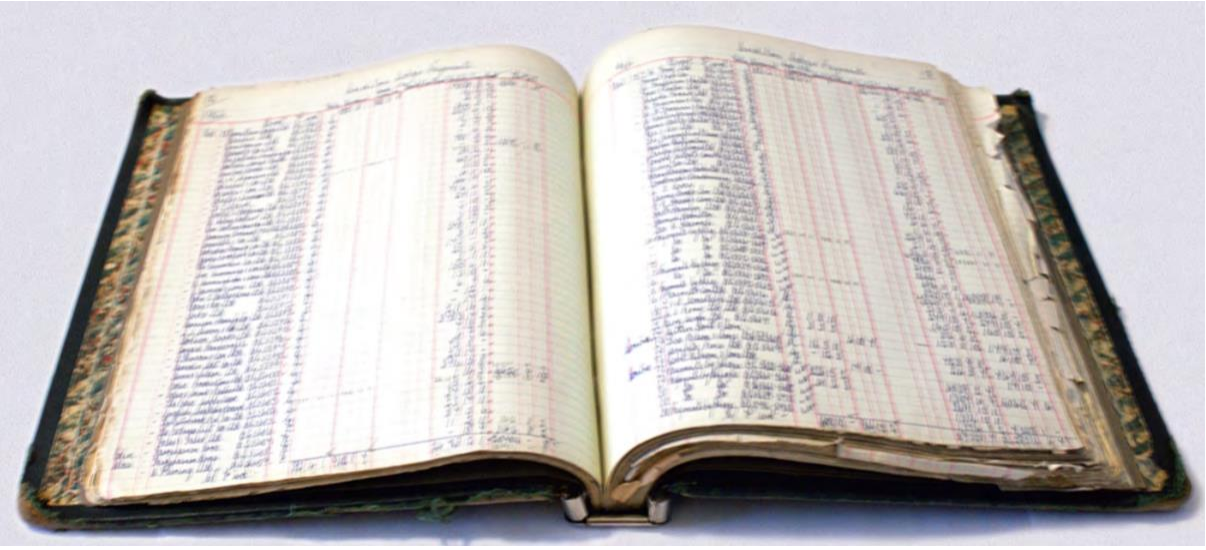
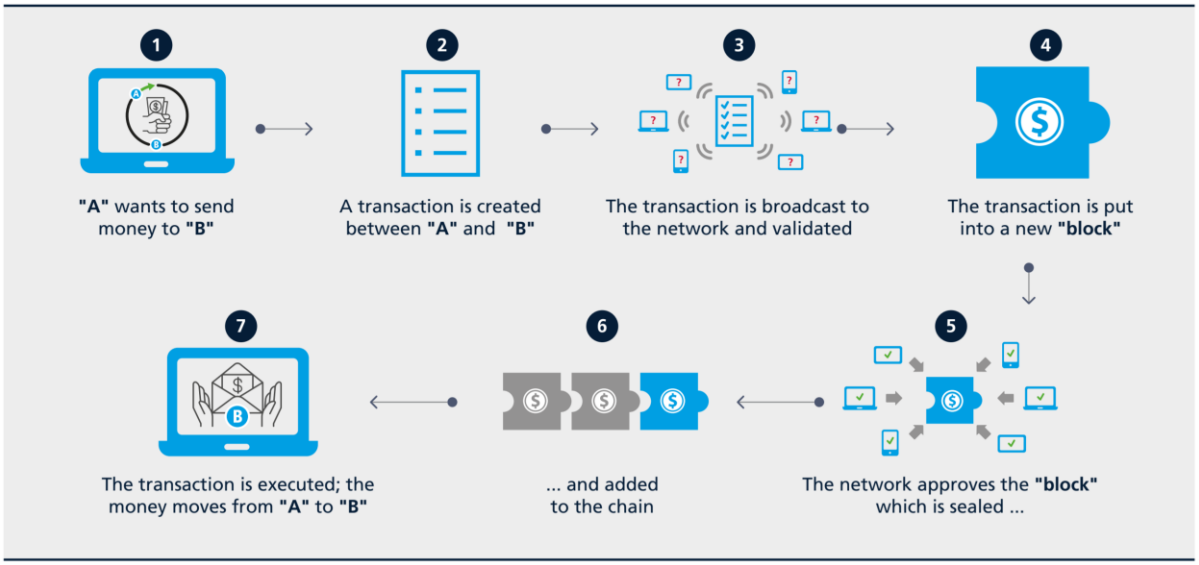


Figure 4: A typical ledger from the 1950s detailing creditor payments (Source: Edinburgh City of Print)



For example, when a user (user A) wants to make a transaction to another user (user B) using blockchain, a new block is created to include the transaction. Each transaction is broadcasted across network nodes to verify it. If the new transaction is verified, the new block is added to the blockchain and distributed across network nodes so that other nodes will update their blockchain. Finally, the transaction is received by another user (user B).

Figure 5: Illustration of a blockchain transaction; Source: DHL /Accenture

This administrator can implement changes to the ledger without requiring consensus from all of the ledger's stakeholders. In contrast, blockchain is a shared, distributed ledger among a network of stakeholders that cannot be updated by any one administrator. Instead, it can only be updated with the agreement of network participants and all changes to the distributed ledger are auditable. To illustrate how this operates, (figure 5) shows a financial transaction recorded on a blockchain. A similar process can be used to trace other types of asset transfer, to commit new data to a blockchain, and to update data in a blockchain. This 'mutualization of data' in a blockchain-based system is only possible with strong cryptographic techniques that make certain that copies are identical, transactions are not duplicated, and specific permissions are enforced to access stored data. Here, public and private keys are used to ensure confidentiality and privacy. In simple terms, a public key can be likened to the address of a physical mailbox, which is publicly known by senders. A private key is similar to the key or password required to unlock the mailbox; it is safeguarded at all times by the owner and must not be shared with third parties.

The transformative power of blockchain comes through the unique combination of its differentiating features and characteristics. Below is a summary of the four key features – these are data transparency, security, asset management and smart contracts.

1. Data transparency – Blockchain technology includes mechanisms to ensure stored records are accurate, tamper-evident, and from a verifiable source. Thus, instead of multiple parties maintaining (and altering) copies of their own dataset, now every stakeholder receives controlled access to a shared

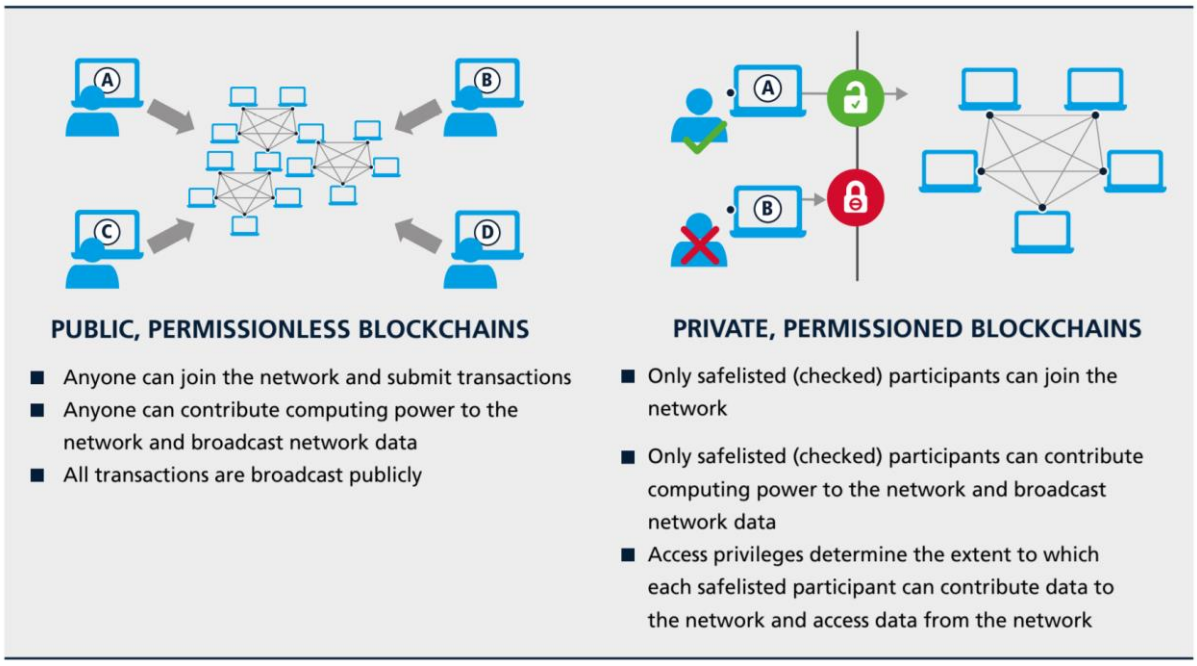
dataset creating a single source of truth. This gives confidence to everyone working with this data that they're using the most recent, accurate, and reliable dataset.

2. Security – Traditional ledgers typically provide a blanket layer of security which, once breached, allows access to all stored data. In a blockchain-based system, the security mechanisms make sure that individual transactions and messages are cryptographically signed. This ensures essential security and effective risk management to tackle today's high risks of hacking, data manipulation, and data compromise.

3. Asset management – Blockchain technology can be used to manage the ownership of digital assets and facilitate asset transfers. For example, it can be used to track the ownership of titles (e.g., land titles and diamond certificates) and rights (e.g., copyright and mineral rights). It can also be used to manage the digital twin of a physical object in the real world.

4. Smart contracts – Manual processes that are normally guided by legal contracts can be automated with a type of self-executing computer program called a smart contract. A smart contract is a component of a blockchain-based system that can automatically enforce stakeholder-agreed rules and process steps. Once launched, smart contracts are fully autonomous; when contract conditions are met, pre-specified and agreed actions occur automatically.

These capabilities can be deployed across two types of blockchain-based system: public permissionless blockchains where anyone can participate (e.g., the bitcoin network) and private permissioned blockchains where participants must be safe listed. Figure 6 shows the key differences between these two types of blockchain-based system.



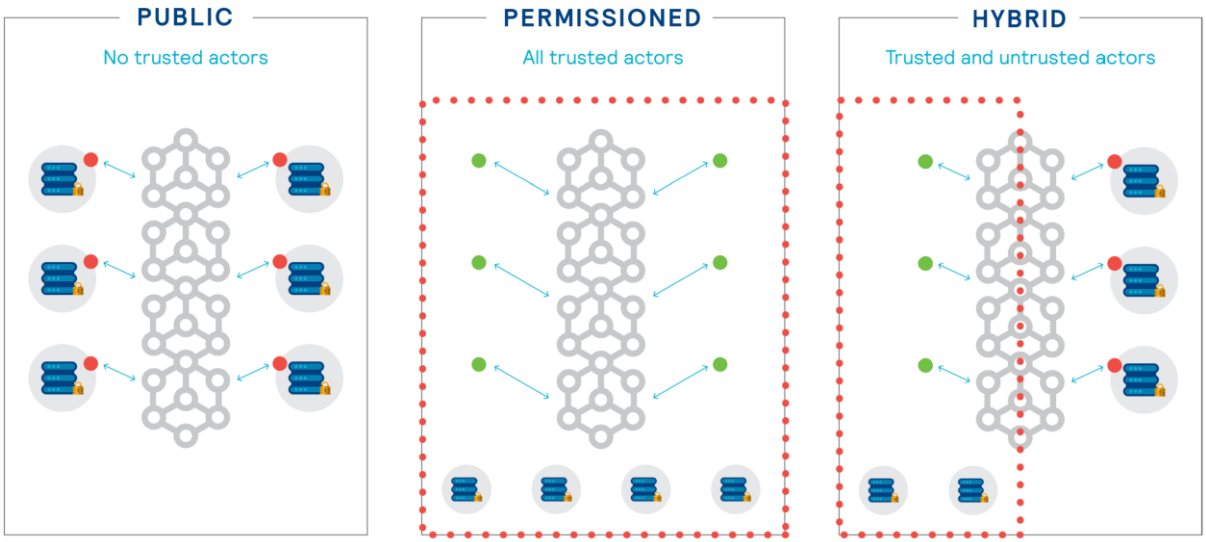


Figure 6: Key differences between public, permissionless blockchains and private, permissioned blockchains (Source: Accenture)

Public, permissionless blockchains are open and therefore likely to spur faster innovation as they can be used by many parties and can gain network effects. However today, companies tend to adopt private permissioned blockchains as these support a closed ecosystem of participants with enterprise features such as strict access controls and privacy protections. Therefore, the choice between using public versus private blockchains should be determined by the individual needs of each blockchain implementation.

Blockchain Governance			
Property	**Public**	**Consortium**	**Private**
Governance Type	Consensus is public	Consensus is managed by a set of participants	Consensus is managed by a single owner
Transactions Validation	Any node (or miner)	A list of authorized nodes (or validators)	
Consensus Algorithm	Any node	Any node (without permission) or A list of predefined nodes (with permission)	
Data Immutability	Yes, blockchain rollback is almost impossible	Yes, but blockchain rollback is possible	
Transactions Throughput	Low (a few dozen of transactions validated per second)	High (a few hundred/thousand transactions validated per second)	

Network scalability	High	Low to medium (a few dozen/hundred of nodes)	
Infrastructure	Highly-Decentralized	Decentralized	Distributed
Features	Censorship resistance Unregulated and cross-borders Support of native assets Anonymous identities Scalable network architecture	Applicable to highly regulated business (known identities, legal standards, etc.) Efficient transactions throughput Transactions without fees Infrastructure rules are easier to manage Better protection against external disturbances	
Examples of technologies	Bitcoin, Ethereum, Ripple, etc	MultiChain, Quorum, HyperLedger, Ethermint, Tendermint, etc .	

Table 1: Blockchain Classification

The launch of the Ethereum platform blockchain enabled blockchain to support transactions in numerous applications besides cryptocurrency. **Most healthcare applications are developed on the Ethereum framework.** Blockchain technology is considered a promising technology for many areas such as public services, reputation systems, Internet of Things (IoT), and security services. Blockchain-based applications utilise smart contracts to store any record or transaction of value such as currency, oil, gold, real estate contracts, energy, and intellectual property rights (IPR).

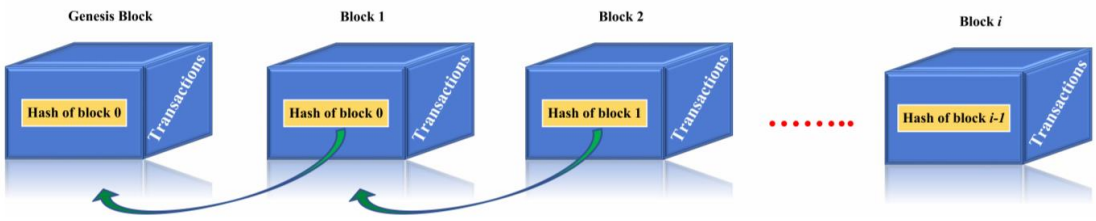
Blockchain technology has two distinct characteristics: anonymity and distributed consensus. Blockchain transactions provide many advantages such as security, decentralization, and instant transactions. This is because Blockchain technology (BT) eliminates the need for intermediary points such as agents or brokers. Since data is an asset in the digital economy, it is crucial to ensure that data in specific applications have not been manipulated or corrupted. *Throughout the years, Blockchain has gone through extensive development, namely digital currency (Blockchain 1.0), digital economy (Blockchain 2.0), and digital society (Blockchain 3.0)*. The first generation is related to the underlying technology platform (i.e., public ledger, hashing, and mining) and overlying protocols (transaction enabling software) to support digital currency. The concept of second generation Blockchain was proposed as an infrastructure for more complex application (i.e., mortgages, derivatives, stocks, and assets that can be monetized). The major innovation of the second generation relies on the usage of Blockchain in managing assets and trust agreements; thus, the concept of smart contracts was conceived. Smart contracts are an emerging use case in this generation, and are defined as computer programs that automatically execute contract terms and manage smart properties. Smart contracts are faster for execution and data can be transferred faster as compared with traditional contracts, making it a key feature in Blockchain technology. Blockchain applications unrelated to economic activity, financial markets, commerce or money are referred to as digital society or Blockchain 3.0. *This generation is associated with broader applications such as education health, science, art and*

governance. In this generation, several technologies are integrated with blockchain, such as cyber physical systems. **In recent years, blockchain technologies have been applied in Electronic Medical Records (EMR) systems to provide control, supervision, accessibility, auditability, and interoperability over large scale data management frameworks using a comprehensive log**. Current blockchain technology enables sharing and consuming computing resources, and delivering computing capabilities anytime, anywhere. It is expected to revolutionize and drive industry and economics because it is secure, fast, trustworthy, immutable, and provides public and private transparent solutions. Transactions on the blockchain ameliorate the need for documentation, duplication, third-party intervention, and remediation. Although blockchain has been used in various applications for secure transactions, there are different challenges that need to be considered when implementing blockchain in healthcare application. This is because healthcare is a regulated domain that involved patient's privacy.

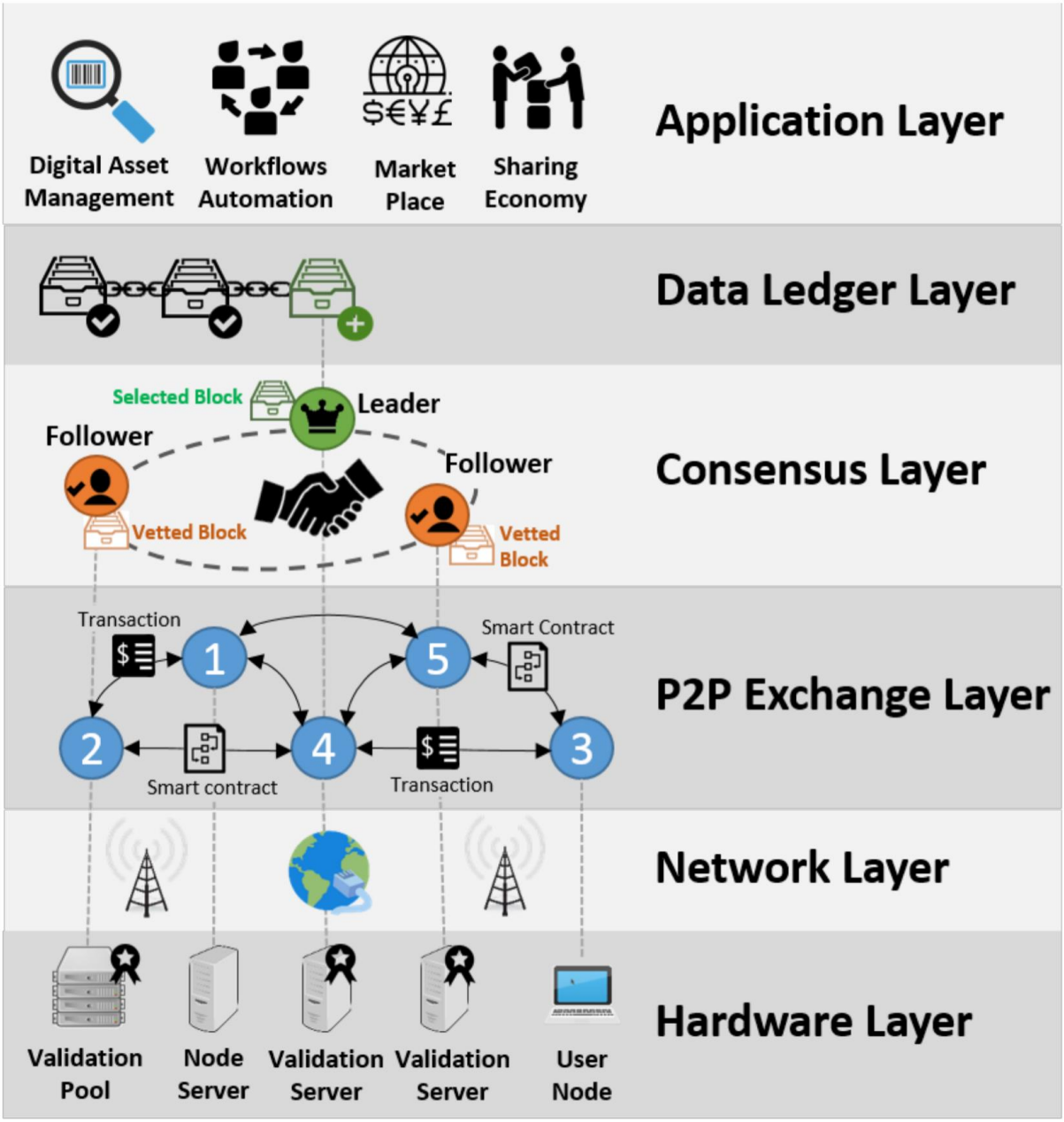
Network architectures can be broadly categorised as *centralized or distributed architecture*. In centralized architecture, a central node is responsible for control and coordination of the whole network. In a distributed architecture, all nodes are connected, eliminating the need for a central point of control. ***A blockchain architecture functions in a peer-to-peer distributed network offering two primary advantages: greater computing power than a centralized architecture, since the computing power of all nodes is combined together; and network reliability, because there is no single point of failure***. Blockchain can also achieve and maintain data integrity in distributed systems due to the high level of security implemented in blockchain technology. The concept of distributed ledger refers to databases that are spread across several computing devices (nodes). Each device updates itself independently through an identical saved copy of the ledger. Blockchain arises from the use of distributed ledgers. However, blockchain and a distributed ledger are not exactly the same. Although both terminologies can be defined as a cryptographically audit trail for a record of consensus of network nodes, distributed ledgers can be implemented using blockchain. Nevertheless, this process is not reversible. Distributed ledgers do not necessarily employ a chain of blocks in order to provide a valid and secure distributed consensus. Blockchain technology manages data by grouping it into blocks and linking these blocks to one another, while using cryptography to provide security.

Blockchain works in a consensus manner where network nodes (called miners) are responsible for adding and validating blocks, which are digital records of immutable (unchangeable) data (such as transactions) stored in packages. Blockchain nodes are responsible for connecting the blockchain network, storing information on the ledger, listening to transactions and newly sealed blocks, validating newly sealed blocks (confirming transactions), passing the valid transaction to the network, and creating and passing new blocks. The blockchain technology, which underlies the distributed ledger, validates the new data (transactions) in the ledger. Each block is generated after fulfilling certain and predetermined requirements. In blockchain, all network nodes receive information about every data or transactions and must verify them in order to be validated. *Platforms such as Ethereum requires all nodes to receive and understand the information*. However, in Corda, only involved nodes receive information about transactions. When the blockchain network contains one or more malicious user(s), unknown reliability and trustworthiness may exist in the blockchain, since unknown peers can exploit

the network for their own purposes. However, it is not easy to break into the blockchain network since there are huge requirements such as computing power and having more than 50% in the network. In blockchain, each block is related to the previous block, and is digitally signed by the responsible miner using a hash function or specifically a hash algorithm (Merkle root hash). The hash function is used to map every single input to a specific hash value to ensure that no duplicate hashing exists. Each block contains the data and hash of the previous block to eliminate any changes or tampering in the blockchain. *New blocks are created when miners validate data using algorithms such as Proof of Work (PoW) and Proof of Stake (PoS) concepts*. For example, PoW requires computing power to calculate the hash associated with a block to be considered valid. When a miner has more computing power, the hash will be calculated more quickly. Thus, the miner is responsible to add the block to the blockchain and receives the associated reward. The associated reward represents the type of reward the user will receive for mining a block. The time of block creation depends on the application and security mechanisms being used. For example, in Bitcoin, it takes 10 min to add a block (to reduce any hyperinflation of the currency), while, in Ethereum, it takes 10 to 20 s. As shown in Figure 2, blockchain can be represented as a conventional public ledger, in which a complete list of transaction (Tx) records is stored on a sequence of blocks (hashed timestamps). Each block has a reference that points to the previous block referred to as the parent block (i.e., block 1 is the parent block of block 2, the genesis block is the parent block of block 1). This reference is represented by a hash value, a single unique value for every block that makes the block valid. The first block of blockchain is called the genesis block, the hash value of the genesis block is straight zeros because it does not have any parent block. Another term that has been proposed by the Ethereum blockchain is the uncle block, which is created when two blocks are mined at the same time. In this situation, one block is considered the official block and added to the chain, while the other remains a stale block and it is called an uncle block (or orphan block in the Bitcoin blockchain). In the Ethereum blockchain, hashes of uncle blocks are also stored [7], unlike Bitcoin, in which the whole block is neglected.



Blockchain lower level architecture



Blockchain high level architecture

Figure 7: Blockchain architecture

The block structure is shown in Figure 8. Every block consists of block version, parent block hash, Merkle tree root hash, timestamp, nBits, and nonce. Block versions illustrate the validation rules that must be followed. Parent hash block represents the hash of the previous block to form a chain. The hash is 256-bit. A timestamp represents the time in seconds since 1970, while nBits indicate the current hashing target, which represents a threshold for the block in order to be valid. nBits is an unsigned integer that the header hash must be below or equal to in order for that header to be a valid part of the blockchain. A nonce is a 4-byte random number generated to produce a hash that makes the block valid. The block hash starts with zeros and the number of zeros increase in time to increase the difficulty of figuring out the hash. Thus, miners continuously calculate and guess the nonce that will produce the

exact hash (including the number of zeros at the beginning), which will make the block valid. In other words, the miners must generate an output that meets certain requirements when plugging the nonce into the hashing algorithm. Miners use brute force to guess the correct value algorithm until an appropriate output value is found. Such calculation is necessary because any change in input data produces an entirely different output. Thus, these calculations must indicate an accurate output that represents a unique input.

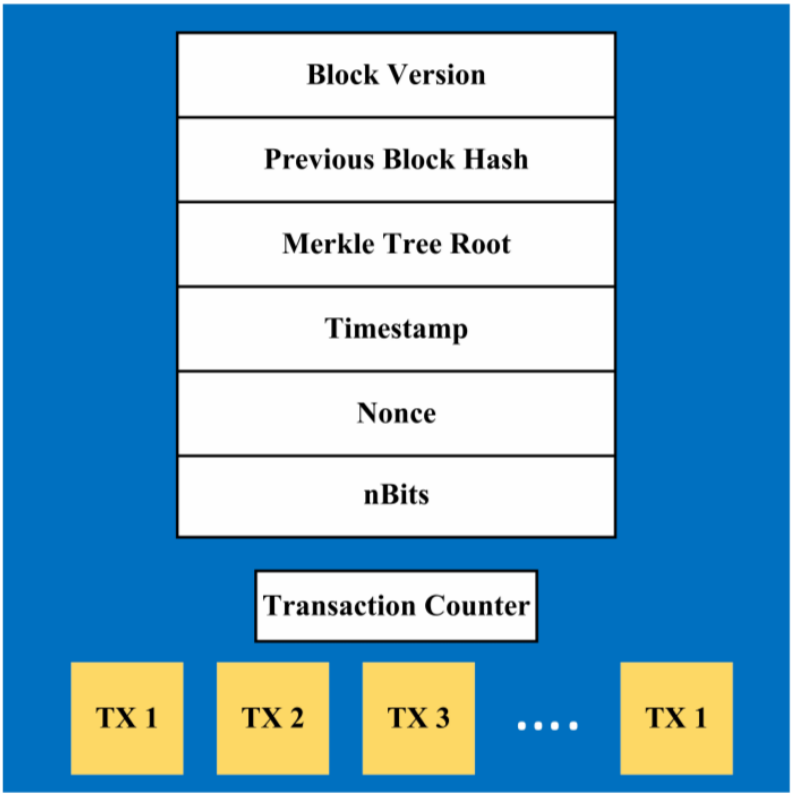


Figure 8: Block header structure

The hash of all transactions in a block is called Merkle tree root as shown in Figure 9. Each pair of transaction hashes is merged together until a single hash is reached for all transactions, which is called Root Hash or Merkle Root. For example, the hashes of transaction A and transaction B are merged together to generate a new hash called Hash AB; the same process is performed with transaction C and D; finally, the root hash (Hash ABCD) is generated by merging Hash AB and Hash CD. The transactions and associated counters are located in the block body. Block size and transaction size are responsible for defining the number of transactions inside a single block. In order to validate the authentication of transactions, blockchain uses a symmetric/asymmetric cryptography mechanism, in which the private key is used to sign and encrypt the data on the sender side. The public key is used to decrypt the data at the receiver side(s). The process of signing transactions produces what is known as a digital signature. The digital signature involves two phases; signing and verification. For example, when user X makes a transaction to user Y, he generates the hash value of the specified transaction. The encryption process is done using user X's (sender) private key. The original data and the encrypted hash are sent to user Y. Anyone in the network can decrypt the hash using the user X's public key.

Thus, user Y decrypts the received hash and compares it with the derived hash of the received data using the hash function of user X to verify the transaction. The Elliptic Curve Digital Signature Algorithm (ECDSA) has been widely used as a digital signature algorithm in blockchains. This is because it has shorter key length as compared to Digital Signature Algorithm (DSA), Rivest-Hsamir-Adleman (RSA) and Diffie–Hellman algorithm. For IoT devices that utilise blockchain technology, a colour spectrum chain can be used to store authentication status of the devices that can access the IoT. In cloud servers, the algorithm confirms the information in the device, stores the authentication state of the identified device in the blockchain, and checks the authentication state of the stored device. When the colour spectrum chain is used in IoT sensors and multi-platforms using blockchain, the vulnerability of IoT devices can be minimised.

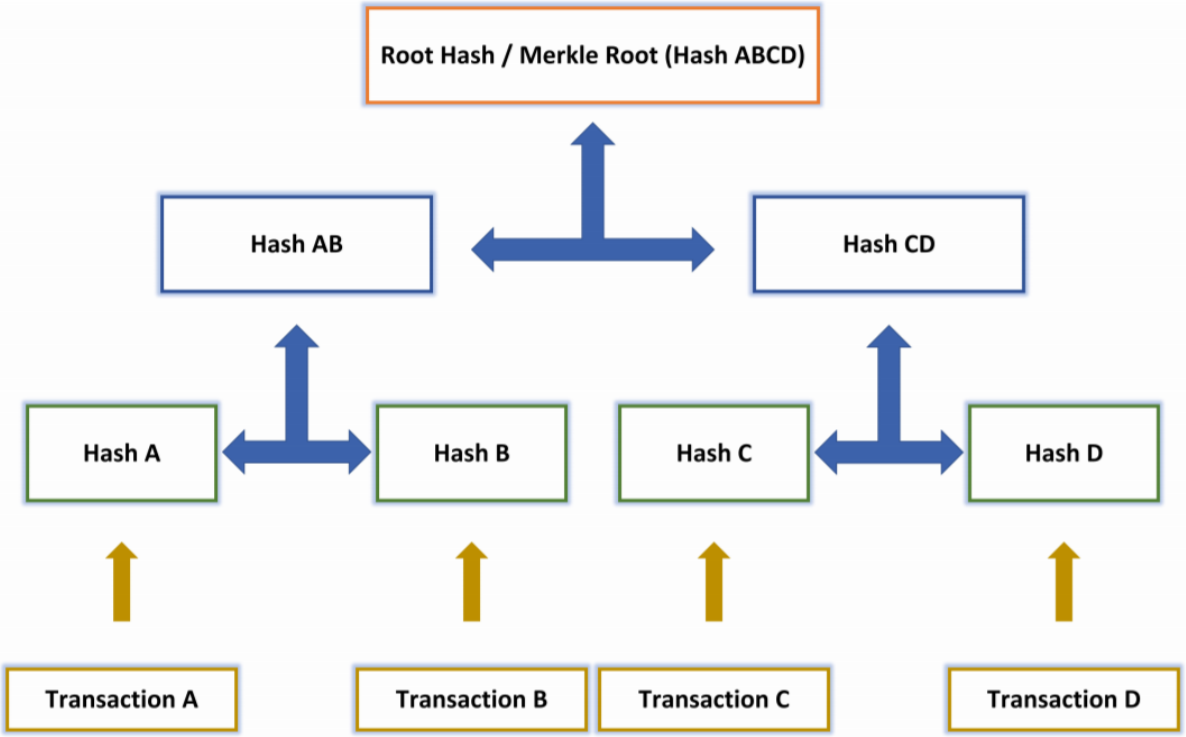


Figure 9: Blockchain Merkle tree root

For any information system, three requirements must be fulfilled to guarantee security: confidentiality, integrity, and availability. Since blockchain is decentralized, it can guarantee the global system functionality even if one or more nodes are compromised. In blockchain, confidentiality includes securing the user's private key because it is needed along with the public key to compromise the system or impersonate someone else (stealing identity). The public and private keys are used to ensure the integrity and security when exchanging information. There is a unique private key for each user, which guarantees the ownership of information for a specific user. The user signs the information with his private key to indicate his authority to the entire network. The public key is derived from the private key based on a specific algorithm that the system uses. The public keys are distributed across the network because they are irreversible (a private key cannot be derived from public keys). Other users need to use public keys to access the information. For example, CONIKS created a key management system

to control and unleash users from encryption key management. Two-step verification is performed in this system. First, the receiver's public key is verified; then, the key is checked to ensure that it is not altered over time. Integrity can be ensured in blockchain because it prevents the information from being tampered with by unauthorised parties. An integrity blockchain-based IoT framework was proposed in to eliminate any trust needed for third parties. Availability is the most straightforward concept achieved by blockchain because of its distributed system design manner. Blockchain security mechanisms prevent hacking through the distributed consensus, ensuring the safety of management systems and the centralized data storage since all transactions are required to be verified and validated by a group or community of miners. Furthermore, a blockchain network is monitored by all nodes in the network, and any malicious node (user) lacks the power to insert manipulated blocks into the public ledger because all nodes maintain a copy of the blockchain. Thus, even hacking several ledgers will not affect the blockchain, since blockchain copies provided by others are considered to be a reliable backup. Blockchain systems have the ability to secure the network from certain malicious activities. However, some of them might cause problem to blockchain network. Although blockchain provides an evolution to current technology, it faces many security challenges such as interoperability, scalability, and data privacy. For example, in a peer-to-peer network, when a user makes more than one payment at the same time using Bitcoins, a security concern known as a double-spending attack arises. This occurs when the pending payments are being broadcasted and, at the same time, the network faces propagation delays or unconfirmed transactions at multiple intervals. To solve this problem, blockchain requires miners to verify the transactions by solving complex mathematical problems (mining procedure). Since it is a time-consuming process and it is hard to solve the problems, usually only one payment passes through correctly and can be registered on the blockchain. Blockchain depends on safeguarding the digital identity (the private key) to provide privacy and anonymity. However, if a key has been possessed or stolen, it is impossible to recover it by any third party, and all the information of the digital identity will vanish. There will then be no way of identifying the person behind it. This process can be very dangerous if third-party institutions are affected.

3.3. Consensus Algorithms

The concept behind blockchain is a secured and trusted architecture due to network consensus. Different consensus algorithms have been implemented in the past for specific applications because each domain has specific requirements. For example, some domains require low computation power, while others require faster processing of transaction. The key function of blockchain technology is consensus algorithm, which illustrates the algorithm needed to reach a total agreement between network nodes during blocks verification process. Consensus algorithms aim to provide equality between miners, giving the same weight to all of them so that majority of the miners can reach a decision. However, while this approach suits controlled environments, this is not possible in a public blockchain because it might lead to Sybil attacks, in which a user can hold multiple identities and control the blockchain. In a decentralized architecture, adding a single block is done only by a single user. The user can be selected randomly or based on certain requirements. Nevertheless, random selection is prone to attacks. The concept of consensus was conceived based on the Byzantine Generals (BG)

problem. During war, Byzantine generals command an army around a single city. The BG problem occurs when these generals must reach an agreement to commence an attack or not. Thus, communication is needed to ensure that there are no traitors between them because any problem in the agreement can lead to an attack failure. This challenge pervades blockchain technology because it is a distributed network, such that no central node can control the whole network. Thus, blockchain has adopted decentralized consensus algorithms to enforce the consistency and reliability of data. Examples of consensus algorithms include Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Transactions as Proof of Stake (TaPoS), Proof of Activity, Proof of Capacity, Byzantine Fault Tolerance (BFT) replication, Practical Byzantine Fault Tolerance (PBFT), Delegated BFT (DBFT), BFTRaft, Proof of Authority (PoA), Proof-of-Stake-Velocity (PoSV), Proof of Burn, Proof-of-Personhood (PoP), Proof of Bandwidth (PoB), Proof of Elapsed Time (PoET), Stellar Consensus Protocol (SCP), Bitcoin-NG, Sieve, Ripple, and Tendermint, among others. Proof of Work (PoW) follows a concept of work, where it is based on the fact that nodes are less likely to attack the network if they perform a lot of work. PoW-based blockchain requires miners to perform computationally expensive tasks (carried out by multiple entities) in order to add a block to the blockchain, thus making it almost impossible for Sybil attacks. PoW works in a manner called mining; nodes will perform calculations until a solution is found. For example, in Bitcoin blockchain, the calculation process aims to find a random number (called nonce) in order to generate the correct hash of block header. Thus, miners must have the ability to perform a certain amount of work in order to calculate the number. When a miner solves the problem, all other nodes are responsible for verifying that the answer is correct. PoW consumes more energy, making it inefficient to be used in low power applications. In addition, PoW nodes that participate in block verification do not correspond to the increase of block transactions; thus, it not scalable.

Proof of Stake (PoS) divides users by their stake of the blockchain. Each node that has a certain amount of stake in the blockchain can be a miner. This consensus algorithm assumes that a user with more stake has a lower possibility to attack the network. Nodes allocate a specific amount of their stake when they become a miner. Thus, the network will hold that amount to make sure that a user is trusted and allowed to mine. PoS has lower energy consumption than PoW because it requires less computational power. The issue with PoS is that the mining process of blockchain targets the wealthiest participants, since they can own a higher stake than other nodes. Delegated Proof of Stake (DPoS) is another consensus algorithm proposed to enhance PoS. In this algorithm, instead of assigning the generation and validation of blocks to the stakeholders, certain delegates are responsible for that procedure. One of the advantages of this consensus algorithm is faster transactions since fewer nodes are involved. In addition, the chosen nodes are able to adjust block size and intervals. Dishonesty can be treated faster because delegated nodes are substituted easily. Transactions as Proof of Stake (TaPoS) is a PoS variant. Unlike PoS, where certain nodes contribute to the security of the network, all nodes contribute to the security framework in TaPoS. In PoS, the limitation is due to stake age that is accumulated, even when the node is not connected to the network. Proof of Activity (PoA) is proposed to reward nodes based on their activity and ownership on the blockchain. Practical Byzantine Fault Tolerance (PBFT) has been proposed for asynchronous environments to solve the Byzantine Generals Problem. It assumes that more than 2/3 of total nodes are legitimate, while less than a third are

malicious. A leader is selected through each block generation, the leader is responsible for ordering transactions. In order to add a block, a minimum of 2/3 of all nodes must support the validation of block. Delegated BFT (DBFT) is a variant of BFT, and works in a similar manner to DPoS, where a certain number of nodes are responsible for validating and generating blocks. Stellar Consensus Protocol (SCP) is similar to PBFT. This algorithm is implemented based on an algorithm called Federated Byzantine Agreement (FBA). The difference between this algorithm and PBFT is that PBFT requires an agreement from majority of the nodes. SCP relies on a subset of nodes that it considers important. Ripple has been proposed to solve the issue of light latencies caused by synchronous communication between nodes. The nodes are defined as trusted to create a subset to determine network consensus, and the subset is connected to a specific server to reduce latency. BFTRaft enhances the Raft algorithm by increasing its security through reformulating it into a Byzantine fault-tolerant algorithm. Tendermint consensus algorithm tolerates up to 1/3 of failures, and it can host arbitrary application states. Network nodes are named validators, which create blocks and vote on whether these blocks are valid or not. To add a block, Tendermint divides the validation process into two stages: pre-vote and pre-commit. When more than 2/3 of validators commit a block, the block is committed and considered valid. BitcoinNG is another consensus algorithm that aims to improve latency, throughput, and scalability. Bitcoin-NG is proved to operate optimally. However, it has limitations in terms of latency of propagation time and nodes' bandwidth. Proof-of-Burn (PoB) is used to define how miners are committed to mining by requesting them to show a proof of their mining activities by burning cryptocurrency (or data that can be spent) to a specific address (spendable address in case of cryptocurrency), instead of consuming (burning) resources. The Proof-of-Personhood (PoP) algorithm is used to provide anonymity through binding physical to virtual identities using ring signatures and collective signing. The Sieve algorithm is Hyperledger-Fabric implementation proposed by IBM research. It uses BFT replication in permissioned blockchain to run non-deterministic smart contracts. Non-deterministic smart contracts processes are replicated in the network and the results are compared. The results are sieved out if a divergence among results is detected within the replicated results. This design sieves out the whole operation if the divergent processes results are excessive. The advantages and drawbacks of different blockchain consensus algorithms are discussed in Table 2.

Table 2: Advantages and disadvantages of blockchain consensus algorithms

Algorithm	Advantages	Drawbacks
Proof of Work (PoW)	- Provides comprehensive decentralization of power and control in the network - More secure network	- High processing power (expensive) - High electricity consumption - Small networks can be compromised
Proof of Stake (PoS)	- More energy efficient - Better rewards with bigger stakes - Provides faster processing of transactions	- Less decentralized network than PoW - Less security than PoW

Delegated Proof of Stake (DPoS)	- Faster processing than PoW and PoS - Better rewards distribution - Energy efficiency - Lower hardware expenses	- More susceptible to attacks - Richer people control the network - Less resiliency due to less decentralization
Transactions as Proof of Stake (TaPos)	- More security than PoS since all nodes contribute in the network - Provides a simplified PoS algorithm	- Lower speed than DPoS since all nodes included - Does not work well when there are short forks on the blockchain
Proof of Activity (PoA)	- High security - Eliminates 51% attack in blockchain network - Improve network topology - Low transaction fees	- Requires large amount of resources in mining phase - Stakeholders have the ability to double sign transactions - Difficult to implement
Practical Byzantine Fault Tolerance (PBFT)	- Ability to make transactions without the need of confirmation like in PoW - Significant energy usage reduction	- Works only in small consensus group sizes due to a high amount of communication between nodes - PBFT uses MACs which is extremely inefficient compared to the communication needed - Hard to prove the authenticity of a message to third parties - Susceptible to Sybil attacks
Delegated BFT (DBFT)	- Provides perfect finality (confirmation of transactions) - No forks with DBFT - Fast transaction execution	- Susceptible 51% attack - Still considered centralized
Steller Consensus Protocol (SCP)	- Efficient decentralized control with large network - Low latency - Flexible trust & asymptotic security	- Fits finance better than any other systems - Problem with choosing quorums and propose new arguments - Inefficient in terms of number of sent messages
Ripple	- Fast transactions - Low power consumption compared to PoW - Path dependent; the chain is uneditable	- Unique Node Lists (UNLs) must be maintained, if UNLs is broken, the network might collapse - It is highly centralized

	- No capacity limitation for the number of transactions	
BFTRaft	- Can tolerate failure of up to 1/2 of the node count - Design simplicity and robustness	- The current implementation can only be considered to guarantee liveness for one Byzantine failure
Tendermint	- Similar to PoS	- Similar to PoS
Proof-of-Burn (PoB)	- Encourages long-term involvement - PoB implementation can be customized - The power of burnt coins decays or reduces partially each time a new block is mined	- Rich get richer problem - Resource waste (the burnt coins are wasted) - High risk protocol, no coin recovery guarantee
Proof-of Personhood (PoP)	- Eliminates PoW and PoS disadvantages	- Fits finance better than any other systems

Chapter 4 - Blockchain technology implementation examples

As blockchain technology matures, businesses in almost every industry are exploring how to capture new opportunities. This chapter reviews a selection of promising and disruptive examples of blockchain application and considers how these can inform future direction.

4.1. Citizen Services – Provisioning Digital Identities

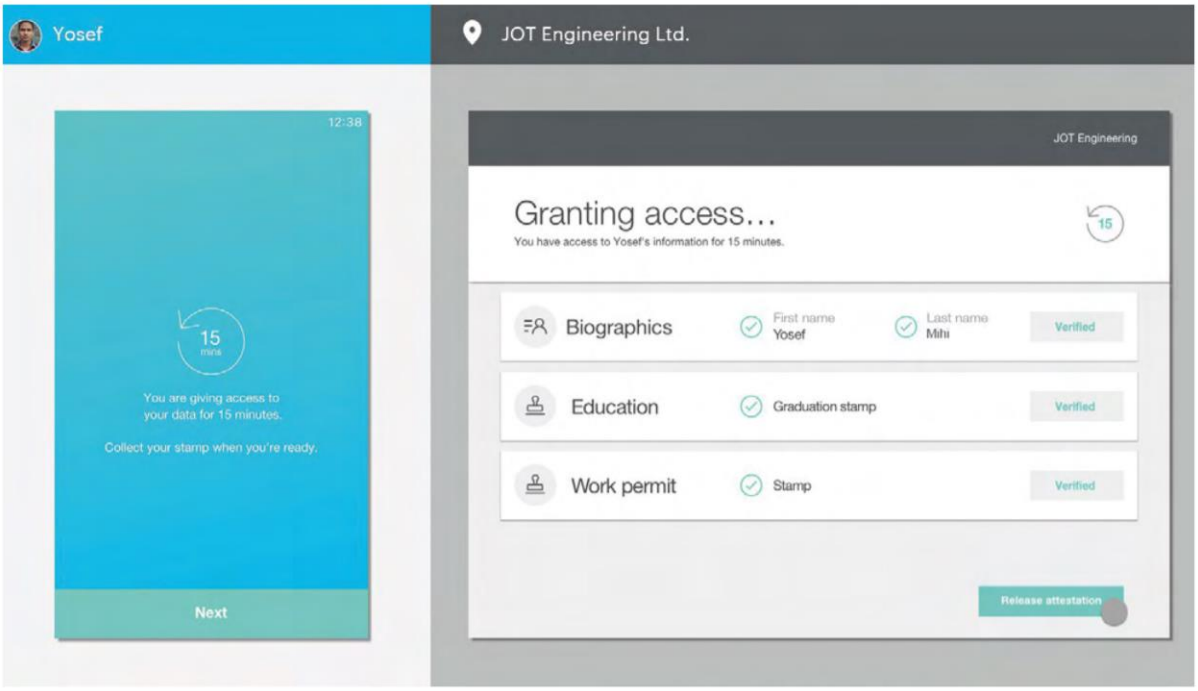


Figure 10: ID2020 – a global ID system using blockchain (Source: Microsoft/Accenture)

Approximately one-sixth of the world's population cannot participate in political, economic and social life because they lack the most basic information: documented proof of their existence.

Blockchain technology provides a tremendous opportunity to solve this challenge through the development of digital identity systems that are cryptographically secure. Governments and non-governmental organizations (NGOs) can use digital identities to provide a variety of citizen services and eliminate certificate forgery and identity theft.

ID2020, an organization affiliated with the United Nations, seeks to provide proof of identity to people without an official form of identification. In essence, ID2020 is using blockchain technology to provision global IDs – its system lets registered users control their personal data to share access and appropriate information without the worry of Figure 10: ID2020 – a global ID system using blockchain; Source: Microsoft/Accenture using or losing paper documentation. Blockchain enables system security and

facilitates trusted transactions, allowing the people with digital IDs to access a wide range of activities, including education, healthcare, voting, banking, housing, and other social benefits.

The ID2020 prototype is designed to interoperate with existing identity systems so that personally identifiable information always resides off chain . The system will deploy a breakthrough biometrics system to manage fingerprints, iris and other data. Coordinated with **Accenture and Microsoft**, the ID2020 alliance expects to move from prototype to implementation with the aim of supporting more than seven million refugees from 75 countries by 2020.

4.2. Retail – Encouraging and Ensuring Ethical, Sustainable Consumption

Blockchain technology is being applied by retailers and consumer goods manufacturers to drive fair and responsible business. For example, it is empowering consumers by providing more information about how each item was produced, particularly identifying whether a product has been ethically and sustainably sourced.

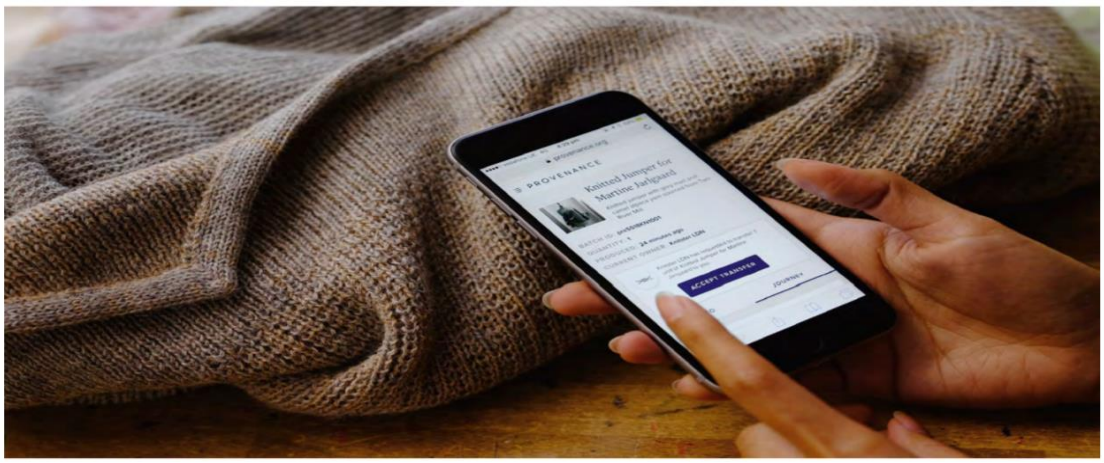


Figure 11: Increasing transparency in fashion supply chains (Source: Provenance)

In the UK, the fashion designer **Martine Jarlgaard** is collaborating with **Provenance** and other partners in a pilot program that makes fashion supply chains fully transparent. This solution encourages and enables consumers and retailers to buy goods from fashion supply chains in which each stakeholder adheres to ethical and sustainable business practices. Users can look up a garment's supply chain history on the blockchain-based system by scanning its QR code or NFC-enabled label with a smartphone app. Building on this successful pilot program, Provenance is now working towards an open traceability protocol. This would allow anyone to track the place of origin for anything, from coffee beans to a roll of fabric, and hopefully accelerate the movement towards sustainable consumption.

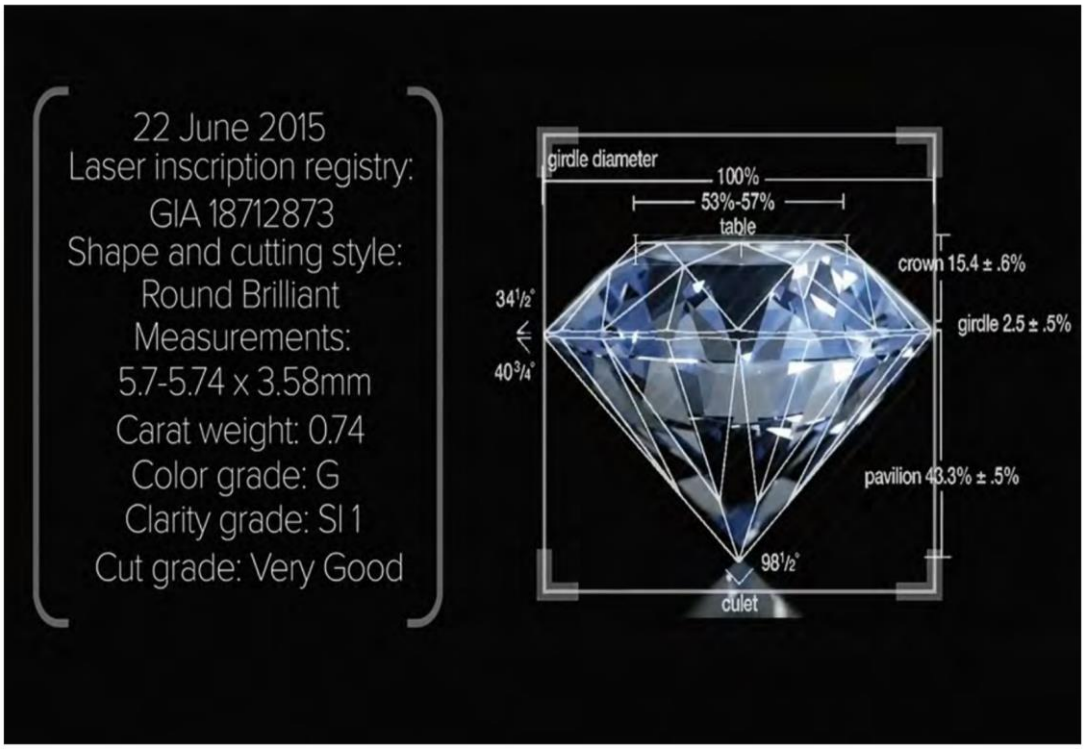


Figure 12: Ethical sourcing of diamonds using blockchain (Source: Altoros/Everledger)

Another example of ethical sourcing is from **Everledger** in the UK. Everledger is developing a blockchain-based system to provide secured proof of origin and ethical sourcing for high-value goods such as diamonds, wine, and even fine art. It uses blockchain to store a digital record for millions of precious goods. For diamonds, this system would replace the flawed paper-based certification process currently used by diamond suppliers, intermediaries and buyers. Unlike paper records which may be forged or lost, blockchain records are permanent. Everledger achieves this by creating a digital thumb-print for each individual diamond. This digital thumb-print contains unique identifiers that consist of over 40 metadata points, the diamond's four Cs (color, clarity, cut, and carat weight) as well as the certificate number which can be laser inscribed on the physical diamond if required. This thumb-print is then made visible and stored with all participants on the blockchain-based system.

4.3. Life Sciences and Healthcare – Enabling a Single Source of Truth

When data is stored on a blockchain-based system, stakeholders gain controlled access to a single source of truth for the most current and reliable dataset. In the life sciences and healthcare industry, where data is often stored in silos and data security is paramount, blockchain has huge potential to be deployed privately and securely. The wide range of applications include clinical trial results, health records management, infectious disease reporting, insurance policies, pharmaceuticals serialization, track and trace, vaccination histories, and many more.

The **United States Food and Drug Administration** (FDA) is exploring the use of blockchain to share and audit electronic medical records, clinical trial results, and health data. By doing so, difficult-to-access data can be securely managed on one blockchain platform shared among stakeholders, driving transparency as well as unlocking potential new efficiency gains. In October 2017, this work expanded

to assist the United States **Centers for Disease Control and Prevention (CDC)** in testing a blockchain-based platform for health surveillance. This solution aims to enable more efficient management of data during a health crisis. The CDC is expected to move from the prototyping phase to application deployment during 2018.

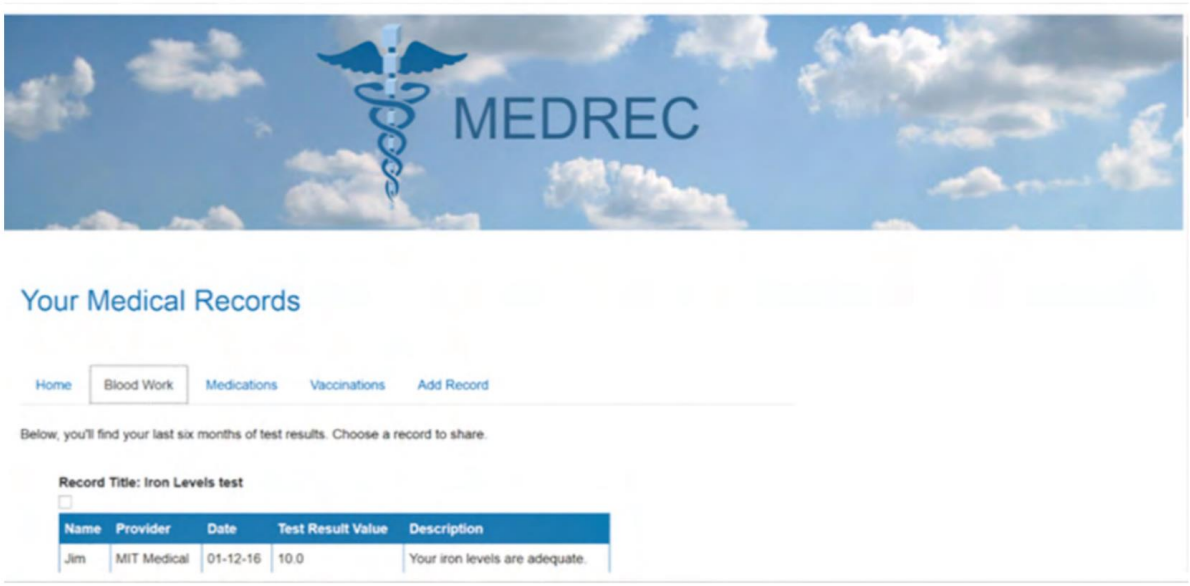


Figure 13: Revolutionizing medical records through a single source of truth (Source: MIT Media Lab)

Other projects are building towards a vision of individual patients controlling their own healthcare data. All of a patient's data from each of their healthcare providers and pharmacies could be stored, and the patient could choose to share (or not share) this data with specific healthcare providers. A prototype system by **MIT Media Lab** called MedRec is getting close to realizing this vision with a blockchain-based system to keep track of each patient's medication.

4.4. Automotive and Manufacturing – Managing Physical Assets with Blockchain

Some of the excitement surrounding blockchain technology in the automotive and manufacturing industries is to do with its application in digital twins.

A digital twin is a dynamic, digital representation of a physical asset which enables companies to track its past, current and future performance throughout the asset's lifecycle. The asset, for example a vehicle or spare part, sends performance data and events directly to its digital twin, even as it moves from the hands of the manufacturer to the dealer and ultimately the new owner. Blockchain can be used to securely document everything related to the asset.

Figure 14: Documenting all aspects of a vehicle using blockchain (Source: Dassault Systèmes)

Groupe Renault is experimenting with storing the digital twin of its vehicles on a blockchain-based system which would provide a single source of truth for each vehicle's maintenance data. In July 2017, the company released a prototype that was created in collaboration with **Microsoft** and **VISEO** – it uses blockchain to connect each new vehicle's maintenance events to the vehicle's digital twin. This data is fully traceable and visible to authorized parties such as the vehicle owner. As the digital twin is fully transferable on the blockchain-based system, each vehicle's maintenance history remains connected to the vehicle even when there is a change of vehicle ownership – a very useful and practical data management service that automotive companies can provide to their customers.

For a different reason, **Bosch** and a German certification authority, **TÜV Rheinland**, are also experimenting with digital twins of vehicles. These organizations aim to prevent illegal odometer manipulation. In Germany, one of Europe's largest used car markets, it is estimated that every third car has been subject to illegal odometer manipulation. The fraudulent increase in value per car is estimated to be USD $3,700 alone, which in Germany means almost $7.5 billion in fraud every year.

Figure 15: Eliminating illegal odometer manipulation (Source: TÜV)

To solve this challenge, the partners created a blockchain-based system with an in-car connector to regularly record the distances travelled by each vehicle which acts as an ongoing, tamper-evident record of odometer readings. Here, the recorded data on a distributed blockchain network makes it obvious if an odometer is manipulated. This use case shows how manufacturers can increase data credibility and protect public safety; it also has value for regulators, fleet owners and drivers who need access to trusted data on used vehicles.

In future, the entire automotive industry could collaborate on a single blockchain-based platform to store the digital twin of every vehicle, including important events and status updates. This would allow, for example, maintenance data and odometer readings to be stored together as a comprehensive record. Of course, to become reality this would necessitate industry-wide collaboration.

4.5. Energy – Eliminating Marketplace Inefficiencies

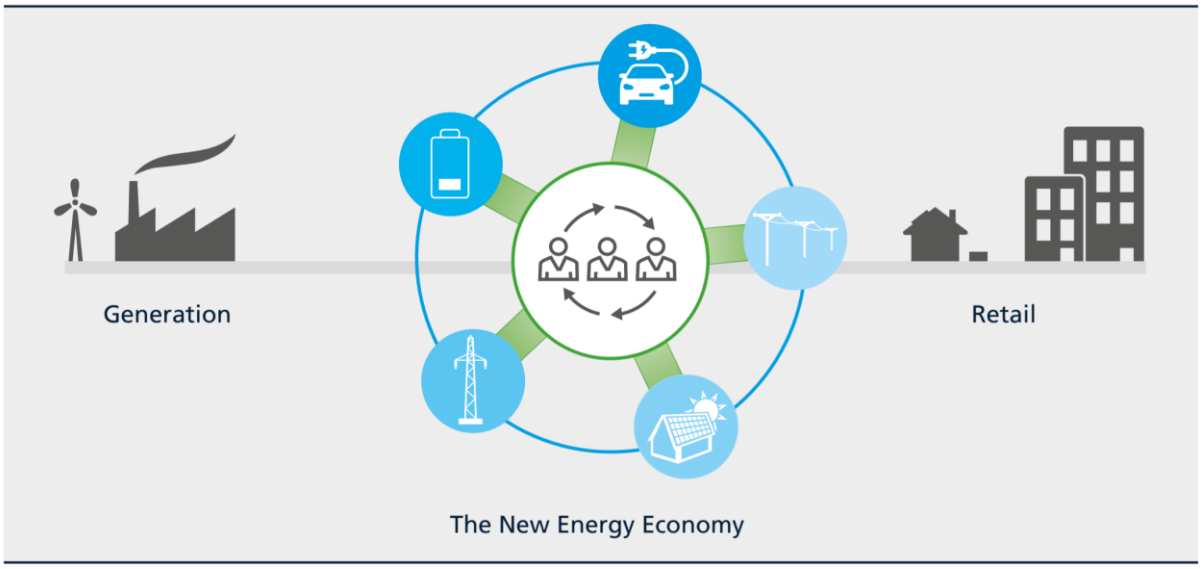


Figure 16: New energy marketplaces based on blockchain (Source: Power Ledger)

The energy industry is likely to find many uses for blockchain technology. Transformational examples include enabling the operation of self-managing utility grids and facilitating peer-to-peer energy exchanges – individual households could sell surplus energy (self-generated by solar panels) to their neighbours. In addition, there are many near-term examples of process improvements that could help energy companies to run more efficiently and save money.

Power Ledger, an Australian startup, has created a local marketplace to sell surplus renewable energy through cryptocurrencies (see figure 16). The blockchain-based system enables the sale of surplus energy generated at residential and commercial developments connected to existing electricity distribution networks, or within microgrids. This empowers renewable energy asset owners to decide who they want to sell their surplus energy to and at what price, and allows for each unit of electricity to be securely tracked from the point of generation to the point of consumption.

From local to cross-border trading, **BP**, **Eni Trading & Shipping**, and **Wien Energie** completed a European energy trading pilot program in mid-2017 using a proprietary blockchain development platform from **BTL Group** in Canada. This pilot used blockchain technology to streamline cross-border trading and back-office processes such as confirmations, actualizations, invoice generation, settlement, auditing, reporting, and regulatory compliance across the energy trade lifecycle. BTL Group now aims to create a live, commercial version of an energy trading solution that will reveal significant cost savings applicable to numerous areas of the energy sector.

It's clear that companies in almost every industry are starting to unlock greater efficiencies and new business models using blockchain. They're doing so by leveraging many of the key capabilities of this technology including data transparency, security, asset management, and smart contracts – all of which can be widely used in logistics. The next chapter explores the ways in which blockchain technology is already benefitting the logistics industry and investigates how it could shape logistics in the near future.

4.6. Fighting counterfeit pharmaceutical goods through Blockchain

One key application is the use of blockchain technology to combat a major challenge in the world today: the counterfeiting of drugs and false medication. According to Interpol, around 1 million people each year die from counterfeit drugs15, 50% of pharmaceutical products sold through rogue websites are considered fake, and up to 30% of pharmaceutical products sold in emerging markets are counterfeit. To answer this challenge, DHL and Accenture are driving a blockchain-based serialization project providing sophisticated track-and-trace capabilities to the pharmaceutical industry (see figure 17).

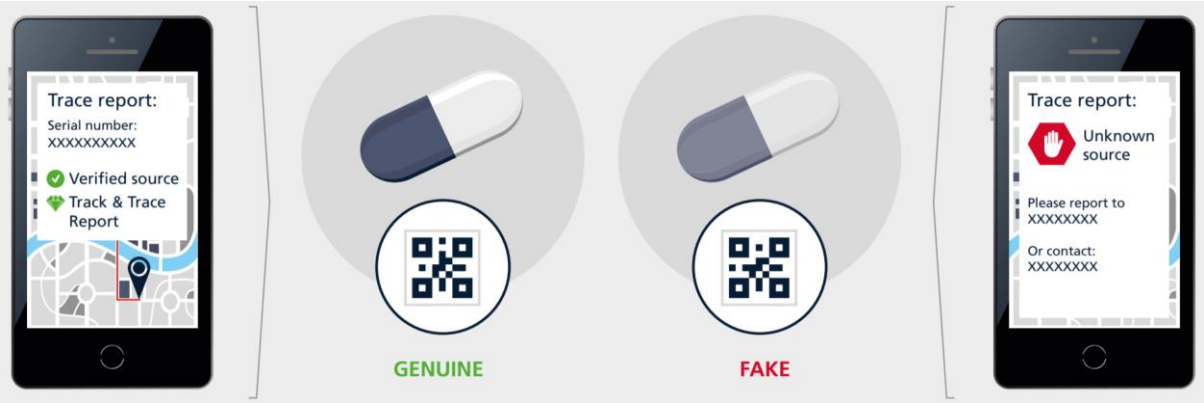


Figure 17: Blockchain can be used to ensure product integrity (Source: DHL)

Pharmaceutical serialization is the process of assigning a unique identity (e.g., a serial number) to each sealable unit, which is then linked to critical information about the product's origin, batch number, and expiration date. Serialization effectively enables a unit to be tracked at virtually any moment, and traced to its location at any stage of its lifecycle. A key serialization challenge is maintaining traceability and transparency especially when these units are repackaged or aggregated from unit to case to pallet for logistics purposes and then disaggregated back down to unit level for consumption.

The DHL /Accenture proof-of-concept was established to overcome this and other challenges by demonstrating the effectiveness of blockchain technology in product verification. The aim is to show that pharmaceutical products have come from legitimate manufacturers, are not counterfeit, and have been correctly handled throughout their journey from origin to consumer.

Most importantly, this initiative proves how end customers can verify the legitimacy and integrity of pharmaceutical products, especially compliance with handling requirements. This not only reassures the end customer at the point of purchase that their medicines are genuine and in perfect condition, but has potentially life-saving implications. To achieve this, the partners have established a blockchain-based track-and-trace serialization prototype comprising a global network of nodes across six geographies. The system comprehensively documents each step that a pharmaceutical product takes on its way to the store shelf and eventually the consumer (see figure 18 on next page). The prototype was a lab performance simulation that demonstrated how blockchain technology could handle volumes of more than 7 billion unique pharmaceutical serial numbers and over 1,500 transactions per second. The project illustrated how blockchain can be used to capture all logistics activities relating to an item of medication – from production to purchase – and ensure this information is made secure, transparent,

and immediately available. Our proof of concept demonstrated the opportunities blockchain presents in the fight against counterfeit pharmaceutical goods. Together with our partners we are actively refining the solution as well as working with key industry stakeholders to operationalize the concept states Keith Turner, CIO Chief Development Office at DHL Supply Chain.

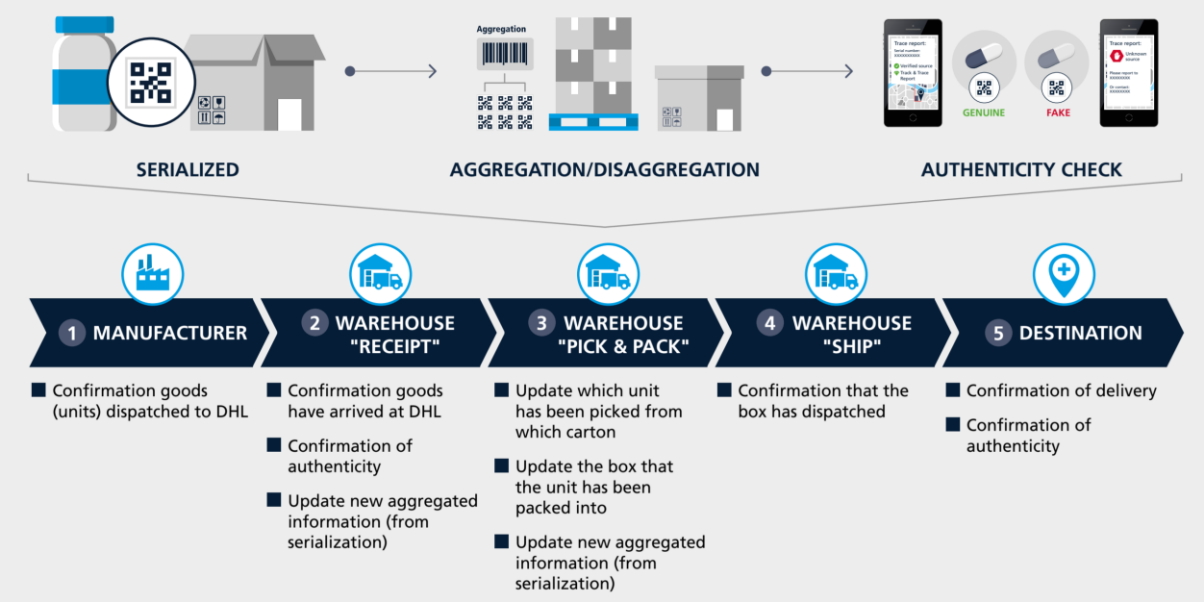


Figure 18: Simplified example of how a blockchain-based track-and-trace system can be used to monitor pharmaceutical goods from manufacturer to end user (Source: Accenture/DHL)

In the consumer goods and retail industry, companies like **Unilever** and **Wal-Mart** are exploring the use of blockchain technology to improve supply chain transparency and to track provenance. Wal-Mart is focusing specifically on food tracking, traceability, and safety (see figure 19).

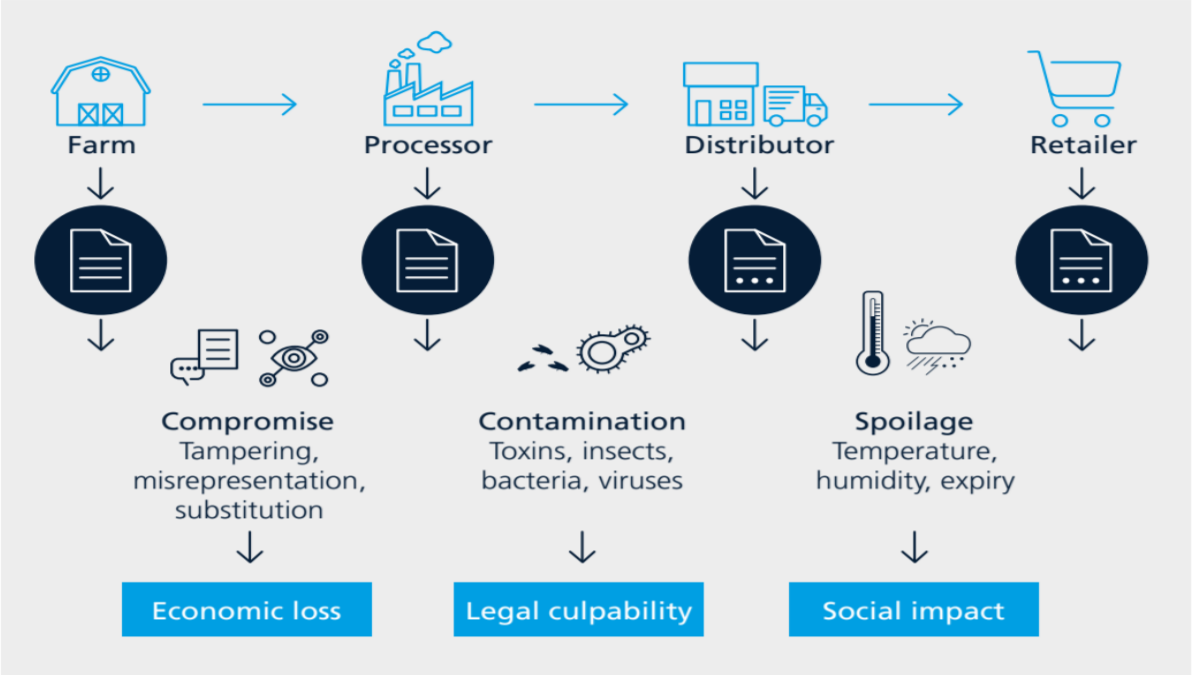


Figure 19: An example of using blockchain to increase safety and reveal product provenance in food supply chains (Source: IBM)

Together with partners, Wal-Mart has conducted a blockchain test designed to trace the origin and care of food products such as pork from China and mangoes from Mexico. To begin with, this initiative documented the producer of each specified food product so that Wal-Mart can easily address any case of contamination, should this arise. Secondly, the test put mechanisms in place to identify and rectify the improper care of food throughout the journey from farm to store. For example, since meat shipments must not rise above a certain temperature, the test took temperature data from sensors attached to the food products and committed this data to the blockchain-based system. From there, automated quality assurance processes notified relevant parties in the event of suboptimal transport conditions. Since launching this test, Wal-Mart has also announced the creation of a Blockchain Food Safety Alliance, an extensive partnership to apply tracking, traceability, and safety benefits to food supply chains in China.

Moving forward, a key requirement for track-and-trace applications will be to adopt more secure and intelligent forms of digital identity for each physical product – moving from the provision of a passive barcode or serial number to, for example, enabling interactivity with the use of Internet of Things (IoT) sensors. Smart devices can be securely tied to or embedded in the physical product to autonomously record and transmit data about item condition including temperature variation, to ensure product integrity, as well as any evidence of product tampering.

4.7. Blockchain in logistics

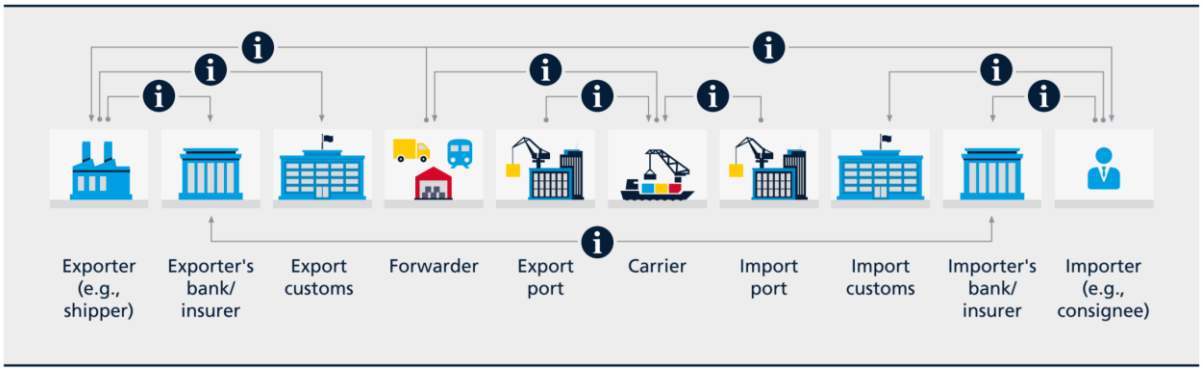


Figure 20: The information flow in international trade is complex, involves many parties, and is documentation heavy (Source: Accenture)

Achieving excellence in logistics involves working collaboratively with others to optimize the flow of physical goods as well as the complex flow of information and financial transactions (see figure 20). But today there is a significant amount of trapped value in logistics, largely stemming from the fragmented and competitive nature of the logistics industry. For example, in the US alone, it is estimated that there are over 500,000 individual trucking companies. With such a huge number of stakeholders involved in the supply chain, this often creates low transparency, unstandardized processes, data silos and diverse levels of technology adoption. Many parts of the logistics value chain are also bound to manual processes mandated by regulatory authorities. For example, companies must oftentimes rely on manual data entry and paper-based documentation to adhere to customs processes. All this makes it difficult to track the provenance of goods and the status of shipments as they move along the supply chain, causing friction in global trade. Blockchain can potentially help to overcome these frictions in logistics

and realize substantial gains in logistics process efficiency. This technology can also enable data transparency and access among relevant supply chain stakeholders, creating a single source of truth. In addition, the trust that is required between stakeholders to share information is enhanced by the intrinsic security mechanisms of blockchain technology.

Furthermore, blockchain can achieve cost savings by powering leaner, more automated, and error-free processes. As well as adding visibility and predictability to logistics operations, it can accelerate the physical flow of goods. Provenance tracking of goods can enable responsible and sustainable supply chains at scale and help to tackle product counterfeiting. Additionally, blockchain-based solutions offer potential for new logistics services and more innovative business models.

Below exploring some of the most prominent use cases for blockchain in the areas of global trade logistics, supply chain transparency and traceability, and commercial processes in logistics (see figure 21).

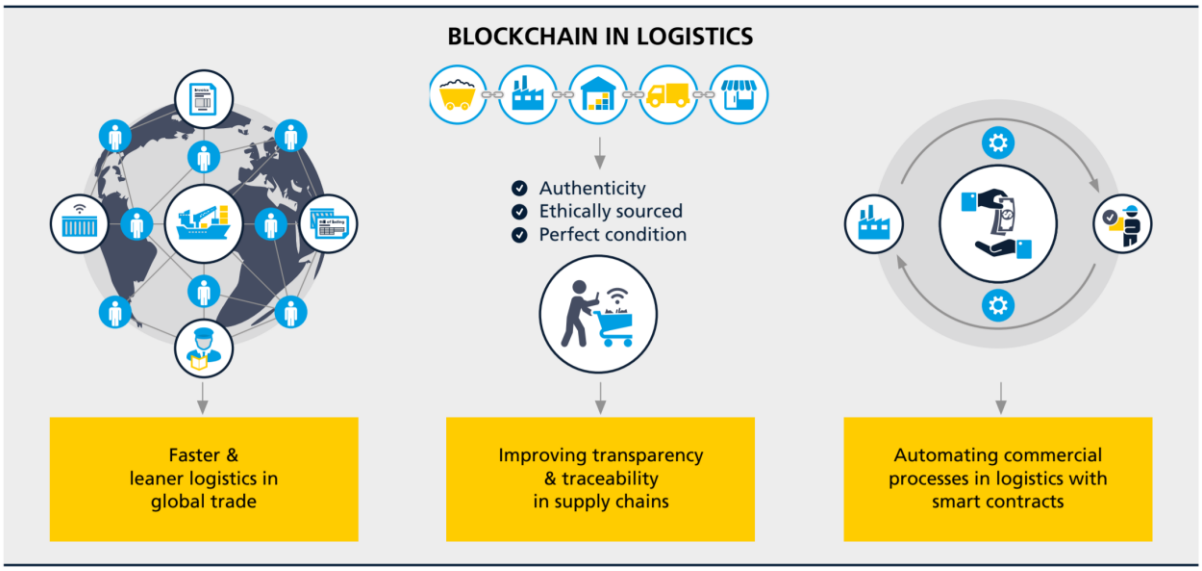


Figure 21: Key blockchain use cases in logistics (Source: DHL)

4.8. Faster and Leaner Logistics in Global Trade

Figure 22: Blockchain can streamline the global movement of freight (Source: Maersk)

Logistics is often considered the lifeblood of the modern world, with an estimated 90% of world trade carried out by the international shipping industry every year. But the logistics behind global trade is highly complex as it involves many parties often with conflicting interests and priorities as well as the use of different systems to track shipments. Therefore, achieving new efficiencies in trade logistics is likely to have significant impact on the global economy. According to one estimate from the World Economic Forum, reducing supply chain barriers to trade could increase global gross domestic product (GDP) by nearly 5% and global trade by 15%. Blockchain technology can help alleviate many of the frictions in global trade logistics including procurement, transportation management, track and trace, customs collaboration, and trade finance. With over 50,000 merchant ships involved in the global shipping industry and multiple customs authorities regulating the passage of freight, a major area of focus for efficiency gains is ocean freight. Blockchain technology has huge potential to optimize the cost as well as time associated with trade documentation and administrative processing for ocean freight shipments. One example that highlights the complexities behind ocean freight today is the estimate that a simple shipment of refrigerated goods from East Africa to Europe can go through nearly 30 people and organizations, with more than 200 different interactions and communications among these parties.

To unlock efficiency in ocean freight, **Maersk** and **IBM** have started a venture to establish a global blockchain-based system for digitizing trade workflows and end-to-end shipment tracking (see figure 23). The system allows each stakeholder in the supply chain to view the progress of goods through the supply chain, understanding where a container is in transit. Stakeholders can also see the status of customs documents, and can view bills of lading and other data. Blockchain technology ensures secure data exchange and a tamper-proof repository for this documentation. The two companies expect this solution to track tens of millions of shipping containers annually. It has the potential to significantly reduce delays and fraud, which could lead to billions of dollars in savings in the logistics industry.

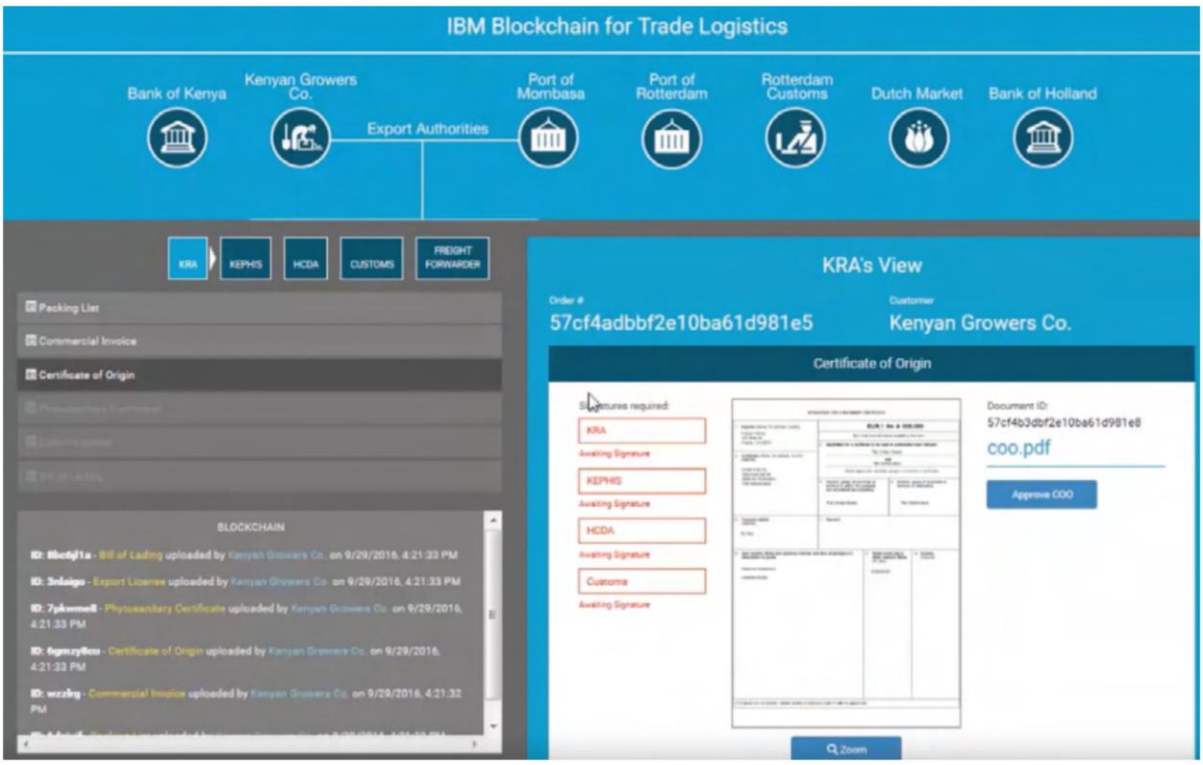


Figure 23: Digitalizing global trade logistics (Source: Maersk/IBM)

Ocean carrier company **ZIM** has conducted a pilot to digitize the actual bill of lading, often hailed as a 'holy grail' application in logistics. The bill of lading is one of the most important documents in ocean shipping, and it acts as a receipt and a contract for the goods being shipped. The information stored on a bill of lading is critical as it contains all necessary details such as the shipment description, quantity and destination, as well as how the goods must be handled and billed. During the trial of a blockchain-based system developed by Wave, ZIM and pilot participants issued, transferred, and received original electronic documents successfully through the decentralized network.

The containers, shipped from China to Canada, were delivered to the importers (i.e., consignees) without a problem. Although still in pilot phase, industry adoption of a digital bill of lading would be significant. It could greatly support supply chains in reducing costs, enabling error-free documentation and fast transfer of original documents. **Accenture** is developing a blockchain-based system also focused on replacing the traditional bill of lading as well as facilitating a single source of truth for all supply chain stakeholders for freight inquiries up to issuance of trade documents. Here, a decentralized network connects all parties in the supply chain and enables direct communication, eliminating the need to go through central entities and rely on intermediaries. According to Adriana Diener, Global Freight & Logistics Lead at Accenture, the proven value of this project is surpassing expectations: Using blockchain to replace the traditional bill of lading documentation to ship goods will drive millions of dollars in process efficiency and operational cost reduction benefits across the supply chain for multiple parties in the trade ecosystem including shippers, consignees, carriers, forwarders, ports, customs agencies, banks, and insurance companies .

4.9. Improving Transparency and Traceability in Supply Chains

Many projects are underway using blockchain technology to improve supply chain transparency and monitor provenance. These initiatives amass data about how goods are made, where they come from, and how they are managed; this information is stored in the blockchain-based system. This means that the data becomes permanent and easily shared, giving supply chain players more comprehensive track-and-trace capabilities than ever before. Companies can use this information to provide proof of legitimacy for products in pharmaceutical shipments, for example, and proof of authenticity for luxury goods. These initiatives also deliver consumer benefits – people can find out more about the products they are buying, for example, whether a product has been ethically sourced, is an original item, and has been preserved in the correct conditions.

4.10. Automating Commercial Processes in Logistics with Smart Contracts

Current industry estimates indicate that 10% of all freight invoices contain inaccurate data which leads to disputes as well as many other process inefficiencies in the logistics industry.18 This problem is so prevalent that in the oil and energy industry alone, Accenture expects that at least 5% in annual freight spend could be reduced through improved invoice accuracy and reduction of overpayments.

Blockchain has the significant potential to increase efficiency along the entire logistics and settlement process including trade finance and help to resolve disputes in the logistics industry. As digitized documents and real-time shipment data become embedded in blockchain-based systems, this information can be used to enable smart contracts (see figure 24). These contracts can automate commercial processes the moment that agreed conditions are met.

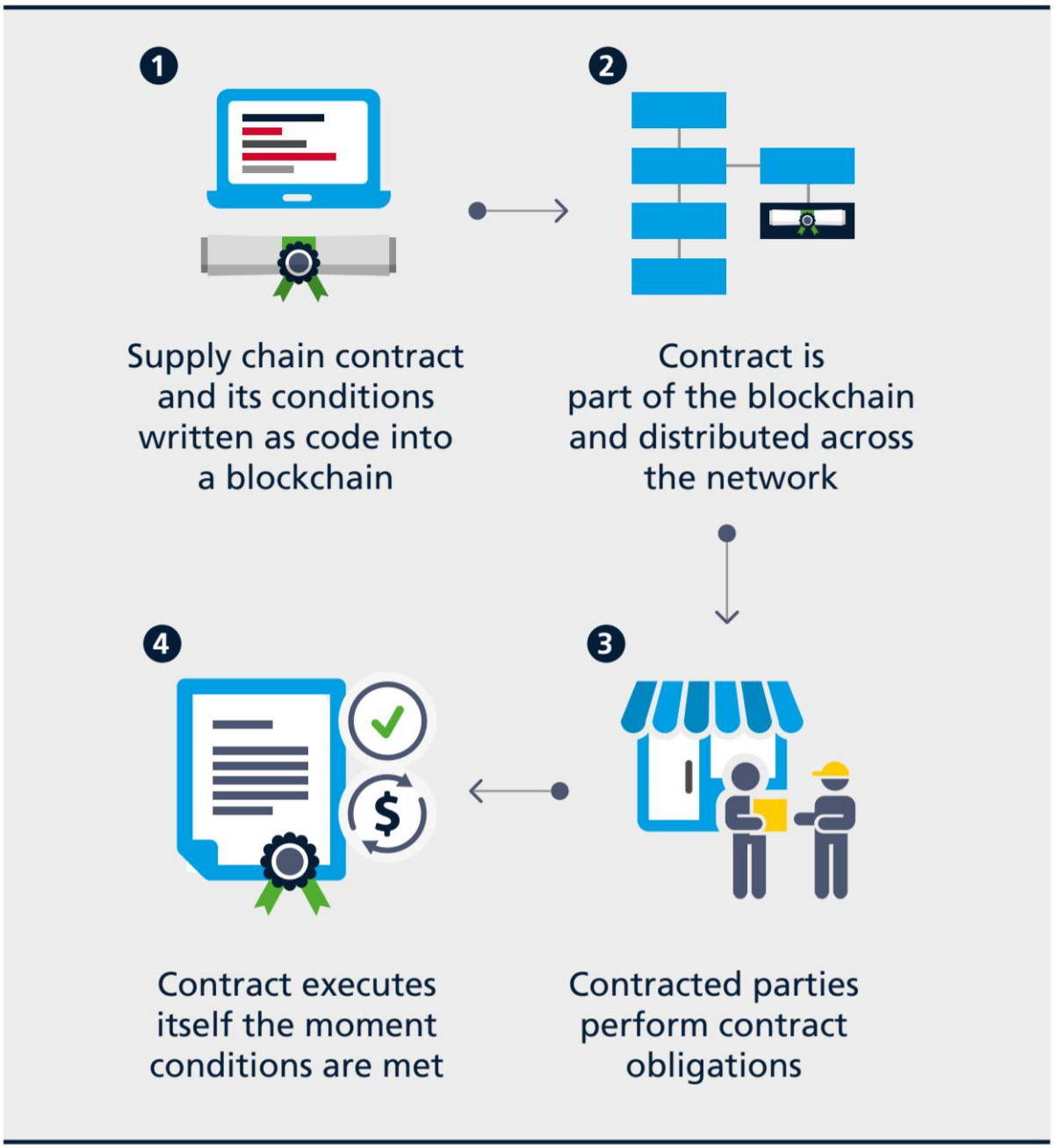


Figure 24: How smart contracts could work in the logistics industry (Source: DHL)

One of the first startups to pursue such smart contract applications in the logistics industry is ShipChain. ShipChain is an early-stage company which has designed a comprehensive blockchain-based system to track and trace a product from the moment it leaves the factory to final delivery at the customer's doorstep. The system is designed to encompass all methods of freight and there are plans to include an open API architecture that can integrate with existing freight management software. All relevant supply chain information is recorded in an immutable blockchainbased database that can execute smart contracts once the conditions have been met (for example, as soon as the driver transmits confirmation of successful delivery). A key element to automating the settlement process is through ShipChain's digital currency called SHIP tokens . Participants of ShipChain's platform purchase these tokens in order to pay for freight and settle transactions on the platform.

In this use case, blockchain in combination with the Internet of Things (IoT) in the logistics industry will enable even smarter logistics contracts in future. For example, on delivery a connected pallet will be able to automatically transmit confirmation and the time of delivery as well as the condition of the goods to the blockchain-based system. The system can then automatically verify the delivery, check whether the goods were delivered as per agreed conditions (e.g., temperature, humidity, tilt) and release correct payments to the appropriate parties, greatly increasing efficiency as well as integrity. Blockchain can further be used in the context of IoT to automate machine-to-machine payments (e.g., connected machines negotiating and executing price based on the logistics activities performed). Another example of smart contracts in the logistics industry is the digitization of letters of credit (L/C) in order to accelerate the preparation and execution of a standard paper-based L/C – a process which currently tends to take from a few days to a few weeks.

The Bank of **America Merrill Lynch (BofAML), HSBC** and the **Infocomm Development Authority of Singapore (IDA)** have developed a prototype to bring the paper-intensive L/C process onto a blockchain. The system essentially enables the sharing of information between exporters, importers and their respective banks on a secure blockchain-based platform. This allows trade deals to be executed automatically through a series of digital smart contracts. In the trial, each of the four parties involved in an L/C transaction could visualize data in real time on a mobile tablet and see the next actions to be performed. In a joint statement, the consortium partners state that the proof of concept shows potential to streamline the manual processing of import/export documentation, improve security by reducing errors, increase convenience for all parties through mobile interaction and make companies' working capital more predictable. The partners now plan to conduct further testing on the concept's commercial application with selected partners, such as companies and shippers.

Startups are also working in this space with one example being **Libelli**. This company is developing a solution to essentially act as an escrow agent between any seller and any buyer to create a smart contract, bypassing the need for buyers and sellers to engage banks and eliminating the paperwork traditionally associated with L/C. The company aims to provide transparency to all stakeholders during the process, and claims that the automation of this commercial process reduces L/C time-to-execution down to a few minutes, with costs ten times lower than currently charged by banks.21 Other functions that could be automated include outsourced transportation management, normative compliance, route planning, delivery scheduling, fleet management, freight forwarding, and connectivity with business partners.

Chapter 5 – Blockchain: A new model for Health Information Exchanges

Most global healthcare systems are broken. Healthcare provision must change and insurers, healthcare providers, governments, pharmaceutical companies, and patient support groups, must be prepared to respond and lead. We can use innovative, transformational technology to build a new and improved precision health ecosystem, combining accurate diagnosis and rule-based therapies. One of these is blockchain.

A blockchain powered health information exchange could unlock the true value of interoperability. Blockchain-based systems have the potential to reduce or eliminate the friction and costs of current intermediaries. Particularly compelling use cases for blockchain technology include the Precision Medicine Initiative, Patient Care and Outcomes Research (PCOR), and the Nationwide Interoperability Roadmap. For these and other high-potential areas, determining the viability of the business case for blockchain is paramount to realize the benefits of improved data integrity, decentralization and disintermediation of trust, and reduced transaction costs. The exchange of Personal Health Records and Health Information Exchange (HIE) data via the Integrating the Health care Enterprise (IHE) protocol is an important part of addressing the challenges of system interoperability and accessibility of medical records. The strategy outlined to date provides the technical requirements and specific incentives for health systems to meet the Meaningful Use interoperability standards necessary to support the envisioned National Health Information Network, buttressed by a network of HIEs operating on a broad scale. That unrealized scale, driven in large part by insufficient incentives outside of compliance, threatens the viability of HIEs and merits exploration of new models. It may be possible that new value-based models embedded in MACRA will be sufficient to make the market model work, but HIEs have been seeking alternative business models. Meanwhile the health systems that see true benefits from establishing a clinically integrated network in order to engage in risk-based contracts focus on private exchanges and are looking for low cost solutions that enable secure integration and support the assembly of virtual health systems that move beyond organizational boundaries. While blockchain technology is not a panacea for data standardization or system integration challenges, it does offer a promising new distributed framework to amplify and support integration of health care information across a range of uses and stakeholders. It addresses several existing pain points and enables a system that is more efficient, disintermediated, and secure.

HIE pain points	Blockchain opportunities
Establishing a trust network depends on the HIE as an intermediary to establish point-to-point sharing and book-keeping of what data was exchanged.	**Disintermediation of trust** likely would not require an HIE operator because all participants would have access to the distributed ledger to maintain a secure exchange without complex brokered trust.

Cost per transaction, given low transaction volumes, reduces the business case for central systems or new edge networks for participating groups.	**Reduced transaction costs** due to disintermediation, as well as near-real time processing, would make the system more efficient.
Master Patient Index (MPI) challenges arise from the need to synchronize multiple patient identifiers between systems while securing patient privacy.	**Distributed framework for patient digital identities**, which uses private and public identifiers secured through cryptography, creates a singular, more secure method of protecting patient identity.
Varying data standards reduce interoperability because records are not compatible between systems	**Shared data** enables near real-time updates across the network to all parties.
Limited access to population health data, as HIE is one of the few sources of integrated records.	**Distributed, secure access** to patient longitudinal health data across the distributed ledger.
Inconsistent rules and permissions inhibit the right health organization from accessing the right patient data at the right time.	**Smart contracts** create a consistent, rule-based method for accessing patient data that can be permissioned to selected health organizations.

5.1. Fixing healthcare: Measuring and responding to a need

To fix most of the global broken healthcare system, we must understand how to measure how our healthcare ecosystems perform. One of the most important factors to consider is how well countries are meeting the critical goal pf maximizing their population's mental and physical health. Most rankings include health infrastructures, availability of preventative care, and responsiveness to the population's expectations.

5.1.1. Measuring stakeholder responsiveness within healthcare

For our purposes, responsiveness refers to the interactions among various stakeholders within the healthcare ecosystem and reflects the client orientation in the delivery of healthcare services. A good healthcare system is affordable: it ensures that poor households are not paying a higher share of their discretionary expenditure on health than wealthier households, and that all people are protected against catastrophic financial losses related to a disease. Global organizations such as the London-based Legatum Institute, the Commonwealth Fund, or the World Health Organization (WHO) are among other scientific and government studies that publish the healthcare rankings annually, by country. Most studies show countries ranking high in prosperity also rank among the world's healthiest nations. However, there are exceptions. Among wealthy nations, the underachiever is the United States, which

tops the world in per capita healthcare expenditure by some measures. The United States performs exceptionally poorly on population health outcomes such as infant mortality and life expectancy. Insurance premiums and drug prices have skyrocketed, leaving US citizens struggling to access affordable care. In contrast, Switzerland, France, Netherlands, Sweden, Israel, Germany, and Norway are among the healthiest countries, as are the city-states of Luxembourg, Singapore, and Hong Kong.

5.2. Establishing trust among stakeholders

A patient-centered, population health-based system should be based on the principle of getting the right information to the patient and members of the patient's healthcare team and transmitting information at the right time in the decision-making process. Most systems fail to meet deadlines because health information systems comprised of insurance, medical, pharmaceutical, and social service organizations are incompatible and complex (Figure 25, next page). All of these entities need to share patient data to coordinate care successfully. This sharing raises technical, governance, and privacy concerns. When stakeholders seek to cooperate, they need to harmonize all systems so that they interact seamlessly. This task requires daunting changes for organizations in each sector. Trustworthiness is the crucial feature of blockchain technology. When transactions are executed and settled on a distributed ledger, all parties in the healthcare system need not trust each other; they can trust the ledger. Blockchain combines the openness of the Internet with the security of cryptography to give everyone a faster, safer way to verify key information, shifting the focus from making money for investors to keeping people healthy and curing disease. Unlike classical legacy systems and paper-based alternatives, blockchain is considered immutable, unhackable, and tamper-proof, reducing concerns around fraud by providing a digital fingerprint that ensures all parties are indeed who they say they are. One of the most significant opportunities for blockchain technology is to save costs and time by eliminating redundant intermediaries, those organizations that operate between institutions or people and link them together in the healthcare value chain. Some of these are very good for the system, such as group purchasing organizations (GPOs), which are buying groups that help reduce transaction costs by negotiating prices on behalf of multiple buyers, thus aggregating demand and leveraging buying power to obtain more favourable pricing for health plans, hospitals, and physician practices. Conversely, other healthcare intermediaries use exclusionary practices and anticompetitive agreements, which can be detrimental to competition and consumers in the healthcare supply chain. When these intermediaries constrain competition, they affect many stakeholders such as smaller distributors, independent pharmacies, and smaller manufacturers of pharmaceuticals, medical devices, and medical supplies. In most of these cases, the intermediaries' incentives do not include promoting social good and, therefore, add no value to the process. We have two ways to address this problem: (1) we could vote for legislators who would step in and address these twisted incentives, but that rarely happens against powerful corporate lobbyists, or (2) we could remove the need for these intermediaries altogether.

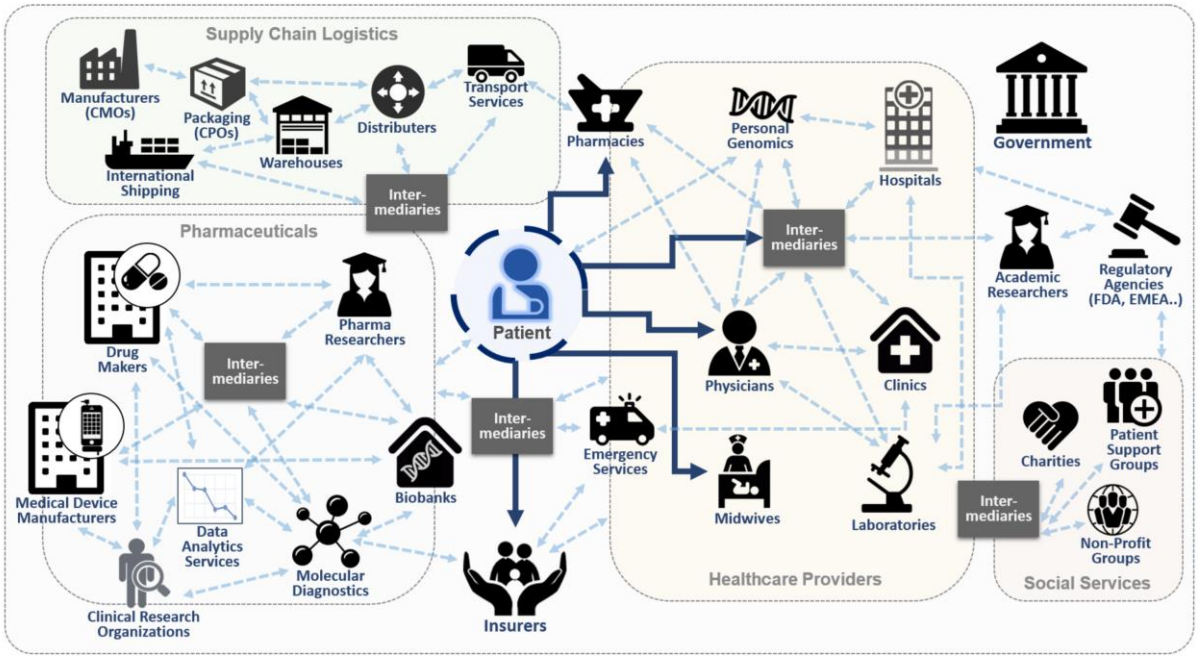


Figure 25: Value-added chain of the healthcare system (Source: BCRI)

Most healthcare systems are tremendously complex because of extreme heterogeneity in their data, processes, and platforms, with patients and healthcare providers separated by jurisdictions and multiple intermediaries. With blockchain, we could put patients at the center of their care, where every element would align with their needs and keep them healthy. To ensure alignment, participants would store all health data (e.g., lab values, health status and risks, genetics, insurance, imaging, prescriptions) about a patient on a blockchain, and the patient in consultation with a primary care provider could determine who had access to these data.

Because blockchains are decentralized and immutable, counterparties can independently transact and verify the data on a ledger without requiring costly third parties to perform similar tasks. Blockchain will not be the demise of intermediaries; however, it will remove those that add no value. The process of disintermediation requires careful planning.

5.3. Addressing roadblocks to reinventing healthcare

Introducing blockchain to our healthcare systems is technically feasible but we have important roadblocks to overcome. As many blockchain innovators are discovering, institutional inertia—comfort with the status quo—is extraordinarily powerful. Many corporate departments and healthcare providers will not give up control of their hierarchical systems and move to peer-to-peer structures. Moreover, most organizations are not prepared for disruptive technology; they are more comfortable with incremental change. Finally, many stakeholders await a strong business case for blockchain adoption—after all, their centralized systems seem to be performing well— whereas many of the new entrants in the blockchain/healthcare market are still working on proofs of concepts, not full-blown business applications. Hospitals, healthcare practices, and insurers have all invested heavily in these database

systems and are reluctant to dispense with these systems without understanding the costs of implementing and the impact of integrating blockchain solutions into everyone's job in the healthcare space.

To overcome resistance, leaders should identify the root causes such as lack of awareness of the benefits, the organization's poor response to previous change initiatives, management's lack of visible support and commitment, and employee fear of job loss.

Not all healthcare ecosystems are interested in adopting cheaper, more transparent systems, especially in environments where healthcare is primarily a business and not a service for the greater good. For example, in the United States, executives who run hospitals have MBAs, not MDs. Their goal is to maximize their revenue. From the hospital executives' perspective, every step that a patient takes within the hospital system affects the hospital's bottom line. A 2016 survey of 11 countries by the Commonwealth Fund found that US citizens were far more likely to go without care because it was too expensive. One third of US adults went without recommended care, did not see a doctor when sick, or failed to fill a prescription because of costs.

There's no incentive for a health industry that is so profitable to innovate. Consumers have no choice but to buy essential services at incredibly high prices. Introducing transparency, empowering patients, and improving healthcare provider responsiveness could help: with actual data about costs relative to prices, healthcare consumers are better positioned to demand change. The challenge for developers is ensuring that those who need the information have ready and safe access. As such, virtually every healthcare stakeholder will need to reengineer its business model.

5.4. Deciding when to implement blockchain technology

Most healthcare systems are undergoing a dramatic transformation. Factors such as the emergence of genomics, precision medicine, big data, artificial intelligence, value-based care, increased regulatory oversight, aging populations, and heightened consumer awareness all contribute to complexity, disorganization, and discontinuity of patient care. To ensure patient safety and quality of care while realizing savings, most stakeholders have to build new relationships and must reinvent themselves. Many healthcare stakeholders are just beginning to understand the merits of exploring blockchain, and it is a new concept for the precision medicine ecosystem.

Blockchain offers economic scalability: early adopters can start small. If the organization is profitable and the owners can scale up, the core business prototype can take advantage of all the benefits blockchain offers. Blockchain also has the potential to connect fragmented healthcare systems, generate new insights, and assess the value of care. With many companies already pushing aggressively into this new space, waiting too long might prove disadvantageous. According to Gartner,

Blockchain is still—and will be for the next five to ten years—an innovation trigger, before reaching the peak of inflated expectations.

Some are still cautious. Blockchain data start-up, Tierion, argued that blockchain presents more pitfalls than promises at this early stage. However, its leadership is optimistic about the long-term impact of blockchain. Indeed, the company moved into the healthcare space, joining the Philips Blockchain Lab

to explore uses of blockchain technology in healthcare. Forrester advised enterprise CIOs to wait five to ten years before introducing blockchain, in part because of legal restrictions. Why wait so long? When applying game theory— for example, seeing an innovative approach, but being too afraid to consider implementing it because no one else has tried it—we get the opposite of what a thought leader and innovator should do to advance transformation.

For health care organizations that have decided to initiate blockchain projects, the next step is to design the use cases. There are two primary use cases to consider: (1) verify and authenticate information, or (2) transfer value.

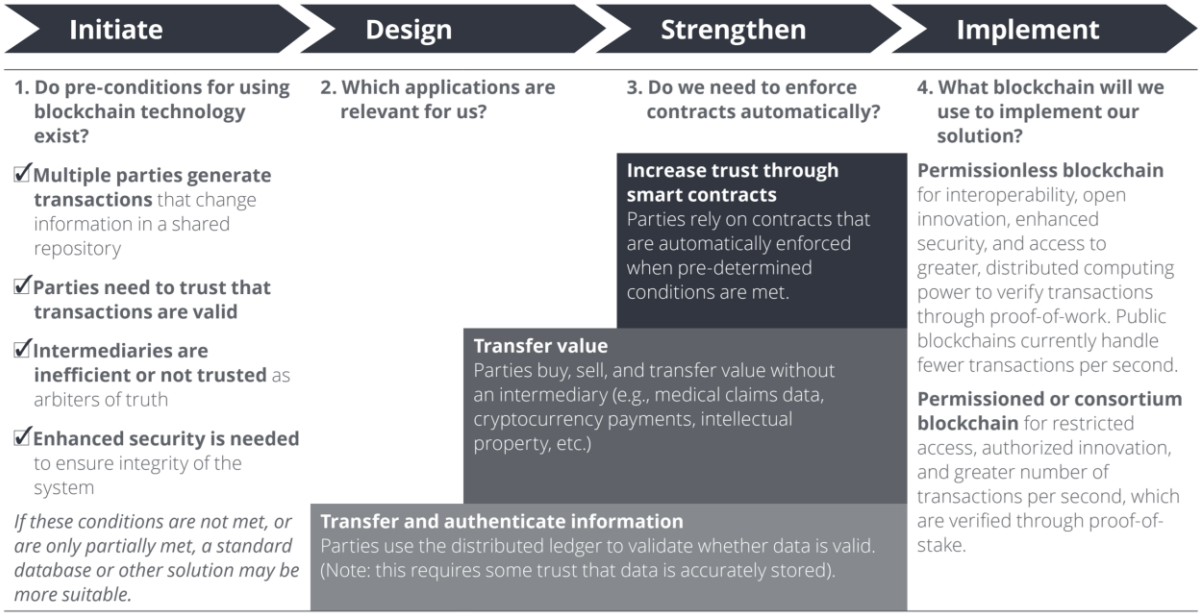


Figure 26: Blockchain Decision Framework (Source: Deloitte)

In the first use, organizations may consider blockchain technology to verify a patient's digital identity, genetics data, or prescriptions history. Prescrypt, a proof-of-concept developed by Deloitte Netherlands, in collaboration with SNS Bank and Radboud3, gives patients complete ownership of their medical records, allowing them to grant and revoke provider access to their data. Providers, in turn, can issue prescriptions on the blockchain. In the second application, organizations can use the technology to transfer value, such as cryptocurrencies or intellectual property rights. Deloitte, in collaboration with Loyyal, developed a prototype that incentivizes desired behaviors using gamification and behavioral economics principles. In the future, health ecosystems may emerge where providers, plans, or fitness centers co-develop programs to incentivize and reward patients for healthy behaviors. In the third stage of the blockchain framework decision making process, organizations have an opportunity to strengthen the system through smart contracts that automatically execute when conditions are met. This application is increasingly sophisticated, using algorithms to fully customize conditions that determine when to exchange value, transfer information, or trigger events. This serves as the foundation for more sophisticated applications of blockchain technology in health care, including prior-authorizations and auto-claims processing. Finally, to implement a blockchain solution, organizations may choose to use a permissionless blockchain, such as the Bitcoin blockchain, or a permissioned blockchain that restricts

access to a pre-determined group. Consortia such as R3 in the financial services industry are experimenting with permissioned blockchains, and R3 has recently completed a successful transfer of commercial paper between banks4. Implementation also requires selection of a blockchain protocol—the underlying blockchain technology and framework that guides the structure of the blockchain and development of applications. Platforms such as Ethereum provide the ability to create decentralized applications built on top of blockchain architecture; it is a leading blockchain protocol for both permissioned and permissionless blockchain development. Additionally, Hyperledger is an open source project created by the Linux Foundation seeking to create a platform for corporate based blockchain platforms and other standards. The choice of blockchain protocol is important, because it will influence the range of possible applications and the number of users participating on the network. While blockchain may have significant potential to improve data interoperability, security, and privacy, it is important to note the boundaries of the technology. Blockchain is not a substitute for an enterprise database. Blockchain powered solutions are not optimized for high volume data that needs absolute privacy and instantaneous access within a single organization. Blockchain solutions are designed to record specific transactional data events that are meant to be shared across a network of parties where transparency and collaboration are mission critical. The Blockchain Framework highlights these preconditions. In the health care landscape, blockchain technology has transformative potential. Nationwide health information interoperability could be realized through a consortium blockchain, which can leverage a leading protocol and create a standardized transaction layer for all organizations. Blockchain technology has the potential to advance strategic goals and investments to standardize health care information by establishing a transaction layer on which all stakeholders can securely collaborate. Organizations considering blockchain technology may find the aforementioned framework useful as a guidepost and a part of an iterative decision process; however, it is not intended to be an exhaustive, prescriptive list. The four steps outlined above are intended as a forcing mechanism to apply disciplined consideration of requirements, limitations, and alternatives before launching costly and time-consuming experiments.

5.5.1. Early steps toward implementation

The healthcare industry consists of many different areas in which blockchain solutions would be beneficial; however, each has different dynamics. Investors in the healthcare sector factor in many variables, including trends in demographics, reimbursement, and regional regulation. According to Venture Scanner, funding is going where there is a high need for innovation and a good chance of short-term returns of investment such as :

- Precision medicine ecosystems (or personalized medicine)
- Health insurance and payment
- Disease-specific genetic testing
- Cost-efficient analytic solutions for healthcare providers
- Personalized consumer reports

- Online health destinations such as health insurance marketplaces and platforms to manage and automate health benefits, websites that provide symptom checklists, drug information, and health resources
- IoT fitness and wellness solutions such as wearables that track personal fitness stats, monitor heart rate, and sports-specific data collection

To reinvent and reform healthcare, we must focus on the need first. The healthcare industry will likely accept products and services that support the transition toward a value-driven reimbursement model on national, regional, and local levels because all stakeholders understand their importance. Governments drive other critical areas such as electronic medical records (EMR) and population health management, and so progress can be slow. The government gains little for taking risks on programs and achieving program goals but faces substantial criticism and potentially personal loss for failure.

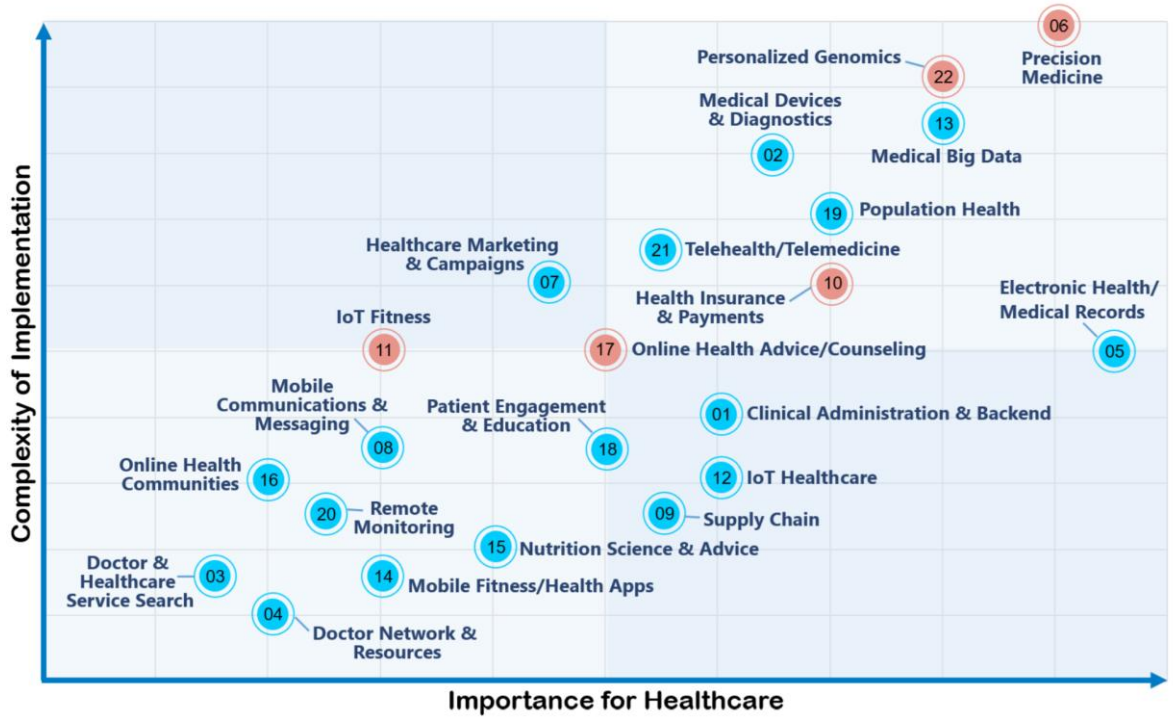


Figure 27: Areas of healthcare in dire need of reform (Source: BCRI)

Many sectors of the healthcare ecosystem can benefit from blockchain technology. However, not all are equally easy to implement (points represent a rough estimate based on communication with healthcare providers). To fix a healthcare system with blockchain technology, we must identify areas where system complexities inhibit progress and where we can develop and implement solutions quickly. The red circles denote those areas with the largest flow of venture capital, according to Venture Scanner.

1: Scheduling, patient transfers, billing, compliance; 2: monitoring, detection equipment; 3: services to search for doctors, healthcare plans, and specialized healthcare; 4: collaboration platform across hospitals, and social networks that identify and share best practices; 5: platforms for electronic medical charts, schedules, prescription tracking, and referral letters; 6: genetic, metabolomics, and epigenetic

testing, analytic solutions, patient personalized reports; 7: healthcare-specific customer relationship management platforms; 8: secure messaging for doctors, data sharing amongst healthcare professionals; 9: cold chain logistics, biobanking, drug shipping; 10: health insurance marketplaces, and platforms to manage and automate health benefits; 11: healthy eating trackers, exercise tracking wristbands, smartphone-controlled devices; 12: glucose monitors, sleep trackers, pain relief wearables; 13: data management, solutions to normalize and link data across different systems, predictive analytics; 14: fitness apps, mindfulness exercises; 15: nutrition information, nutraceuticals, lifestyle plans; 16: online communities that connect patients, and doctors, generalized medical information; 17: symptom checklists, drug information, and resources on specific issues; 18: in-hospital multimedia systems, clinical trial recruiting, patient relationship management; 19: population data management, coordinated care across populations; 20: services that provide caregivers to senior citizens, alert systems for in-home care; 21: patients to doctor video conferencing, remote monitoring, remote diagnosis; 22: pharmacogenomics, direct to customer genomics, ancestry.

Probably the most accessible markets to conquer fall in the lower right quadrant of Figure 27, clinical administration (e.g., for billing and patient transfer), Internet of Things (IoT) in healthcare (e.g., connected devices such as glucose monitors), and pharmaceutical supply chain (particularly cold chain logistics and drug shipping). The greater the complexity of a project, the greater the effort and the need for collaboration. All entrants into those fields must evaluate the maturity of each potential market to gain insights into strengths, weaknesses, and barriers for a value-based reimbursement model, considering the interoperability aspect.

5.5.2. The healthcare ecosystem supply chain

The healthcare supply chain was the first to consider using blockchain technology to address a range of ailments from counterfeit goods to disputes over ownership. As an industry, the global supply chain is worth over $40 trillion per year, and there are seemingly infinite international laws and regulations governing each step. Many processes are still based on paper transactions, such as bills of lading (detailing merchandise shipment and ownership) and letters of credit (used by banks to guarantee that buyers receive their payments), with auditors or middlemen at each step to add delays, complexity, and cost. To address these inefficiencies and add trust and visibility into the flow of goods and commerce, several companies are beginning to use blockchain technology. While a few specialized start-ups such as ascribe and Everledger use the blockchain to track single product types, including digital artwork and diamonds respectively, other companies aim to track any product throughout every part of its lifecycle. In these cases, blockchain will create an entirely decentralized network that connects all producers, carriers, banks, traders and other parties of the international trading supply chain. Using decentralized technologies, all communication between these parties will be direct and not pass through a specific central entity or middleman. However, the market for blockchain solutions is already crowded, with some start-ups as well as industry giants such as Walmart, IBM, Microsoft, and SAP launching efforts to better track the movement of goods and information.

Blockchain service providers in supply chain logistics

Catkin, www.catkin.eu

Chronicled, chronicled.com

CargoChain, cargochain.com

Guardtime, guardtime.com

IOTA, iota.org

iSolve, iSolve.com

modum, modum.io

Mojix, www.mojix.com

OTdocs, otdocs.com

Provenance, www.provenance.org

Skuchain, www.skuchain.com

Stratumn, stratumn.com

Synthium Health, www.synthiumhealth.com

The LinkLab, www.thelinklab.com

Blockchain is particularly effective with cold chain logistics and pharmaceutical serialization, especially when combined with smart contracts. This process ensures that contractual rights and obligations, including the terms of payment and delivery of goods and services, are executed automatically by an autonomous system.

5.5.3. The pharmaceutical supply chain: Risks and challenges

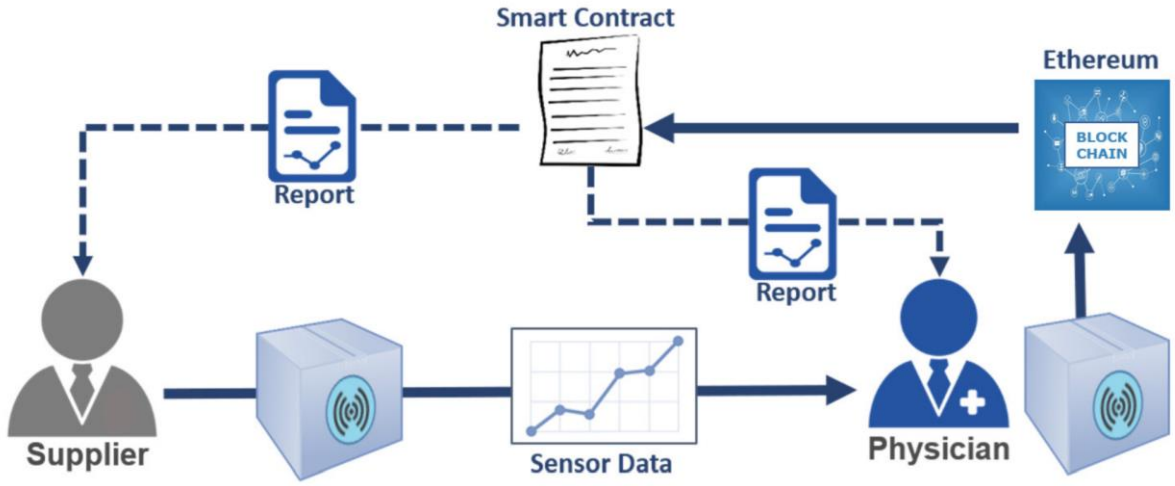
Until now, pharmaceutical companies that have benefitted from the old healthcare ecosystem, which brought enormous profits; therefore, they had few incentives to change. As a result, they had grown unresponsive to consumers who, in turn, resented them. Some companies, however, have realized that the business model had to change. Early adopters, Pfizer and Genentech, formed the MediLedger Project, a network that uses blockchain to control pharmaceutical supply chains. The pharmaceutical supply chain is defined as the management of product supply from raw material sourcing to active pharmaceutical ingredient, manufacturing through formulation, packaging, and distribution to the patient. Traceability of supplies throughout an international process is challenging. Under current systems, drug shipments pass through many hands and involve paperwork that people can tamper with. Using distributed ledgers can improve revenue sharing, solve patent issues, trace transfer of assets, and enable proof of work or proof of service.

For example, if stakeholders in the blockchain could chart the pharmaceutical supply chain from a batch number and factory of origin all the way to distributor, sale and storage, and adherence, then they could identify issues with greater granularity and speed. If regulators or payers identify a hotspot of

patients who have a specific problem with a drug, they could trace the problem back to the batch or administration of drug regimens. Pharmaceutical companies must comply with the guidelines and regulations:

- The European Commission's Good Distribution Practice of Medicinal Products for Human Use requires companies to report any deviations, such as cold chain disruptions, humidity, or light conditions to the distributor and the recipient of the affected medicinal products. Companies must adhere to recent changes.
- The US Drug Supply Chain Security Act (DSCSA) outlines steps to build an electronic, interoperable system for identifying and tracing certain prescription drugs during distribution across the United States. This traceability enhances FDA's ability to protect consumers from drugs that might be counterfeit, stolen, contaminated, or otherwise harmful.

A Swiss start-up, Modum, is working on supply chain solutions with its first use case in cold-chain logistics. The company combines sensor devices and blockchain technology to provide data integrity for pharmaceutical logistics under new regulations. Modum's team is developing a blockchain-based temperature tracking system for medicinal products so that distributors can fulfil new requirements for an auditable record of temperatures of products in transit. Users can activate a fully programmable sensor and connect it to a shipment. Upon the shipment's arrival at its destination, sensor data are automatically transferred to the Ethereum blockchain, triggering smart contracts that compare these data against the regulatory or customer requirements. Then the shipment is either released or, if a deviation is detected, then both the sender and the receiver are notified (Figure 28). Modum can apply its technology to any product in transit or throughout the entire supply chain where data collection is required and its integrity is crucial. What good is a blockchain solution if only one link in the pharmaceutical supply chain is using it or if only one pharmaceutical giant adopts it? Chronicled, a San Francisco-based company, is producing blockchain systems for these companies. It is crucial to bring together industry partners to design and develop pilots of potential solutions that can meet the GDP and DSCSA legislation, fulfil companies' needs worldwide, and eliminate counterfeit production and distribution. Drug counterfeiting is a widespread problem for pharmaceutical businesses and consumers.



Modum sensors constantly record environmental conditions on batches of drugs in transport. When the shipment is at its destination and goods change ownership, the collected data is checked against the specific smart contract in the Ethereum blockchain. The contract validates that the transaction meets all the standards set forth by the customer (e.g., no temperature deviations), the customer's clients, or the regulator, and then triggers various actions: notifications to sender and receiver, payment, release of goods, or insurance clauses in case of damaged goods.

Figure 28: Modum's blockchain solution for cold-chain logistics (Source:Modum)

The WHO estimates that up to 10 percent of drugs sold around the world are counterfeit; this might be as high as 50 percent in some countries.10 Many of these drugs might not contain any active ingredients while others contain incorrect quantities of necessary ingredients. If patients take counterfeit drugs, they might experience severe allergic reactions, unexpected side effects, or a worsening of their medical condition, sometimes leading to death. In 2013, over 8,000 patients died over a five-year period in a remote Himalayan hospital because an antibiotic had no active ingredients. Economic incentives might be spurring the growth in counterfeiting. Also, the ability to sell drugs directly to consumers through purchases over the Internet adds to the problem. Traditionally, to tackle these issues, many countries have implemented pharmaceutical serialization practices, such as recording, authenticating, maintaining, and sharing accurate records of items before dispatch using track and trace technology. However, these programs and regulation depend heavily on local, national laws and standards, and many pharmaceutical companies struggle to identify the best approach to work with serialization.

5.5.4. Blockchain solutions to the pharmaceutical supply chain

The BlockRx Project offers a solution to encourage stakeholder buyin: invite all stakeholders to participate in a blockchain. This includes series of initiatives by iSolve to verify and enhance the integrity of the drug supply chain and to accelerate new drug development by leveraging the blockchain to support and manage the drug development lifecycle. The idea behind BlockRx is initiating a tracking process that could start with a central authority. For example:

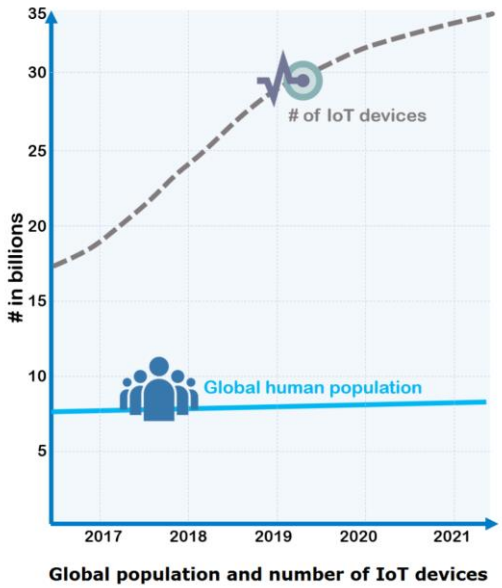
- A pharmaceutical company that owns the drug IP decides on the participants in its blockchain, such as suppliers, warehouses, quality controls, distributors, and retailers.
- Once a drug ingredient is manufactured, a notification is broadcast on the blockchain network, and a hash is generated with all the relevant manufacturing details.
- The hash is printed on the drug package.
- The drug is delivered to the assigned distributor.
- The delivery is registered as a transaction: a new hash is generated and linked to the previous hash, containing further information about the shipment, cold chain control, or distributor details.
- Once the distributor ships to the retailer, the same process continues and the blockchain grows.
- Finally, the consumer who buys the drugs at the pharmacy or via the Internet receives the public key on the invoice, which allows the consumer to verify that the medication originated from an authentic manufacturer and hasn't been opened or adulterated.

This process should also work across borders, helping countries work together to share detection technologies, collaborate on a universal database of legitimate pharmaceuticals, and pass international standards. There are other opportunities to connect blockchain technology with measures to counteract the increase in fake drugs on the market, including stronger state licensure supervision of drug suppliers and the use of radio frequency identification devices (RFID) to identify original drugs accurately. Whatever approach companies take, the pharmaceutical industry will spend fewer resources on anticounterfeiting workarounds and regulatory compliance. The US Center for Supply Chain Studies started a blockchain study bringing together members of the pharmaceutical supply chain, technology companies, and standards and government agencies to explore blockchain's potential in the DSCSA space. The center was established in 2015 as a neutral, nonprofit industry exploration and education forum. Several blockchain projects are planned and interested parties can still join. Early results from one project indicate that blockchain holds promise in providing a single platform for trading partners to connect system; blockchain could be the missing ingredient in the interoperable system. The study defines a preliminary solution model that demonstrates a standard set of commands for solutions to interact with the blockchain on behalf of a manufacturer's supply chain customers. This enables large-scale supply chain interoperability and provides a stable market in which solutions can compete and collaborate.

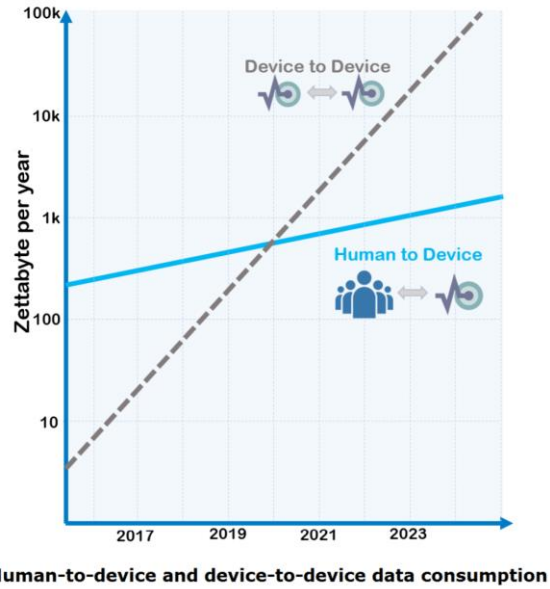
5.5.5. Internet of Things healthcare

Blockchain can make a considerable impact where sensitive data and/or high volumes of data need to be transferred securely and privately. That's precisely what the Internet of Things (IoT) needs to do. IoT refers to using electronic devices for capturing or monitoring data, connecting to a private or public cloud, then automatically triggering certain events. IoT has many healthcare applications, from remote monitoring (e.g., fetal monitors), to smart sensors (e.g., temperature monitors or blood glucose level sensors) and medical device integration (e.g., artificial cardiac pacemakers or neural stimulators). The growth of IoT technologies in healthcare will be driven by such factors as the steep rise in the global

aging population due to longer life expectancies, the increased demand for health and fitness monitoring solutions, and the prevalence of lifestyle diseases such as diabetes and obesity. IoT can now accurately analyze a patient's health, identify inefficiencies, and develop patient-specific care plans. Nevertheless, barriers to adopting wearables in the healthcare sector exist because of concerns surrounding privacy. Most mobility approaches currently do not provide solutions that simultaneously fulfill security needs while enabling mobile access, without causing privacy and usability concerns with end users. Blockchain could support IoT applications by facilitating transaction processing and coordination among interacting devices and downstream analytical processes. For example, blockchain can make it easier to synthesize data from IoT devices for chronic disease management, remote monitoring, or patient-provider communication, enabling fee-for value systems. Large information and communications technology companies dominate the IoT market because of its complexity. Such tech giants as Microsoft, Cisco, and IBM control the IoT software and services segment for healthcare, and Apple, Huawei, Siemens, Google, and Samsung are investing significant resources into developing devices that will help bridge the gap between personal fitness tracking and professional healthcare. Adopting blockchain solutions in the IoT space can have a significant competitive advantage, for a market that is expected to explode. If we review projections from the leading consulting firms we can see that gaining market share with blockchain technology can matter enormously. Bain predicts that by 2020 annual revenues in global IoT market could exceed $470 billion for the IoT vendors selling the hardware, software, and comprehensive solutions. BI Intelligence anticipates that the global market for IoT healthcare tech alone will top $400 billion in 2022, while Gartner predicts over 20 billion connected devices will be in use worldwide in 2020.



Global population and number of IoT devices



Human-to-device and device-to-device data consumption

Adapted from World Population forecast (Census.gov), International Data Corporation IoT forecast (idc.com)

The adoption of small medical devices and IoT applications will produce an unprecedented amount of health data consuming a huge amount of storage space. A zettabyte is a measure of storage capacity two to the 70th power or 1021 bytes.

Figure 29: How the relationships among people and machines will change

With such a vast market, new entrants from the blockchain space are choosing to join existing IoT ecosystems and defining a clear value proposition such as improving the utility of wearables. While adoption levels are rising, the wearables market is driven mainly by consumers who want to quantify personal health metrics. A blockchain could collect information from these mobile applications and through sensors in fitness trackers and other wearables and integrate it through representational state transfer (REST) application programming interfaces (APIs). RESTful APIs, which are quickly gaining traction in healthcare Bio-IT, are methods of allowing communication between a web-based client and a server through such standards as HTTP, URI, JSON, and XML.

FHIR (pronounced fire), for fast healthcare interoperability resources, is increasingly supporting interoperability of systems. Created by Health Level Seven International (HL7), a healthcare standards organization, FHIR is a draft standard describing data formats, elements, and an API for exchanging EHRs. The standard facilitates interoperation among legacy healthcare systems so that healthcare providers can share information on such devices as computers, tablets, and smartphones.

5.5.6. Clinical administration

Clinical administration management is the third area where implementation of blockchain is straightforward and solutions can be developed and put in place relatively quickly. A blockchain based payment process system can improve the efficiency of the hospital revenue cycle, in part, by eliminating the need for intermediaries between hospitals, physicians, insurers, and patients, according to Deloitte. One use might involve enabling patients or insurers to deposit a payment, which would not be released until a predetermined clinical outcome is reached. Also, for hospitals, a blockchain-enabled health information exchange would alleviate security concerns related to data sharing among different providers. Patients would be able to access and share their data and providers would be able to update relevant information with using individual keys. In September 2017, Black Book Market Research, a full-service healthcare-centric market research and public opinion research company, conducted a survey of 88 healthcare payers and 126 healthcare provider technology executives, managers and IT specialists to deliver comprehensive insights of current and planned enterprise deployment of blockchain solutions. The results demonstrate that the healthcare sector identifies the value in blockchain, but the lack of technical standards for a still-immature technology is causing regulatory uncertainty. For many people working in the healthcare space, the concept of blockchain is complex. However, the Black Book study found that understanding the healthcare blockchain has developed dramatically, with 29 percent of hospital leaders and 82 percent of health insurance executives having a general knowledge of the technology.

Actual breaches and cybersecurity events have boosted readiness significantly, and executive blockchain education has evolved from blockchain 101 to selecting the appropriate healthcare

blockchain technology protocols. Sixty-eight percent of payers expected blockchain to be integrated into their systems by the end of 2018, but only 12 percent of provider health organizations and systems have firm plans to implement by then. According to the study, the slow adoption of the technology in hospitals is mainly due to the undetermined cost of such solutions, which makes healthcare providers cautious to set a timeframe or deadline for potential deployment. Black Book respondents who were either deploying or considering implementing blockchain, ranked blockchain companies on their impressions of presentations and offerings to date. Of the vendors named, eleven companies received significant awareness.

Best known blockchain vendors in the healthcare space

BurstIQ, www.burstiq.com

Blockchain Health, blockchainhealth.co

Bloq, bloq.com

Gem, gem.co

Guardtime, guardtime.com

Hashed Health, hashedhealth.com

HealthCombix, www.healthcombix.com

IBM Blockchain, www.ibm.com/blockchain

PokitDok, pokitdok.com

Tierion, tierion.com

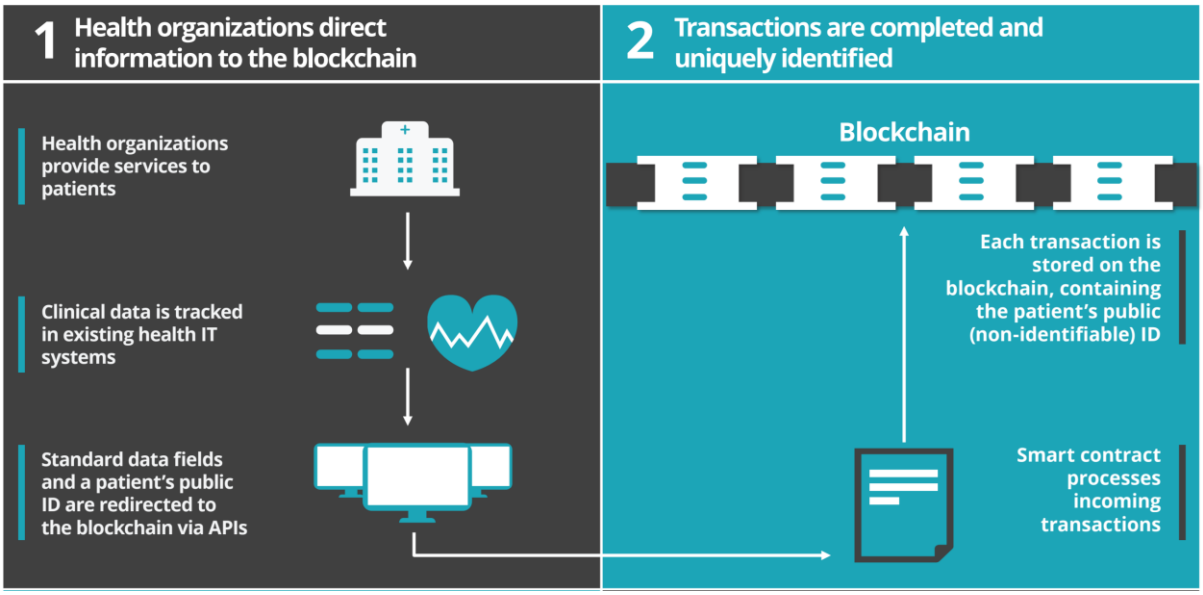
YouBase, www.youbase.io

The healthcare industry has been full of disruptions in the last decade, ranging from the explosive growth of medical devices within the Internet of Things to genome editing, and incredible advances in machine learning that could reshape diagnostic medicine. Blockchain might be the next disruptor, addressing industry's biggest challenges, patient data, especially the proverbial holy grail of the medical industry, the elusive EHR.

5.5. Blockchain as an enabler of nationwide interoperability

The Office of the National Coordinator for Health Information Technology issued a Shared Nationwide Interoperability Roadmap, which defines critical Policy and Technical Components needed for nationwide interoperability, including (1) Ubiquitous, Secure Network Infrastructure, (2) Verifiable Identity and Authentication of All Participants, (3) Consistent Representation of Authorization to Access Electronic Health Information, and several other requirements. However, current technologies do not fully address these requirements, because they face limitations related to security, privacy, and full ecosystem interoperability. The current state of health care records is disjointed and stove-piped due to a lack of common architectures and standards that would allow the safe transfer of sensitive information among stakeholders in the system. Health care providers track and update a patient's

common clinical data set each time a medical service is provided. This information includes standard data, such as the patient's gender and date of birth, as well as unique information pursuant to the specific service provided, such as the procedure performed, care plan, and other notes. Traditionally, this information is tracked in a database within a singular organization or within a defined network of health care stakeholders. This flow of information originating from the patient through the health care organization each time a service is performed does not need to stop at the individual organizational level. Instead, health care organizations could take one more step and direct a standardized set of information present in each patient interaction to a nationwide blockchain transaction layer. The surface information on this transaction layer would contain information that is not Protected Health Information (PHI) or Personally Identifiable Information (PII); rather, select and non-personally identifiable demographics and services rendered information could enable health care organizations and research institutions access to an expansive and data-rich information set. Information stored on the blockchain could be universally available to a specific individual through the blockchain private key mechanisms, enabling patients to share their information with health care organizations much more seamlessly. This deployment of a transaction layer on the blockchain can help accomplish ONC HIT's interoperability goals while creating a trustless, and collaborative ecosystem of information sharing to enable new insights to improve the efficiency of the nation's health care system and health of its citizens.



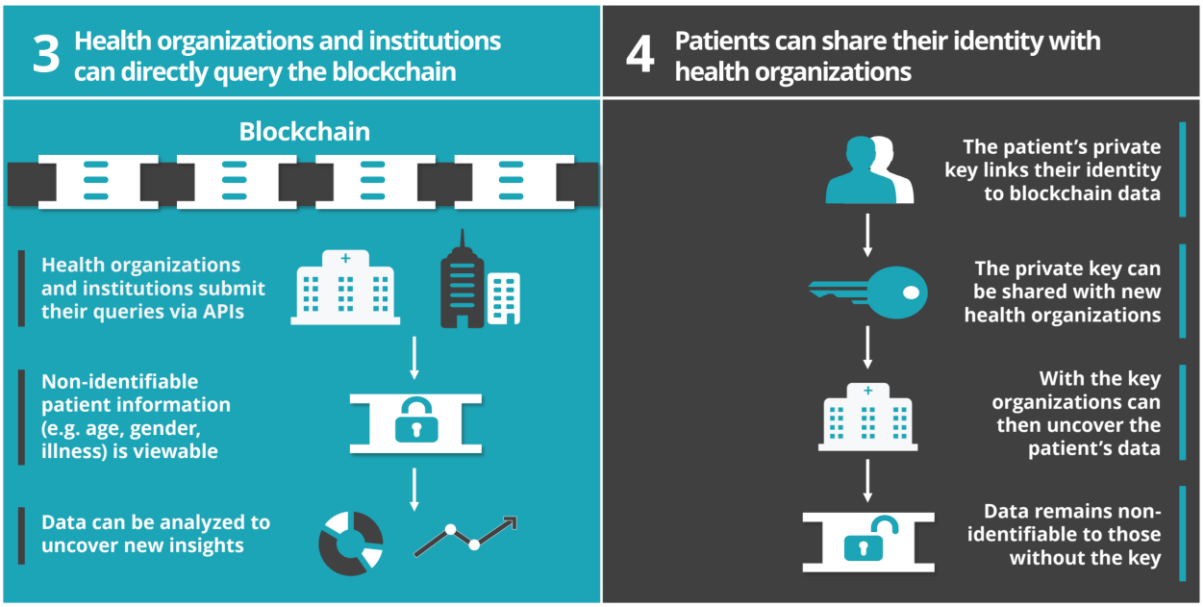


Figure 30: Illustrative Healthcare Blockchain Ecosystem

5.5.1. Toward blockchain interoperability

As a transaction layer, the blockchain can store two types of information: (1) On-chain data that is directly stored on the blockchain or (2) Off-chain data with links stored on the blockchain that act as pointers to information stored in separate, traditional databases. Storing medical information directly on the blockchain ensures that the information is fully secured by the blockchain's properties and is immediately viewable to those permissioned to access the chain; at the same time, storing large data files slows block processing speeds and presents potential challenges to scaling the system. In contrast, encrypted links are minimal in size and are activated once a user with the correct private key accesses the block and follows the encrypted link to a separate location containing the information.

	On chain data	**Off chain data**
Data types	Standardized data fields containing summary information in text form (e.g. age, gender)	Expansive medical details (e.g. notes) and abstract data types (e.g. MRI images, human genome)
Pros	Data is immediately visible and ingestible to all connected organizations, making blockchain the single source of truth	Storage of any format and size of data
Cons	Constrained in the type and size of data that can be stored	- Data is not immediately visible or ingestible, requiring access to each health care organization's source system for each record

		- Requires Off-Chain micro-services and additional integration layers - Potential for information decay on the blockchain

As an example, the blockchain cannot directly store abstract data types such as x-ray or MRI images: this type of data would require links to a separate location. Organizations considering how data should be stored should therefore carefully evaluate both technical and confidentiality constraints. Creating interoperability requires frictionless submission and access to view data. As such, the blockchain could serve as a transaction layer for organizations to submit and share data using one secure system. This will be most effective if a specific set of standardized data were to be stored directly on the blockchain for immediate, permissioned access, supplemented by off-chain data links when necessary. A standardized data set could include information such as demographics (gender, date of birth, other data), medical history (immunizations, procedures), and services rendered (vital signs, services performed, and other data). As the field matures, further evaluation and guidance will be needed to determine where and how each data type should be stored. Once a standardized set of health care information is established, the specific data fields can be created in a smart contract to employ rules for processing and storing information on the blockchain, as well as stipulating required approvals prior to blockchain storage. Each time a patient interaction occurs, health care organizations will pass information to the smart contract —where the parameters of the contract will verify that valid information has been submitted. As an example, the smart contract can stipulate that all fields need to be provided prior to blockchain storage or that a specific field must contain a particular data type (e.g. numerical) to be valid. Once the smart contract validates that the correct data fields have been submitted, it will direct the transaction to the blockchain for storage.

5.5.2. Interoperability and electronic health records

EHRs are at the core of all data flows. Consequently, they have been a topic of heated discussions in the healthcare industry for over a decade. Conceptually, EHRs are relatively simple and should not be difficult to design. Each record should contain the patient's consolidated medical history, including all key administrative and clinical data relevant to that person's care under a particular provider, including demographics, progress notes, medications, pharmacogenetic data, vital signs, immunizations, laboratory data, genomic data, and radiology reports. However, managing EHRs becomes challenging when the information comes from a variety of sources—providers, insurers, laboratories, and hospitals, each with its own patient records system and a reluctance to share information. As a result, data ownership becomes unclear; and regulations on access, control, and sharing of the information become complicated. Several large US companies failed to develop consolidated and widely accepted EHR systems, including Google Health, the Microsoft HealthVault, the Veterans Information System and Technology Architecture (VISTA).

5.5.3. Challenges to EHRs and data interoperability

For a healthcare system to be responsive, it must be interoperable. In healthcare, interoperability is the ability of different information technology systems and software applications to communicate, exchange data, and use the transferred information. Data exchange schema and standards should permit data to be shared across clinician, lab, hospital, pharmacy, and patient regardless of the application or application vendor. Health systems are unable to communicate with each other; time and again, patients have complained about and suffered due to poor information sharing among healthcare providers, sometimes even between departments in the same hospital. According to a 2014 study, only six percent of US healthcare providers could access and exchange information with different EMR systems.17 Health informatics should focus on achieving 100 percent interoperability among healthcare networks and the efficient exchange of EHRs.

5.5.4. Example- EHR interoperability problem in Germany

Not only the US healthcare system has serious problems with EHR interoperability; Germany, a country whose healthcare system performs very well in most rankings, is also facing a major infrastructure crisis. When it comes to e-health, many Germans feel as if they are living in the Stone Age. For example, Germany has neither an all-inclusive EHR nor a national patient identifier. Although most physicians use electronic billing and documentation in private practice, only about half of the doctors adopt non-clinical systems, such as online services. Even worse, prescriptions are still on paper, as are referrals and sick notes.

Some stakeholders are skeptical about the value of electronic health cards. They are concerned that health data will be stored centrally, not directly on the card and could offer a single entry-point for hackers. Consequently, medical associations and health insurance companies are now speculating about the end of the electronic health card. Tests have shown that these cards are not practical and already technologically outdated. Some insurers started developing their own digital platform; however, these new platforms are making the digital healthcare landscape increasingly fragmented, which is the worst thing that can happen to a healthcare ecosystem. The dispute over the design and feasibility of the electronic health card is likely to persist for many years.

In 2002, the German government decided to modernize the statutory health insurance, including the implementation of an electronic health card. However, the companies involved in this project failed to deliver a working solution, mostly due to complicated data protection regulations. Consequently, in 2015, the Federal Cabinet passed a bill for secure digital communication and healthcare applications, which provided concrete deadlines for implementing a nationwide, technically mature telematics infrastructure for interconnecting patients, doctors, hospitals, and health insurance companies.

However, the implementation did not go ahead as planned. Too many stakeholders took part in the development, a scenario that led to the technical requirements changing over 150 times. Thus, despite many years of development and a staggering 1.9 billion euros, the current card holds only the patient name, address, date of birth, illnesses, health insurance number and insurance status, as well as a photograph of the cardholder; it does not store data such as known allergies, patients' specific

medication plans, implants or previous diseases, as had been planned. In addition, it is not intended to store other critical health data, such as information garnered from medical devices, or genomic-, proteomic- or metabolomic data that can be used to improve precision medicine.

5.5.5. The danger of fraudulent practices

Fraudulent healthcare claims are also an increasing burden on many healthcare systems. Generally, healthcare frauds are not obvious and thus difficult to detect. They often originate from the inside of an organization. Typical examples of healthcare fraud techniques include:

- *Providers who bill for services not provided.*
- *Doctors who administer tests or conduct procedures not medically necessary.*
- *Administrators who practice multiple-billing.*
- *Healthcare providers who charge more than peers for the same services.*
- *Researchers who modify clinical trial or research study data.*
- *Policy holders who allow others to use their healthcare cards.*

5.5.6. The danger of cyberattacks

More high-profile cyberattacks have hit companies in recent years, such as Quest Diagnostics, which provides diagnostic services to millions of Americans each year and health insurance giant Anthem, the second largest health insurer in America. The attackers gained unauthorized access to Anthem's IT system and obtained the names, birthdays, medical IDs, social security numbers, street addresses, email addresses and employment information, including income data of 78.8 million customers. According to Protenus, a company that monitors health data breaches in the United States, on average, there are daily, costly breaches in healthcare systems, with the majority (59.2%) of breached patient records—230,044 records (for January 2017)—are attributed to insider incidents.

5.5.7. Where interoperability shows promise

Despite Health-related regulations, healthcare organizations still aren't doing enough to protect themselves or their customers from such cyberattacks; those companies must take steps now to prevent future incidents. One step forward could be the decentralization of health and research and development data via blockchain technology. In this scenario, patients will control their own data through a patient-centric EHR blockchain—a network of computers that stores identical encrypted medical records that protects patients' privacy against corruption because encrypted duplicates are permanently stored on the network. We might need new rules and guidelines to help healthcare professionals understand how health related regulations would potentially apply to blockchain technology. Client information would need to remain secure through any data transfer process, even across regulatory borders. Although 100 percent crime prevention is impossible, using blockchain would allow for the possibility of gaining full detection, accountability, and audibility across highly complex systems.

Beth Israel Deaconess Medical Center took the first step toward the necessary physical, technical, and administrative safeguards to make all processes possible. A teaching hospital of Harvard Medical School in Boston, the center made blockchain technology a working reality by implementing a system called MedRec, a platform for managing medical records that uses the Ethereum blockchain, a decentralized platform that supports applications that run exactly as programmed without possibility of downtime, censorship, fraud, or third-party interference. In addition, Amazon is developing an EHR blockchain via its stealth team, named 1492.20 With the aggregation of a critical mass of patient EHRs in the AWS blockchain, Amazon can mine these significant data stores with deep learning tools to identify disease patterns, aging trends, and efficient treatment models more quickly. Furthermore, it can potentially sell or make available anonymized patient data to researchers studying aging demographics, disease prevention, and public health issues.

Estonia was the first country to implement a blockchain into its electronic healthcare record system with the collaboration of Guardtime, a local team of over 150 cryptographers, developers and security architects, using their keyless signature infrastructure (KSI). Governments should learn from Estonia's example. This small Baltic country continues to be one of the most digitally advanced, using blockchain to keep citizens' data safe. Guardtime was one of the very first companies to leverage blockchain technology in the EHR-space. So far, mostly start-ups have followed, typically in the early stages of platform development, such as Medibond, which seeks to improve interaction between the biggest healthcare industrial players to help provide services more efficiently and securely to end users. On its platform, a trinary multisignature sign-off from all parties (insurance, pharmacies, doctors) is required for the dispensation of any data to third parties.

Another start-up, Medicalchain, is looking to give users of the platform full access and control over their EHRs, enabling them to license their EHRs to pharmaceutical companies for research. When used in conjunction with Medicalchain's conditional permissioned access system, users will be able to set parameters on what information is available and how long companies may access it. Similarly, E-Nome, an Australian private company, developed a system based on blockchain and encrypted database technology that empowers consumers to control their medical history on their smartphone. The system allows consumers to share their data anonymously to participate and assist in medical research.

Google's health-tech subsidiary, DeepMind Health, is also piloting what it calls the verifiable data audit using a digital ledger that automatically records every interaction with patient data in a cryptographically verifiable manner. Any changes to, or access of, the data would be visible. The ledger will be append-only, so that once a record of data usage is added, it cannot be erased. Moreover, like traditional blockchain solutions, the ledger will allow third parties to verify that nobody has tampered with any of the entries. The company's data audit system uses a mathematical function called a Merkle tree, which allows a relatively small record to represent the entire history of the data, yet instantly shows any attempt to rewrite history.

DeepMind Health's solution has also attracted criticism because of the difficulty of distinguishing between uses of data for care and research. Patient groups criticized the overly broad data sharing agreements, raising fears that the data sharing mechanism has the potential to give DeepMind, and

thus Google, too much power over regulators and patients. DeepMind Health tried creating a board of independent reviewers for the DeepMind Health platform to address criticism; however, only transparency and better control of the data can build genuine trust in the long term.

Blockchain companies involved in medical/health record management

BurstIQ, www.burstiq.com

DeepMind Health, deepmind.com

E-Nome, enome.io Gem, gem.co

Guardtime, guardtime.com

HealthHeart, www.healthheart.io

Labchain, www.labchain.nl

Medicalchain, medicalchain.com/en

MediBond, medibond.io

Minthealth, minthealth.io

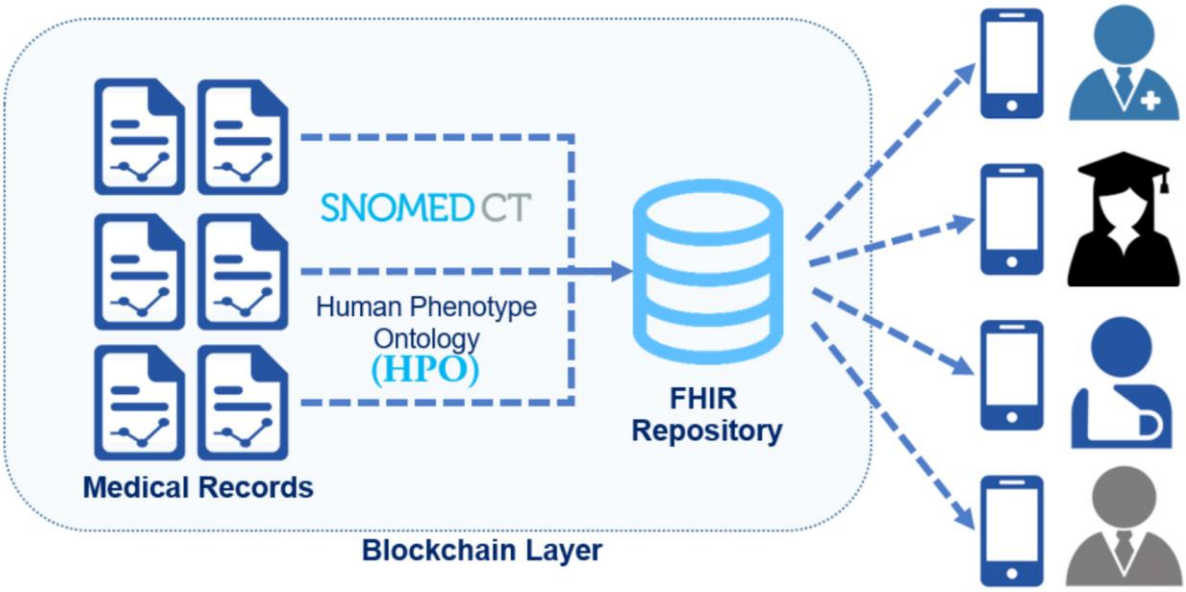
Patientory, patientory.com

Solve.care, solve.care

YouBase, www.youbase.io

5.5.8. Interoperability standards

For EHR interoperability, all stakeholders must adopt certain governance and trust principles, create business agreements, and use highly detailed guides for implementing standards. Tackling these issues requires both a multi-stakeholder approach and strong incentives. This is often a problem. Many stakeholders in the healthcare industry do not have a proper motivation. Many sellers of items or services can keep customers they might otherwise lose if they make it difficult to move data to another vendor's system. Similarly, healthcare providers can keep lucrative patients they might otherwise lose if they make it cumbersome and expensive to transfer a medical record to a new provider. Patients and policymakers have the clearest and strongest interest in promoting interoperability. It is up to them to push for robust, cross-vendor interoperability in the healthcare ecosystem. In highly competitive markets, providers might turn the other way even when the cost and complexity of interoperability are reduced. Starting such processes anew with blockchain technology has enormous potential, but stakeholders must avoid the implementation mistakes of other industries from the start. Blockchain enthusiasts should seek to leverage existing standards that support clinical data capture and exchange (Figure 31, next page).



In healthcare, standards provide a common language and set of expectations that enable interoperability among systems and devices. New platforms based on blockchain technology need to adopt standards. Vendors and communities that develop new EHR platforms should use the HL7 FHIR standard so that users could transfer healthcare information over standard APIs.

Figure 31: The need for standards development and adoption

An advantage of using FHIR is that it can transfer specific bits of healthcare information—a word or code, not a whole record—from one place (e.g., the physician) to another (e.g., billing) so that healthcare workers need not sort through volumes of extraneous data to find what they need quickly. Communities of developers and researchers such as the Global Alliance for Genomics and Health (GA4GH) are supporting and developing FHIR for the exchange of health data. GA4GH is driving projects to build out the information infrastructure (forms, term lists, information models). These projects will help us to understand the terminology, and we need new information models to describe a clinical phenotype and support clinical care and research. Representing these data as FHIR resources with standard terminologies such as human phenotype ontology (HPO) and systematized nomenclature of medicine— clinical terms (SNOMED CT) will enable interoperability in the health system and help data analytics in research. HPO aims to provide a standardized vocabulary of phenotypic abnormalities in human disease. SNOMED CT is a comprehensive, multilingual clinical healthcare terminology to encode the meanings used in health information and support the active clinical recording of data.

While most established players in the EHR-ecosystem make their own systems, third-party developers could connect all the information through open APIs. This environment heralds an excellent opportunity for start-ups and smaller companies to enter the market. Tech giants embrace many new technologies such as nanotechnology, self-driving cars, artificial intelligence, and virtual reality. Blockchain presents one of the most substantial non-corporate start-up opportunities to further interoperability.

5.6. Block Chain Implementation challenges and considerations

Blockchain technology presents numerous opportunities for health care; however, it is not fully mature today nor a panacea that can be immediately applied. Several technical, organizational, and behavioural economics challenges must be addressed before a health care blockchain can be adopted by organizations nationwide.

5.6.1. Scalability constraints: trade-offs between transaction volumes and available computing power

The Blockchain Framework suggests that organizations can roll out permissionless or permissioned implementations of blockchain technology. Permissionless blockchains are appealing, because they enable broader access, allow for open-innovation, and tap greater computing power across the network. At the same time, existing permissionless blockchains, such as Ethereum or Bitcoin, face transaction volume constraints. Today, the Bitcoin blockchain processes approximately seven transactions per second, yet there are over 10 million users and 200,000 daily transactions. Many in the field are calling for the technology to evolve to allow faster processing times. Permissioned blockchains, for their part, can expedite the transaction processing times, but they may face computing power constrains due to reduced participation in the network. Theoretically, HHS could supply the computing power necessary to process all blockchain transactions on one, permissioned network for select participants; however, this would result in HHS being the relative owner of the blockchain and could preclude the value of a truly decentralized system. A nationwide blockchain, with a large number of health care participants, would make the system not only more interoperable, but it would also make it more secure.

5.6.2. Data standardization and scope

In addition to evaluating permissionless and permissioned blockchains, organizations should consider what information is stored on or off the blockchain. For health care information stored on the blockchain, the most immediate concern is the size of information stored on the blockchain. A free-form submission of data to the blockchain, such as doctor notes, could create unnecessarily large transaction sizes that could adversely impact the performance of the blockchain. Yet, the blockchain can still be efficiently operable with a specific, and confined set of data, such as demographic information, medical history, and codes for services rendered. To standardize data stored on the blockchain and to manage performance, organizations should align on a framework for defining what data, size, and format that can be submitted. In some cases, technical APIs can concatenate and de-concatenate the information stored and broadcasted to condense the data size. Lastly, participants can privatize the blockchain to restrict access only to registered and valid organizations.

5.6.3. Adoption and incentives for participation

Two levels of incentives are necessary for blockchain to succeed. On a technical level, a network of interconnected computers (nodes) must be present to supply the computing power necessary to create blocks once a transaction is submitted. In a permissionless blockchain, monetary incentives in the form of cryptocurrency encourage individuals to lend their computing power to the network. For permissioned

blockchains, participation could be encouraged through financial incentives or access to blockchain data in exchange for processing transactions. In addition to incentives for blockchain to work technically, further support may be needed to encourage organizations to adopt the technology and participate in a shared network. While some organizations are already testing the technology to verify and track medical records and claims internally, blockchain will be more powerful when the number of users on the shared network increases. Programs similar to the Center for Medicare and Medicaid Services (CMS)'s Meaningful Use program, which incentivizes providers to switch to electronic medical records, could increase adoption and facilitate a nationwide blockchain health exchange.

5.6.4. Costs of operating blockchain technology

While blockchain technology enables faster, near-real time transactions, the cost of operating such a system are not yet known. Health and government organizations spend a significant amount of time and money setting up and managing traditional information systems and data exchanges; requiring resources to continuously troubleshoot issues, update field parameters, perform backup and recovery measures, and extract information for reporting purposes. Blockchain's open-source technology, properties, and distributed nature can help reduce the cost of these operations. Once a blockchain and its smart contracts are configured, the parameters become absolute, negating the need for frequent updates and troubleshooting. Since blockchain records are also immutable and stored across all participating users, recovery contingencies are unnecessary. Moreover, blockchain's transparent information structure could abolish many data exchange integration points and time-consuming reporting activities.

At the same time, a blockchain consumes significant computing power to process transactions. The cost of computing power is derived from the volume and size of transactions submitted through the network; further varying by the type of transactions occurring on the chain (e.g. data storage vs. value exchange). Beyond the Bitcoin blockchain, there are scarce blockchains in full production, and as such, it is difficult to forecast the possible costs of operating a blockchain at scale within a private enterprise or among a consortium of partners. Therefore, to understand the potential costs of a fully scaled blockchain, customized to meet HHS and partner needs, targeted experiments and common blockchain guidelines are needed to iteratively test the technology with a view to scale.

5.6.5. Regulatory considerations

Health care policy makers should consider deep collaboration with industry in order to understand and facilitate growth of the ecosystem within the bounds of the existing regulatory framework and new administration policy objectives. Considerations may include the implication of the distributed storage nature of the blockchain, who has ownership of records (and when does ownership change?), and how is access granted using the blockchain. HHS, through HIPAA Privacy Rule, establishes national standards to protect individuals' medical record privacy. The Rule sets the conditions with which to protect the privacy of personal health information and sets limits and conditions on use and disclosures which may be made without patient authorization. Because of these conditions, a blockchain solution could address the HIPAA Privacy Rule by separating and encrypting identity, PII and PHI into

segregated entities that can be accessed through the blockchain based on KSI hierarchies. As addressed in the interoperability section, patients can share distinct identity attributes with the health care ecosystem on as-needed-basis. At the same time, the type of high-level demographic information stored on the blockchain requires careful consideration; a combination of this demographic information paired with location data, could in theory allow for the triangulation of a specific individual. As an example, the potential to identify an individual with a rare health condition may be greater in a rural area as compared with a densely populated urban center. These concerns may be partially mediated through a permissioned blockchain. Nonetheless, as blockchain experiments advance, the questions will need to be carefully considered.

5.7. Shaping the Blockchain Future

Blockchain technology creates unique opportunities to reduce complexity, enable thrustless collaboration, and create secure and immutable information. HHS is right to track this rapidly evolving field to identify trends and sense areas where government support may be needed for the technology to realize its full potential in health care. To shape blockchain's future, HHS should consider mapping and convening the blockchain ecosystem, establishing a blockchain framework to coordinate early-adopters, and supporting a consortium for dialogue and discovery.

6.1.1. Map and convene the ecosystem

Blockchain technology is evolving rapidly, and new developments emerge weekly. As the technology advances and new applications become possible, the Office of the National Coordinator can play a valuable role in convening stakeholders from health care providers, plans, life sciences companies, startups and academics to discuss progress, share lessons learned, and identify unanswered questions. To that end, HHS could develop a sensing mechanism to track promising new startups and establish a forum for connecting them to more established organizations to undertake experiments.

6.1.2. Establish a consortium to experiment

Consortium has an opportunity to support a health care to test blockchain technology. As blockchain matures in health care, the financial services industry could offer valuable lessons learned. R3 CEV is a consortium comprised of financial services industry veterans, technologists, and over 40 financial institutions. A similar consortium could support the exchange of electronic medical records in early blockchain trials. Consortium could play a vital role in forming and convening select players for experimentation.

6.1.3. Design and execute experiments

Blockchain experiments could help authorities to determine what the technology can readily accomplish. The experiment design should look to addressing holistic work stream problem sets with transactions crossing multiple parties from creation to archival storage. Creating the experiment early and following it through complete transaction cycles can help developers and policy makers to address friction points and identify areas of advantage prior to nationwide implementation.

6.1.4. Consider the investment

The investment into blockchain technology is growing in industry and the major consortiums requesting for funding to pay for the blockchain enterprise experiments. The potential efficiencies, cost savings and increased security could save government and industry. In a resource constrained environment, however, existing capabilities or technologies could be leveraged for near-term benefits while targeted experiments can demonstrate where blockchain technology might create transformational, long-term value.

6.1.5. Establish suggested guidelines for blockchain in health care

Similar to the Internet, blockchain's potential increases with the number of participants in the network; yet for all participants to derive value from the network, a common approach is needed. The concerned Govt Ministries may issue guidelines for standardizing and storing data on the blockchain. Specifically, could evaluate which information should be stored on or off the blockchain and the format in which it should be stored. Blockchain technology, while still nascent, presents numerous opportunities. A blockchain-enabled, trusted exchange of health information can provide longitudinal views of patients' health, generate new insights about population health, and support the move toward value-based care. With greater transparency, trust, and access to data, authorities can then also garner insights for better safety, effectiveness, quality, and security of foods, drugs, vaccines, and medical devices. The promise of blockchain has widespread implications for stakeholders in the health care ecosystem. Capitalizing on this technology has the potential to connect fragmented systems to generate insights and to better assess the value of care. In the long term, a nationwide blockchain network may improve efficiencies and support better health outcomes for patients.

Chapter 6 – Health Informatics based framework for Pandemic Management

We will focus on some areas—identity and data governance, healthcare talent management, and incentives for behavioural change. —in which both public and private sectors to participate.

6.1. Self-sovereign identity and shared data

Data is perhaps the most powerful asset in fighting pandemics. If governments, clinicians, and citizens had access to data about a virus, they could take effective steps against it. We need data about what, where, when, how, who—how many people are infected, where are they located, when were they infected (and when did they recover), how were they infected, and who else did they contact?

The countries with good access to such data—China, South Korea, and Singapore, for example—have had some measure of control over this coronavirus. Since they had experienced SARS or MERS, they were much faster to ban travel, impose quarantine, and enforce social distancing. Now Hubei province in China has lifted travel bans, and shopping malls in Wuhan are reopening under banners, Wuhan is back! Countries with poor data—Italy, Spain, and now the United States—have fared much worse.

But getting good data these days comes at a high cost to privacy and individual rights. Brian Magierski, CEO and founder of Care to Cure, observed that the virus spread like wildfire where civil liberties reign supreme, whereas governments that more rigorously controlled the viral contagion did so at the expense of these liberties.

For example, Chinese authorities slowed and eventually impeded the spread of the virus through mass surveillance and big data analytics combined with propaganda. Let's start with the surveillance. There are an estimated 170 million closed-circuit television cameras in China, roughly one camera per dozen citizens. These continually stream video into a centralized system that applies facial recognition software and other AI to identify people within their database and check their whereabouts against their identities—which is all the easier because it's a real-name system, meaning that citizens must use their government-issued IDs to buy mobile SIM cards, open social media accounts, and travel by air or rail. No pseudonyms. So, if the Chinese lawfully buy SIM cards, the government can track citizens by their mobile devices. In Hangzhou, authorities deployed security staff wearing Rokid smart glasses with augmented reality. As they roamed the streets, security officers could check the temperatures of several hundred people in only a few minutes. During the total lockdown, people needed

special permission to travel outside their immediate neighbourhood. If they were caught on camera but didn't have permission to be where they happened to be, then the police showed up. If they ventured beyond the nearest grocery store, they got a phone call from the police. Combined with a campaign of collective action and personal sacrifice, China managed to save countless lives and instill pride in its citizens for their unified response, compared to the seemingly impotent efforts of the West.

Blockchain opens a new world of possibilities that shift control to individuals. In the city of Hangzhou in Zhejiang Province, VestChain Technology—a tech firm that develops open-source blockchain solutions on Ethereum in support of smart contracts and machine learning—has launched a decentralized application for identity management. Called Access Pass, the app integrates with WeChat to generate QR codes that enable residents only to enter their gated communities. According to VestChain, the app collects, encrypts, and stores users' personal data in VestChain's blockchain-based cloud servers; not even VestChain can access these data, and it has committed to deleting the data when the pandemic has run its course. This is important for the future of health, prosperity, and freedom because your medical information is a subset of your digital identity— the virtual you. The digital crumbs that you leave in daily life create a mirror image that knows more about you than you do. You probably can't remember dozens of your personal identifiers: the numbers and other details of your driver's license, passport, credit cards, marriage license, university or corporate ID. But unless your brain works differently from ours, you definitely don't recall your exact location a year ago, what you bought or how much money you spent and received that day, what you said online, and maybe not even which medications you took. Blockchain ledgers can remember for you. That's just the beginning. In the future, the virtual you will contain detailed medical information like your heart rate, blood pressure, temperature, and myriad other real-time measures of what you do, how you function, where you are, and perhaps even how you feel. The trouble is that the virtual you are not owned by you. Imagine if General Motors did not pay for its steel, rubber, or glass—its inputs, economist Robert J. Shapiro once said. That's what it's like for the big Internet companies. It's a sweet deal. We create the asset, but powerful companies and governments expropriate it.

6.1.1. Why should we care about our medical data?

- We came up with at least four reasons for caring deeply about our own and our dependents' medical data, especially for those of us with teenagers hugely active on social media or elderly parents unfamiliar with the latest online scams

- We can't use our own data to plan our lives—our health, our financial planning, our education, and so forth. These data reside in other people's silos, which we can't access—but third parties like Cambridge Analytica can, often without our knowledge.
- We enjoy none of the rewards of this third-party data usage, yet we bear most of the risk and responsibility for its clean up, should they lose or abuse our data.
- Our privacy is at risk. Privacy is not an absolute and sometimes, perhaps in say a pandemic, it may be necessary to trade on this privacy for the social good. The trouble is however that once the crisis is over there is no way to capture our data back.
- We can't monetize these data assets for ourselves, resulting in a bifurcation of wealth and all its discontents.

Social media companies like Facebook and other big digital conglomerates have suggested ways we could access some of our data. That's a step forward. However, it only partially solves one of four problems listed above—access to our data. We need more than access to some of our data. We need ownership of it.

Some governments have attempted to help solve this problem by implementing laws such as European Union's General Data Protection Regulation, which is a partial measure at best, and hypocritical in light of the new EU common identity repository. Nor is a heads-willroll type of policy that calls for the breakup of Amazon, Facebook, and Google for violating anti-monopoly laws. State-run identity systems are problematic. In the last ten years, at least 48 government databases have been breached, exposing the data of 1.44 billion people—and that number doesn't include hacks to government-managed healthcare and education records.

Yet, we're dependent on system administrators who can freeze access, delete our voter registration or other credentials, and use banks, telecoms, and tech firms to surveil us. Nothing about these institution-centric systems is citizen-friendly. In some countries, these systems discriminate against the poor, the rural, the homeless, the imprisoned, and the overworked in society. Syrian refugees in particular put a spotlight on the crisis of statebased identification. The reality of a government-sourced and sanctioned identity is untenable—both administratively and philosophically. Why should any government get to rubber-stamp who we are? We should be establishing our own identities and, as Joseph Lubin of ConsenSys wrote, bootstrapping ourselves into economic enfranchisement.

6.1.2. The self-sovereign identity in the time of pandemics

What each of us needs is a self-sovereign and inalienable digital identity, one that is neither bestowed nor revocable by any central administrator and is enforceable in any context, in person and online, anywhere in the world. What we need is a wholesale shift in how we define

and assign ownership of data assets and how we establish, manage, and protect our identities in a digital world. Change those rules, and we end up changing everything.

As we argued in Blockchain Revolution, the means now exist to assert what developer Devon Loffreto calls sovereign source authority : identity is not simply endowed at birth; it is endowed by birth. Each identity is in a black box on a blockchain. It sweeps up the exhaust of all our daily transactional and information data—from purchases to our biological data—protecting it and enabling each of us to use it any way we want.

So imagine that each of us owned our digital identity and stored it in a digital wallet on a blockchain. It sweeps up the exhaust of all our daily health and transactional data—from our biological data to purchases or our location at any point in time—protecting it and enabling each of us to use it any way we want. Our medical records are central to this identity. Our bodies generate medical data. We, not big companies or governments, have a heart rate and a body temperature. When clinicians measure us or take tests of various kinds, that's great, but the data are still data from our bodies. Increasingly with wearables and the IoT, we can capture these data from our insulin levels, blood pressure, body temperature, and the number of steps we take and stairs we climb in a day. By owning our medical and other personal data we could solve the four problems stated above—access, security, privacy, and monetization.

6.1.3. But how could we help officials in a pandemic?

Here's where the blockchain comes in.

- By law, governments could mandate that citizens make available anonymized data about critical health information like, say, body temperature or location for aggregate tracking and predictive analytics.
- Citizens could instruct their digital identities to provide pertinent health information to any registered clinician should they need it, for example, if they were to be hospitalized. Citizens may decide to withhold some information, such as a fracture from an accident a few years ago or a psychiatric problem they have faced. But the smart contract managing their identity would release all other information that may help with their treatment.
- Incentive systems could reward us for making our private data available to appropriate clinicians and government planners, even with identifiers attached. Many citizens would share their data out of sense of a social responsibility and community. Personally, we both would happily reveal medical information about our body temperature or a dry cough or for that matter a positive test of COVID-19 to authorities to help manage the problem in our communities. But there could be extrinsic blockchain-based incentive systems to help as discussed later in this report.

- All these data would represent the entire population, not some partial and potentially misleading sample of it. Never before have clinicians, epidemiologists, and authorities had such extraordinary access to such a wealth of data. Using next generation data analytics and AI they could understand the possible trajectories of a virus and take steps to crush it in the egg, like never before.
- As individuals recover and develop verifiable immunity, they could receive a health certification to attach to their digital identity, to prove that they're safe to work publicly again. Each citizen could choose which personal information other parties may retain. Some citizens might choose to recall access rights to their released medical information, leaving only the anonymized data.

6.1.4. Transitioning to a new paradigm for identity and personal data

This transition will take time. The ultimate solution must exist independent of any corporation, government, or other third party, and should not be subject to the agency risk of executives or political parties. It must interoperate with these institutions, even as it outlasts them. In fact, it must be built to outlive its users and enforce their right to be forgotten. This would mean separating data rights from the actual data, so that the rights holder could delete it. To be inclusive, it must be user-friendly with a low-tech mobile interface and low-cost dispute resolution.

We expect organizations to take at least three actions to rebuild the trust of those whose data they hold. The first involves governance. Many large corporations and government agencies have strong governance mechanisms for their hard assets, but really poor governance of information assets. Companies must define decision rights around their data and develop an accountability framework that disciplines how employees use data. Said David Jaffray of the University of Texas MD Anderson Cancer Center, We need an entire stack of data governance technologies. To me, blockchain is the illustration that makes me believe that it's actually possible.

The second involves the discontinuation of practices that collect and store customer data. This could involve either destroying these massive customer databases altogether (after returning files and records to customers) or migrating these data to distributed storage systems, such as the IPFS, and then transferring control to customers.

The third involves the cultivation of a new core competence: the ability to work with huge anonymized datasets rented from large numbers of people, all handled in a distributed and trust-minimized manner. It will remove data as a toxic asset from the corporate balance sheet and make it a fundamental human asset from birth. It will flip the data-analytics business model on its head and reward corporations for serving as data brokers on behalf of individuals. This

will see the end of the large centralized data frackers that scrape, hoard, and rent, but don't protect this data.

These new approaches to privacy and ID management give citizens ownership of their medical information and their identities, the facts of their existence, and the data they create as they live their lives. The self-sovereign identity is one the pillars of a new social contract for the digital economy, and will be critical to the transformation to a more open, inclusive, and private economy. Of course, such changes are massive, and we can't expect to implement them fully in time to help us with COVID-19. As the pandemic takes hold, we are making decisions without reliable information, said Dr. Alex Cahana, ConsenSys Health's chief medical officer and market lead for Europe, the Middle East, and Africa.

6.2. Creating a rapid response registry for the workforce

Another supply chain experiencing dire distortion because of the pandemic is the supply of medical talent around the world. Hospitals and clinics are finding doctors and nurses themselves in short supply, exacerbated by the shortage of personal protective equipment.

In the best of times, there exists what Andy Spence calls a talent management paradox, where organizations continuously struggle to tap into the talent supply chain despite the abundance of talented people looking for work. During a pandemic, the ability for the healthcare industry to source medical professionals becomes even more challenging.

6.3.1. Licensing and staffing challenges

The red tape and redundancies of licensing are not new to the medical industry. Typical human resources operations have to deal with opaque talent supply chains, candidate fraud, and rapidly shifting talent pools as they face the challenge of finding the right candidate with the right skills for the job. COVID-19 highlights this problem. Vetting the licenses of medical professionals slows down the deployment of this crucial talent, as staffing agencies are forced to review a mishmash of identities and certifications from a number of institutions.

Although the current system of certification provides a level of trust essential to the healthcare industry, we could eliminate redundancies while maintaining trust by using cutting-edge technologies such as blockchain. Applying blockchain to this problem—and its values of decentralization, transparency, and trust—would create the kind of system we need to match certified medical professionals quickly and efficiently to the hospitals and clinics desperate for help.

6.3.2. Issuing medical certifications on the blockchain

The creation of self-sovereign digital identities managed through a digital wallet system opens up opportunities here. An individual's digital identity could include government-licensed ID and healthcare records as well as certificates of achievement in education and professional development, all verified and recorded to a blockchain. A network of identities managed through a blockchain platform like Sovrin would create a transparent and trusted skills marketplace, where supply and demand of labour could interact seamlessly without recruiters. Delay in (re)certification relates to redundant activities of applicants and staffing agencies: all go through multiple institutions to verify each person's certification and identity.

In a blockchain-based medical talent marketplace, certifying bodies would record these distinct pieces of identity and skills to the individual's digital identity wallet. Instead of the applicant's sending data from varied sources, and the association's having to verify each piece of identity data against their issuers, all parties could use a rapid response registry. It could be as simple as a smart contract that automatically checked whether a candidate met the criteria, and had the experience and certification necessary for (re)licensing. If these conditions weren't met, that system could send an automated message to that wallet holder with feedback on what the individual had to change in order to be licensed.

Candidates can also update their knowledge and profile on the blockchain, e.g. Online education platforms such as Nurse.com and IntelyCare are providing COVID-19 specific training to nurses; if these courses were run on this kind of blockchain-based system, COVID-19 training certification could be added automatically to a nurse's digital wallet once they completed training.

6.3.3. Deploying the global medical talent marketplace

Once medical professionals' credentials are verified and they have received licenses to work, the blockchain-based registry can automatically match skills and talent to job openings. Newly licensed individuals can make themselves searchable in the marketplace, and the authenticity of their digital identity provides a layer of trust for those looking to fill their talent gaps. Instead of completing background check and clearances, the staffing unit already knows that this individual meets the organization's requirements. The self-sovereignty of the license also means that it is not administered centrally and can therefore be enforced anywhere in the world.

This talent marketplace is also adaptable to changes in regulation. As governments relax restrictions on the jurisdiction of professional licenses, the system can immediately respond to regulatory change by updating the criteria for nurses in the respective jurisdiction. Deploying

medical professionals across state and country lines, dependent on regulation changes, becomes much faster and more transparent.

6.3.4. A health credential for workers and job seekers

Redeploying workers who have contracted and recovered from the disease should be a priority. If we could certify them as virusresistant and add that credential to their identity, then they could more quickly return to work in hospitals, grocery stores, and other essential services with greater certainty that they were no longer contagious or susceptible.

6.3. Incentive models for change

If ever there were a time for individuals to act in a way that serves the greater good, it is during a pandemic. Public health has always been a collective responsibility, and as such, the steps to getting there are not always easy or agreeable. Being simultaneously for the people and by the people, achieving a functional, public health commons is made more complex because on one hand, not all people have equal access to care, and on the other hand, the thoughtless actions of a few can undermine the concerted efforts of many. As we are discovering during COVID-19, rallying together to self-isolate and engaging in other public health measures to try to save the lives of our elders and prevent our front-line healthcare workers and hospitals from becoming overwhelmed, is more easily said than done. We need a new blueprint. There are two issues at play.

The first pertains to individual accountability in a healthcare crisis. How do we get people to conduct themselves appropriately so that public health need not be an elusive goal? How do we balance individual liberties in the pursuit of the collective good? What kinds of incentives do we need to have in place so that humans manifest the behaviours that will both prevent viral outbreaks from becoming pandemics in the first place, or to behave in such a way as to mitigate the damage they cause? And how can we protect individual privacy in the process of understanding viral transmission from one person to another?

The second issue is that the responsibility for public health does not solely rest on the shoulders of the individual but with the many organizations and governments the world over. Institutions are responsible for public health policy, border control, reliable delivery of public health services, infrastructure, crisis responsiveness, and the allocation of budgets. What incentives are needed to improve the current public healthcare infrastructure and provide adequate budgets, stockpiles of supplies, and preparations for outbreaks of the future?

It is in this context that we see a profound role for blockchain technology to drive much-needed behaviour change by both individuals and entities alike. Blockchain is the platform that facilitates a secure and transparent digital exchange of assets of all kinds, while

simultaneously rewarding favourable activities, preserving privacy, and doing so in a secure fashion, all with the potential to be as ubiquitous as the mobile phone.

In a pandemic scenario, data are highly sought-after assets, specifically data around virus properties, transmission rates, fatalities, carrier travel histories, and so on. But data are not the only assets that matter. Good old-fashioned money—which enables access to resources such as food, rents, medicine, personal protective equipment, and in some jurisdictions, healthcare itself—is just as important during a time of crisis as it is in our pre-pandemic lives. It is not only possible but probable that blockchain can be the driver of change by aligning our individual need for survival through resource accumulation with our collective need for behaving in a socially responsible way.

6.3.1. Incentives to change individual behaviour

Controlling a pandemic depends on all of us doing the right thing, all the time. So how do we get there? What kind of incentives will work best? Incentives for individuals are indeed a powerful tool to create a new kind of order in the world. Rewards produce reinforcing behaviours. When rewards accumulate, we find ourselves better off.

The beauty of blockchain technology is that it is programmable money. Depending on the application in question, an economic reward in the form of digital currency or a loyalty token can be issued to a given party when certain conditions are met. Blockchain based rewards, delivered to individuals through an application on their phone, can make the right behaviour more feasible than if those rewards were non-existent. Individuals are generally motivated to work toward their economic and personal self-interest.

6.4. Implementation challenges Crises create opportunities for change

Just as the rising costs of climate-related incidents have moved insurance companies to consider the impact of adverse climate events on a given policy, we could witness a similar reckoning in healthcare as we come to terms with the high costs of this pandemic on society. Now is the time to lead the rapid deployment of blockchain technology. Yet so much can get in the way of progress: the absence of leadership, the lack of shared values and governance, competing standards, and inertia.

6.4.1. Leadership

This crisis has revealed the need for a coordinated, multi-stakeholder approach to problem-solving. That means motivating different governments, industry participants, and civil society

to work together. Unfortunately, this pandemic could not have come at a worse time: rising populism has led to an every-country-for-itself attitude that is undermining our global response.

6.4.2. Shared values and governance

We are living in the polarizing tension between freedom and security. Right now, the threat to our security is a pandemic, and the threat to our freedom is current and future corporate and governmental surveillance. Data is a critical resource for governments fighting a pandemic, but we must ensure that its use doesn't compromise individual liberty permanently and irrecoverably as a result .

6.4.3. Sense of urgency

COVID-19 may well be the wake-up call to governments, hospitals, and other stakeholders in the healthcare space, and there's no time to waste in implementing solutions that drive positive global health outcomes. Now, when the need is greatest, is the time for organizations and governments to overcome their inertia and their unwillingness or inability to implement new technologies, business models, and roles for people. Otherwise, once the crisis has passed, this sense of urgency will subside with every normal day, and time will dull the sharp memories of suffering and pain. Pandemics are a white swan, not black swans—they happen regularly, if infrequently—and thus we have no excuse for our unpreparedness. Blockchain is not a panacea for pandemics. We need functioning governments and institutions, global collaboration, a conscientious, healthy, and engaged populace, and businesses that plan for the long term and the unexpected. But we can and should harness this technology straightaway to address these many challenges.

6.5. Recommendations for Block chain based Pandemic Management: A coordinated plan

We all have a role to play. Leaders around the world are looking for ways to mitigate the effects of this crisis—and, when the dust settles, they should be implementing changes so that a pandemic does not grip our world in the same way ever again. It's time to get serious about blockchain and the more secure, transparent, high-performance, distributed, and data-rich systems and institutions that we can build with this technology. Again, there is nothing so powerful as an idea that has become a necessity. All three pillars of society—government, the private sector, and the civil society all have a role to play in this crisis. For each, immediate action is possible. For each, we should get cracking on implementing new approaches to achieving long-term goals.

6.5.1. What governments can do

First, every national government should create an emergency task force on medical data to start planning and implementing blockchain initiatives. Governments should lead but they must engage private sector and civil society leaders. To implement pilots now, we need new laws in many areas: our current legislative parameters use outdated frameworks that limit the ability to access and use data while protecting citizens' rights. Governments must set the policies to ensure that the second era of the digital age actually serves people. As we discussed at length in the roundtable, the COVID-19 crisis has emphasized the tension between our civil liberties and our health and security. By creating sensible legislation around privacy, security, and identity, policymakers can open up opportunities for blockchain innovation in self-sovereign identities and data governance.

Second, governments can stimulate the development of technology companies working on the solutions outlined in the report. Many of these are early stage companies that are critical but most vulnerable. This can be achieved not just through financial investments, but there are numerous other tax changes that can encourage investment in these companies, such as implementing flow through shares for investments in technology. Securities legislation in most countries hampers the development of blockchain fundraising activities like token generation events, and entrepreneurs must deal with regulatory unclarity or outright regulatory hostility toward this technology and its leaders. Further, governments can act as model users of the important platforms and applications coming out of this crisis.

Third, governments must pass legislation to mobilize stakeholders to create the self-sovereign health record and citizen identity. We can have our cake and eat it too; that is, real-time, granular data about the health of every citizen in a country, while at the same time protecting their identity, its privacy and security, its accessibility, and its monetization. We need dedicated, speedy work on consent frameworks and legislation that confers ownership of data on the individual. Consent and data governance are key to unlocking this potential of blockchain and how the technology can better serve society's needs. Policy makers, legislators and technologists must engage immediately both for better crisis/pandemic management and to deliver the much-needed emergency dollars to save the economy.

Fourth, they should pilot blockchain incentive systems to mobilize populations to self-isolate and behave responsibly as described in this report Yes, governments must require citizens to do certain things in time of crisis, such as during a war. Government mandated behavior is necessary in this crisis, but this can be supplemented, and the negative effects ameliorated through blockchain based incentive systems.

Fifth, governments have the biggest supply chains in the world, many of which are now involved in producing critical medical supplies and delivering services. The opportunities presented in this report for more proactive, flexible, and trustworthy supply chains should be thought-provoking for officials who must manage not only shortages but the public's faith in their systems.

Governments should move rapidly to implement national fiat digital currencies.

6.5.2. What the private sector can do

Blockchain is already beginning to change many industries, including parts of the financial services industry, shipping and global transportation logistics, upstream oil and gas, natural resource tracking and consumption, manufacturing, and segments of our global supply chain including food and electronics—many of which have been drastically hit by this crisis. That said, we are still in the very early days of this second era of the Internet, and deployment is still immature, pretty much across the board. Companies can act now, and benefit in the long term through understanding how blockchain can transform their businesses.

First, large players in these industries affected by COVID-19 must still lead the way, starting today, by incorporating blockchain into their infrastructures. Building systems using blockchain will create a wider, more thorough data environment to mitigate future crises like this one.

We don't want to build a system that is waiting for the next disaster. We want to build a system that is being used day-to-day, that then enhances our ability to respond in a disaster, said Wolpert of Golden State Foods.

Second, firms must build blockchain consortia in the industries affected by the crisis. By pivoting toward COVID-19, working groups can provide useful solutions to help mitigate the crisis, as well as demonstrate the value of blockchain in the face of distorted supply chains and data opacity, planning an important role as we return to a state of normal. We need coopetition among even the biggest competitors—especially in this time of crisis, as we all fight a common enemy.

Third, the private sector needs to continue its work to create pilots framed around all these opportunities: pilots on medical records, credentialing systems, incentive structures, and other sovereign identity solutions. Implementing a sovereign digital citizen identity that includes these aspects of identity will require cooperation with government.

Fourth, when architecting these pilots, companies would do well to consider embedding incentive systems to mobilize their consumers to behave in a socially responsible way—whether that be sharing their data for health research and infection tracking or following government-mandated pandemic protocols. To achieve effective.

6.5.3. What civil society can do

First, we recommend that privacy advocates turn away from focusing purely on laws and governmental regulation to protect privacy. Rather, it is time to advocate for a self-sovereign medical record and citizen identity to protect data privacy while also making it more easily accessible. As we have seen throughout this report, this crisis stems from a crisis in data accessibility. Without transparent data records, politicians, healthcare providers, researchers and citizens are not prepared to build proactive solutions. Citizens—the creators of this data—have a vital role to play in moving this dial forward.

Second, professional associations would benefit from exploring the sovereign patient record and becoming its strongest advocates. As Blockchain can enable patients to provide rights easily to their medical data to scientists and clinicians for critical research and planning.

Third, these associations, along with schools, colleges, and universities should consider blockchain-based platforms for medical licensing and accreditation. We need the right clinicians and practitioners at the right places in the right times and blockchain is the new platform for credentials and trust.

6.6. Conclusion

This pandemic has showed us the extent to which our current systems are not ready for the next age of our global economy and society. We weren't even ready for a highly predictable global calamity such as COVID-19. What makes anyone think we're prepared for the next global crisis, the next transformation to our economy, or the next shift in our way of life? A new era of transformative digital technologies is arriving, an era in which technology is working to understand and interpret in actionable terms for enterprise executives, government officials, heads of non-profit organizations, and their teams at the top in key economic sectors.

6.7. Future Work

Covid-19 outbreak affected the survey part, because Warriors are tremendously engaged 24X7 in fighting this pandemic. Hence, they were not able to part of the survey. Without them survey never be fruitful and effective.

In future survey of these different stakeholders (like Administrators, Doctors, Patients, Individuals from Society, Law Specialist, Logistics Specialist, Pharmacy Specialist, etc.) much needed to be conduct. That will help in building strong plan & roadmap for implementation of Blockchain in Health informatics.

References

- Joshi, A.P.; Han, M.; Wang, Y. A Survey on Security and Privacy Issues of Blockchain Technology. Math. Found. Comput. 2018, 1, 121–147. [CrossRef]
- Ji, S.; Cai, Z.; Han, M.; Beyah, R. Whitespace measurement and virtual backbone construction for Cognitive Radio Networks: From the social perspective. In Proceedings of the 2015 12th Annual IEEE International Conference on Sensing, Communication and Networking, SECON 2015, Seattle, WA, USA, 22–25 June 2015; pp. 435–443.
- Han, M.; Yan, M.; Li, J.; Ji, S.; Li, Y. Generating uncertain networks based on historical network snapshots. Lect. Notes Comput. Sci. 2013, 7936, 747–758.
- Duan, Z.; Yan, M.; Cai, Z.; Wang, X.; Han, M.; Li, Y. Truthful incentive mechanisms for social cost minimization in mobile crowdsourcing systems. Sensors 2016, 16, 481. [CrossRef] [PubMed]
- Kostakis, V.; Giotitsas, C. The (A)political economy of bitcoin. TripleC 2014, 12, 431–440.
- Efanov, D.; Roschin, P. The all-pervasiveness of the blockchain technology. Procedia Comput. Sci. 2018, 123, 116–121. [CrossRef]
- Buterin, V. A Next-Generation Smart Contract and Decentralized Application Platform; Ethereum White Paper; 2014. Available online: http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_ contract_and_decentralized_application_platform-vitalik-buterin.pdf (accessed on 15 June 2018).
- Ethereum Community. A Next Generation Smart Contract and Decentralized Application Platform. Available online: https://github.com/ethereum/wiki/wiki/White-Paper (accessed on 1 April 2018).
- Underwood, S. Blockchain beyond bitcoin, Commun. ACM 2016, 59, 15–17. [CrossRef]
- Zheng, Z.; Xie, S.; Dai, H.N.; Chen, X.; Wang, H. Blockchain Challenges and Opportunities: A Survey. Int. J. Web Grid Serv. 2016. [CrossRef]
- Agbo, C.C.; Mahmoud, Q.H.; Eklund, J.M. Blockchain Technology in Healthcare: A Systematic Review. Healthcare 2019, 7, 56. [CrossRef] [PubMed]
- Akins, B.W.; Chapman, J.L.; Gordon, J.M. A Whole New World: Income Tax Considerations of the Bitcoin Economy. Pittsburgh Tax Rev. 2015, 12, 24–56. [CrossRef]
- Sharples, M.; Domingue, J. The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward. In Adaptive and Adaptable Learning; Springer: Cham, Switzerland, 2016; pp. 490–496.
- Zhang, Y.; Wen, J. An IoT electric business model based on the protocol of Bitcoin. In Proceedings of the 2015 18th Intternational Conference on Intelligence in Next Generation Networks, ICIN 2015, Paris, France, 17–19 February 2015; pp. 184–191.

- Noyes, C. BitAV: Fast Anti-Malware by Distributed Blockchain Consensus and Feedforward Scanning. arXiv 2016, arXiv:1601.01405.
- Armstrong, J.S. and Overton, T.S., 1977, “Estimating nonresponse bias in mail surveys”, Journal of Marketing Research, 14(3), 396-402.
- Ahmed, E., Yaqoob, I., Hashem, I., A., T., & Khan, I., (2017). The role of big data analytics in Internet of Things. Computer Networks, vol. 129(2017), pp. 459-471.
- Ajzen, I. (1985). The Theory of Planned Behavior. Organizational Behavior and Human Decision Processes, vol. 50 Marc, pp. 179-211.
- Amoako-Gyampah, K. &Salam A.F. (2004). An extension of the technology acceptance model in an ERP implementation environment. Information &Management, vol. 41(6):731–745.
- Andrews, L., Gajanayake, R., & Sahama, T. (2014). The Australian general public's perceptions of having a personally controlled electronic health record (PCEHR). International Journal of Medical Informatics, vol. 83(12), 889-900.
- Anthony, D.L. & Stablein, T. (2015). Privacy in practice: professional discourse about information control in healthcare. Journal of Health Organization and Management, vol. 30(2), 207-226.
- Ba, S. &Paulov, P. A. (2002). Evidence of the effect of trust building technology in electronic market: price premium and buyer behaviour. MIS Quarterly, vol. 26 No. 3, pp. 243- 268/September 2002.
- Bagozzi, R. & Yi. Y. (1988). On the evaluation of structure equation models. Journal of Academy of Marketing Science, January 1988, DOI 10.1007/BF02723327.
- Bansal, G., Zahedi, F. M. &Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. Decision Support Systems, vol. 49 (2010) 138–150.
- Bem, D. J. (1967). An alternative interpretation of cognitive dissonance phenomena. Psychological Review, 1967, vol. 74, No. 3, 183-200.
- Berry, L. L. & Bendapudi, N. (2007). Healthcare: A fertile field for service research. Journal of Service Research, Vol. 10(2), 111-122.
- Eastlick, M. A., Lotz. S. L. & Warrington, P. (2006). Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. Journal of Business Research, pp. 59(2006), pp. 877–886.
- Kim, Y. (2016). Trust in health information websites: A systematic literature review on the antecedents of trust. Health Informatics Journal, 2016, vol. 22(2), pp. 355–369
- Li, H., Wu, J., Gao, Y. & Shi, Y. (2016). Examining individuals’ adoption of healthcare wearables devices: An empirical study from privacy calculus perspective. International Journal of Medical Informatics, vol. 88(2016), pp. 8-17.

- McCullough, J. S., Casey, M, Moscovice, I. & Prasad, S. (2010). The Effect of Health Information Technology on Quality in U. S. Hospitals, Health Affairs, vol. 29(4), pp. 647-654.
- Lin, C., He, D., Huang, X., Choo, K-K., R., Vasilakos, A. (2018). BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0. Journal of Network and Computer Applications, 116(2018), 42-52.
- Littlejohns, P., Kieslich, K., Weale, A., Stokes, T., Gauld, R. & Scuffham, P. (2018). Creating sustainable healthcare system. Journal of Health Organization and Management, vol. 33(1), pp. 18-34.
- Lupton, D. (2014). Health promotion in the digital era: A critical commentary. Health Promotion International, vol. 30(1), pp. 174-183.
- Chaudhry, B., Wang, J., Shinyi Wu, S., Maglione, M., Mojica, W., Roth, E., Morton, S. C. & Shekelle, P. G. (2006). Systematic review: Impact of health information technology on quality, efficiency, and costs of medical care. Annals of Internal Medicine, vol. 144(2006), pp. 742-752.
- Buntin, B. B., Burke, M. F., Hoaglin, M. C. & Blumenthal, D. (2011). The benefits of health information technology: A review of the recent literature shows predominantly positive results. Health Affairs, vol. 30(3), 464-471.
- Li, L., & Benton, W.C. (2006). Hospital technology and nurse staffing management decisions, Journal of Operations Management, vol. 24(2006), pp. 676–691.
- Queenana, C. C., Angstb, C. M., & Devaraj, S. (2011). Doctors' orders—If they're electronic, do they improve patient satisfaction? A complements/ substitutes perspective. Journal of Operations Management, vol. 29(2011), pp. 639–649.
- Devaraja, S., Terence, T. &Kohli, R. (2013). Examining the impact of information technology and patient flow on healthcare performance: A Theory of Swift and Even Flow (TSEF) perspective. Journal of Operations Management, vol. 31 (2013), pp. 181–192.
- Piccinini, P., Gamberini, R., Prati, A., Rimini, B., & Cucchiara, R. (2013). An automated picking workstation for healthcare applications, Computers & Industrial Engineering, pp. 64(2013), 653–668.
- Lahiri, A., & Seidmann, A. (2012). Information hangovers in healthcare service systems. Manufacturing & Service Operations Management, vol. 14(4), pp. 634-653.
- Sharma, L., Chandrasekaran, A., Kenneth K. Boyer, K. K. & McDermott, C. M. (2016). The impact of Health Information Technology bundles on hospital performance: An econometric study. Journal of Operations Management, pp. 41(2016), pp. 25-41.
- Yang, J. J., Li, J., Mulder, J. Wang, Y., Chen, S., Wu, H., Wang, Q. & Pan, H. (2015). Emerging information technologies for enhanced healthcare. Computers in Industry, vol. 69 (2015), pp. 3-11.

- Wan, J., Zheng, P., Si, H., Xiong, N., N., Zhang, W., & Vasilakos, A., V. (2019). An Artificial Intelligence Driven Multi-Feature Extraction Scheme for Big Data Detection, IEEE Access, vol. 7(2019), 80122-80132.
- Wang, Y., Kung, L. & Byrd, T. A. (2016). Big data analytics: Understanding its capabilities and potential benefits for healthcare organizations. Technological Forecasting & Social Change, http://dx.doi.org/10.1016/j.techfore.2015.12.019.
- Gan, W., Lin, J., C-W., Chao, H-C., Vasilakos, A., V., Yu, P., S. (2020). Utility-Driven Data Analytics on Uncertain Data, IEEE Systems Journal, DOI: 10.1109/JSYST.2020.2979279.
- Zhong, R.Y., Newman, S.T., Huang, G.Q. & Lan, S. (2016). Big Data for supply chain management in the service and manufacturing sectors: challenges, opportunities, and future perspectives. Computers & Industrial Engineering, vol. 101(2016), pp. 572- 591.
- Agarwal, R., Gao, G., DesRoches, C., & Jha, A. K. (2010). Research commentary—The digital transformation of healthcare: Current status and the road ahead. Information Systems Research, vol. 21(4), 796-809.
- Cutler, D. M., Feldman, N. E. &Horwitz, J. R.(2005). U.S. adoption of computerized physician order entry systems. Health Affairs, vol. 24(6), pp. 1654–1663.
- Jha, A.K., DesRoches, C.M., Campbell, E.G., Donelan, K., Rao, S.R., Ferris, T.G., Shields, A., Rosenbaum, S. & Blumenthal, D. (2009). Use of electronic health records in U.S. hospitals. New England Journal of Medicine, vol. 360(16), pp. 1628–1638.
- Kazley, A. &Ozcan, Y. (2007). Organizational and environmental determinants of hospital EMR adoption: A national study. Journal of Medical Systems, vol. 31(5), pp. 375– 384.
- McCullough, J. S. (2008). The adoption of hospital information systems. Health Economics, vol. 17(5), pp. 649–664.
- Ekblaw, A., Azaria, A., Halamka J. D., &Lippman, A. (2016). A case study for blockchain in healthcare: "MedRec" prototype for electronic health records and medical research data. White Paper, MIT Media Lab, Beth Israel Deaconess Medical Center, August 2016.
- Qadri, Y., A., Nauman, A., Zikria, Y., B., Vasilakos, A., V., Kim, S. W. (2020). The Future of Healthcare Internet of Things: A Survey of Emerging Technologies. IEEE Communication Surveys & Tutorials, DOI: 10.1109/COMST.2020.2973314.
- Porambage, P. Ylianttila, M., Schmitt, C., Kumar, P., Gurtov, A. & Vasilakos, A. V. (2016). The Quest for Privacy in the Internet of Things, IEEE Cloud Computing, vol. 3(2016), pp. 36-45.
- Perera, C., Qin, Y., Estrella, J., C., Reiff-Marganiec, S., & Vasilakos, A. (2017). Fog Computing for Sustainable Smart Cities: A Survey, ACM Computing Surveys, vol. 50(3), pp. 32-43.

- Wazid, M., Das, A., K., Kumar, N., Conti, M., Vasilakos, A., V. (2018). A Novel Authentication and Key Agreement Scheme for Implantable Medical Devices Deployment, IEEE Journal of Biomedical and Health Informatics, vol. 22(4), 1299- 1309.
- Wazid, M., Das, A., K., Khan, M., K., Al-Ghaiheb, A., A-D., Kumar, N., Vasilakos, A., V. (2017). Secure Authentication Scheme for Medicine Anti-Counterfeiting System in IoT Environment, IEEE Internet of Things Journal, vol. 4(5), 1634-1646.
- Victor Hugo, speech at a banquet in his honor, Hotel Continental (now a Westin), Paris, 1883. It is said that the phrase is an adaptation of "More powerful than an invading army is an idea whose time has come."
- Bill Gates, "The Next Outbreak? We're Not Ready," TEDTalk, TED2015: Truth and Dare, Vancouver, Canada, 16–20 March 2015. www.ted.com/talks/bill_gates_the_next_ outbreak_we_re_not_ready?language=en, accessed 30 March 2020.
- Ed Yong, "How the Pandemic Will End," The Atlantic, Atlantic Monthly Group, 30 March 2020. www.theatlantic.com/health/archive/2020/03/how-will-coronavirus-end/608719, accessed 1 April 2020.
- SARS stands for severe acute respiratory syndrome, and MERS for Middle East respiratory syndrome. James Hamblin, "You're Likely to Get the Coronavirus," The Atlantic, Atlantic Monthly Group, 24 Feb. 2020, updated 25 Feb. 2020. www.theatlantic.com/health/ archive/2020/02/covid-vaccine/607000; and Emma Graham-Harrison, "Experience of SARS a Key Factor in Countries' Response to Coronavirus," The Guardian, Guardian News and Media Ltd., 15 March 2020. www.theguardian.com/world/2020/mar/15/experience-ofsars-key-factor-in-response-to-coronavirus, both accessed 1 April 2020.
- Karson Yiu, "Wuhan Is Claiming a Coronavirus Turnaround, But Doubts Linger," ABC News, ABC Internet News Ventures, 31 March 2020. abcnews.go.com/Health/coronavirusturnaround-wuhan-back/story?id=69894804, accessed 6 April 2020.
- Brian Magierski, e-mail to Hilary Carter, 2 April 2020, 7:54 a.m.
- Anthony Cuthbertson, "China Invents Super Surveillance Camera That Can Spot Someone from Crowd of Thousands," The Independent, Independent News and Media Ltd., 2 Oct. 2019. www.independent.co.uk/life-style/gadgets-and-tech/news/china-surveillancecamera-facial-recognition-privacy-a9131871.html, accessed 6 April 2020.
- Amy Gunia, "China's Draconian Lockdown Is Getting Credit for Slowing Coronavirus. Would It Work Anywhere Else?" Time, Time USA LLC, 13 March 2020. time.com/5796425/ china-coronavirus-lockdown, accessed 6 April 2020.

- Sarah Dai, “Hangzhou Park Security Uses AI-powered Smart Glasses to Detect People with Fever,” South China Morning Post, Alibaba Group, 26 March 2020. www.scmp.com/ tech/gear/article/3077122/hangzhou-park-security-uses-ai-powered-smart-glassesdetect-people-fever, accessed 6 April 2020.
- Elaine Ou, “Apps to Track Infections Can Speed Return to Normal Life,” Bloomberg Opinion, Bloomberg LP, 2 April 2020. www.bloomberg.com/opinion/articles/2020-04-02/ covid-tracking-apps-won-t-create-surveillance-state?srnd=opinion&sref=82tKgOA7, accessed 6 April 2020.
- Shawn Yuan, “How China is Using AI and Big Data to Fight the Coronavirus,” Al Jazeera News, Al Jazeera Media Network, 1 March 2020. www.aljazeera.com/news/2020/03/chinaai-big-data-combat-coronavirus-outbreak-200301063901951.html, accessed 6 April 2020.
- George Thompson, “This is How China Beat the Corona Virus. Should We Copy?” YouTube. com, Google LLC, 19 March 2020. www.youtube.com/watch?v=0W0B2Qg3r2k, accessed 6 April 2020.
- “China Focus: Blockchain Technology Improves Coronavirus Response,” edited by Huaxia, Xinhua, Central Committee of the Communist Party of China, 17 Feb. 2020. www. xinhuanet.com/english/2020-02/17/c_138791795.htm, accessed 2 April 2020.
- “China Focus: Blockchain Technology Improves Coronavirus Response,” edited by Huaxia, Xinhua, Central Committee of the Communist Party of China, 17 Feb. 2020. www. xinhuanet.com/english/2020-02/17/c_138791795.htm. According to BraveNewCoin, “VestChain was accused of being a scam after it was found that [its] website listed fake employees and team members who did not exist. VestChain latter commented that this was an accident and that it was simply a ‘test’ of the website page.” bravenewcoin.com/ data-and-charts/assets/VEST/summary, accessed 2 April 2020.
- Steve Lohr, “Calls Mount to Ease Big Tech’s Grip on Your Data,” New York Times, New York Times Company, 25 July 2019. www.nytimes.com/2019/07/25/business/calls-mount-toease-big-techs-grip-on-your-data.html, accessed 6 April 2020.
- Kevin Granville, “Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens,” New York Times, New York Times Company, 19 March 2018. www.nytimes. com/2018/03/19/technology/facebook-cambridge-analytica-explained.html, accessed 6 April 2020.
- Edward C. Baig, Nathan Bomey, and Janna Herron, “What’s the Cost of Data Hacks for Customers and Businesses?” USA Today, Gannett Company, 30 July 2019. www.usatoday. com/story/tech/2019/07/30/capital-one-data-breach-2019-what-cost-you/1869724001, accessed 6 April 2020.
- Blockstack, n.d. blockstack.org, accessed 6 April 2020.

- Civic, n.d. www.civic.com, accessed 6 April 2020.
- Sovrin, Sovrin Foundation, n.d. sovrin.org, accessed 6 April 2020.
- "Hyperledger Indy," Hyperledger, The Linux Foundation, n.d. www.hyperledger.org/ projects/hyperledger-indy, accessed 6 April 2020.
- Connect.Me, Evernym Inc., n.d. connect.me, accessed 6 April 2020.
- "A Global Movement to End Corona Virus," EndCoronaVirus.net, n.d. endcoronavirus. net/#, accessed 6 April 2020.
- "A Global Movement to End Corona Virus," EndCoronaVirus.net .
- "Guidelines," EndCoronaVirus.net, n.d. endcoronavirus.net/guidelines, accessed 6 April 2020.
- "Blockchain-based Donation Tracking Platform Launched in China," edited by Huaxia, Xinhua News, Central Committee of the Communist Party of China, 10 Feb. 2020. www. xinhuanet.com/english/2020-02/10/c_138771526.htm, accessed 2 April 2020.
- "China Focus: Blockchain Technology Improves Coronavirus Response," edited by Huaxia, Xinhua, Central Committee of the Communist Party of China, 17 Feb. 2020. www. xinhuanet.com/english/2020-02/17/c_138791795.htm, accessed 2 April 2020.
- . Andrew "Andy" Spence, "Blockchain and the Chief Human Resources Officer: Transforming the HR Function and the Market for Skills, Talent, and Training," foreword by Don Tapscott, Blockchain Research Institute, 29 Jan. 2018. www.blockchainresearchinstitute. org/project/blockchain-and-the-chief-human-resources-officer .
- "COVID-19: How to Register," College of Nurses of Ontario, 31 March 2020. www.cno.org/ en/trending-topics/covid-19-faqs, accessed 31 March 2020.