البرنامج الوطني للذكاء الاصطناعي

NATIONAL PROGRAM FOR ARTIFICIAL INTELLIGENCE

United Arab Emirates

BLOCKCHAIN GUIDE

FOREWORD

The fast pace of technological advancement is forcing countries to take action to ensure the latest innovations are responsibly incorporated into their societies. The countries that lead in the future are those taking these actions today. Under the guidance of our nation's visionary leadership, the UAE has emerged as a significant hub for innovative ideas that will shape the future. The country is building itself into an incubator for future technologies.

A commitment to blockchain technology in all sectors of society is a critical part of this transformation. Blockchain technology is part of the digital infrastructure that will underpin tomorrow's society. The UAE was one of the first countries to embrace blockchain to improve the work of government, reduce paper waste and develop the best possible experience for citizens and residents.

In 2018, the government launched the UAE Blockchain Strategy 2021 with plans to move 50% of applicable government transactions to digital transactions by 2021. When completed, the UAE Government will save 398 million printed documents annually, 77 million annual work hours and billions in transaction costs. While the UAE has embraced this exciting new technology, much of Blockchain's global potential remains largely untapped.

Blockchain offers a promising new approach to digital transactions, producing secure, verifiable and indelible records. Robust and secure systems using blockchain increasingly facilitate everything from commerce to city governance.

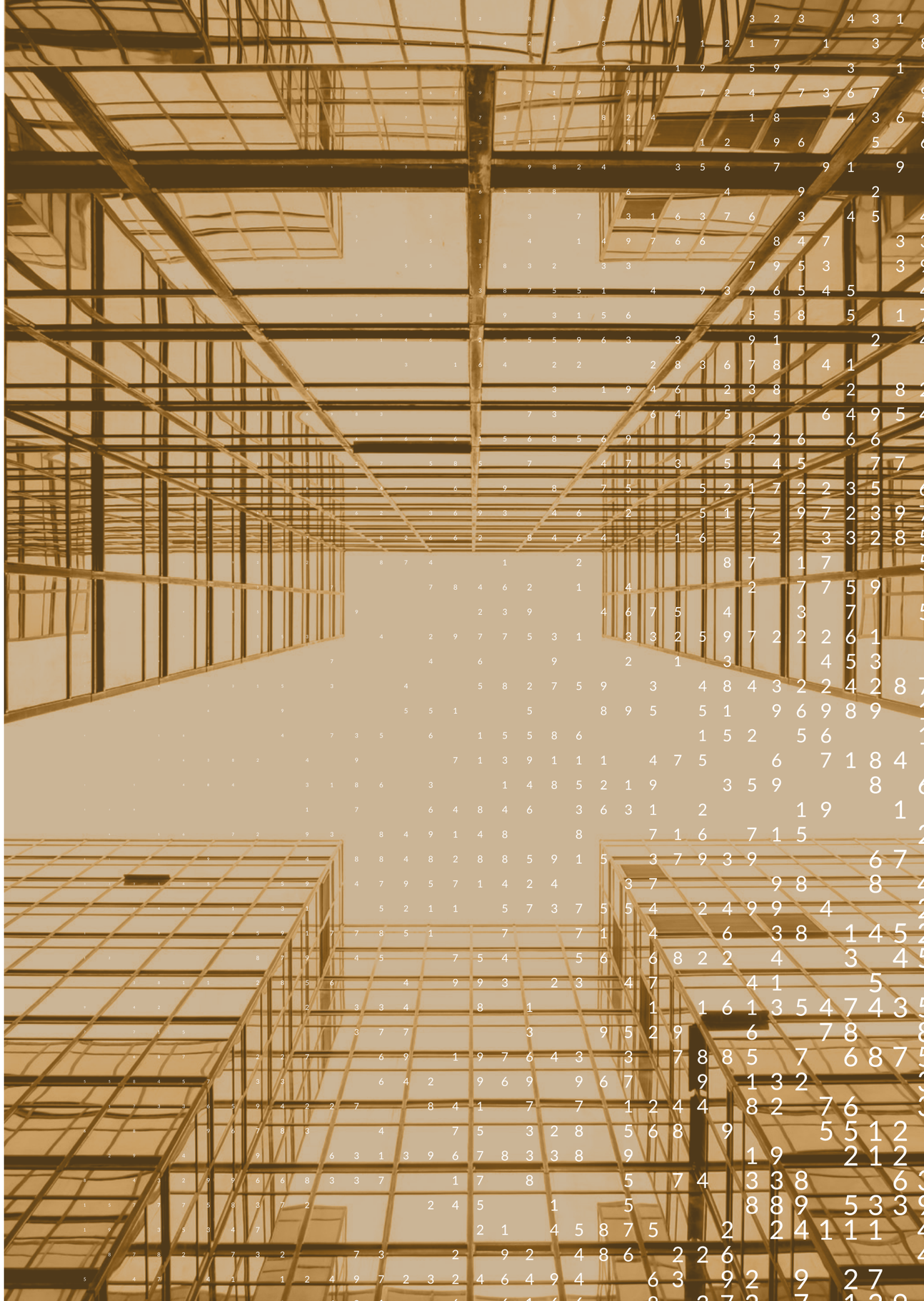
This guide breaks down each step in a blockchain transaction, helping business leaders and individuals to understand how blockchain can benefit society and themselves. It then considers how the technology has been used in practical applications.

The guide also outlines challenges facing blockchain's implementation. There remain significant uncertainties about the final form of this technology and how it will become widely adopted. In the UAE, we see this as an opportunity for the government to help shape a technology's growth – so that it produces the greatest value for society.

The evolution of blockchain is anything but straightforward. Conceived by contemporary cyber rebels, refined by brilliant coders, and driven forward by innovators who sense its endless potential, the future of blockchain is being written today. Building on the UAE's early adoption of blockchain, this guide is a first step into the exciting technology. It is our hope that you will take this first step with us, so we can fully embrace the potential of this powerful new technology.

H.E. Omar Sultan Al Olama
Minister of State for Artificial Intelligence

CONTENTS



1. INTRODUCTION & OVERVIEW

1. INTRODUCTION & OVERVIEW

Over the last decade, a radical new technology has started to force a collective rethink on the potential of the internet. Not the iPhone, nor social media or the Internet of Things, it is blockchain that some have called the new internet.

A technology that enables the development of decentralized and distributed applications in a trustless environment.

Blockchain will not replace our databases, programming languages, internet protocols, cloud computing, caches, cryptography, firewalls, servers, or anything that can be used to make an application. But, it can be the thread that weaves them together across markets, industries, and nations.

While more people are becoming aware of the potential of blockchain, few until now have grappled with the practicalities of the technology. Despite its hype, blockchain has been found most useful as an unglamorous technology that operates behind the scenes, often to streamline administrative processes and reduce costs. This gulf in understanding is slowly shrinking as major industries, governments, and individuals are becoming aware of the technology's strategic importance and publicly embracing blockchain platforms.

One of blockchain's biggest innovations is decentralizing trust. The technology hit the mainstream at a time when trust was in short supply. The global financial crisis in 2008 tested the foundations of the global economic establishment.

Bitcoin, a blockchain application, is "A purely peer-to-peer version of electronic cash that allows online payments to be sent directly from one party to another without going through a financial institution." – Satoshi Nakamoto. Satoshi went on to create a technology with the aim to unchain online transactions from the shackles of third parties.

Blockchain is an experiment in redefining trust for the contemporary internet and in the modern marketplace.

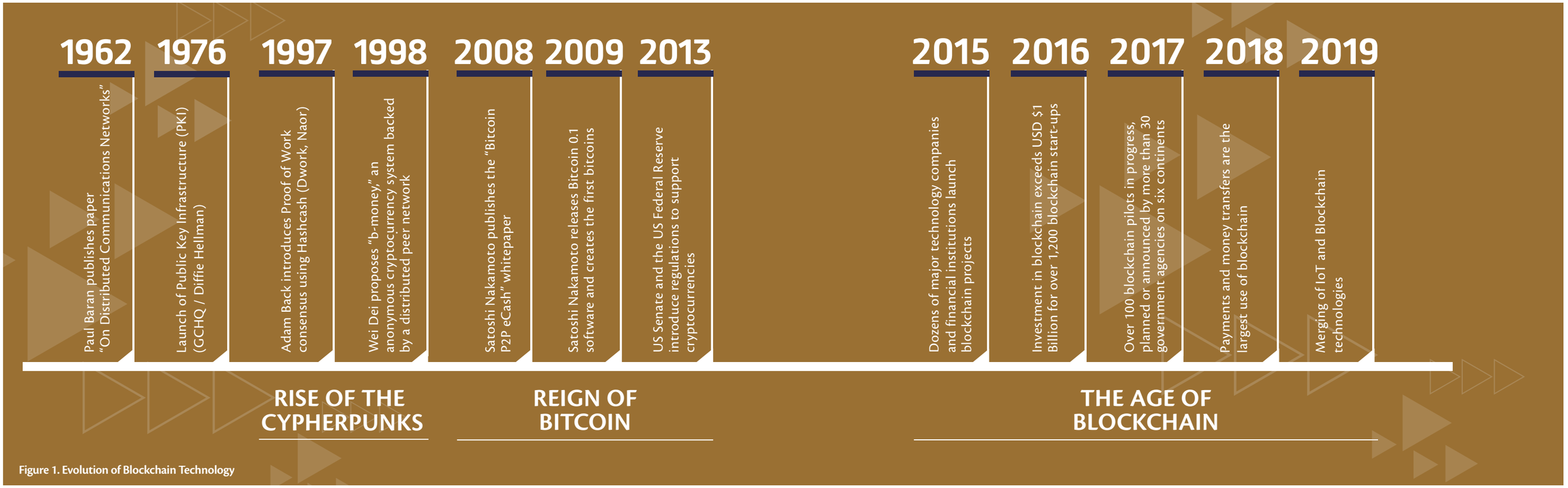


Figure 1. Evolution of Blockchain Technology

1. INTRODUCTION & OVERVIEW

In order for the technology to live up to its potential, however, it is time to move past theory and speculation and forge ahead with implementation. There are a growing number of trials of blockchain around the world, led by governments and companies that have recognized the potential of blockchain to make the world a better place. The future of blockchain is being written now.

1.1 A BRIEF HISTORY OF BLOCKCHAIN

As a young researcher working for the non-profit American research institution RAND in the early 1960's, Paul Baran introduced a critical paper describing how decentralized communication networks could withstand a nuclear attack (Figure 1). Instead of communications going through a central point, which could be disabled in a war or taken over by a hostile entity, Baran argued that distributed communication points in a decentralised structure would have the best chance of survival. Although the evolution of the modern internet took a different course, Baran's paper became instrumental in the development of the distributed networks that are critical to blockchain systems.

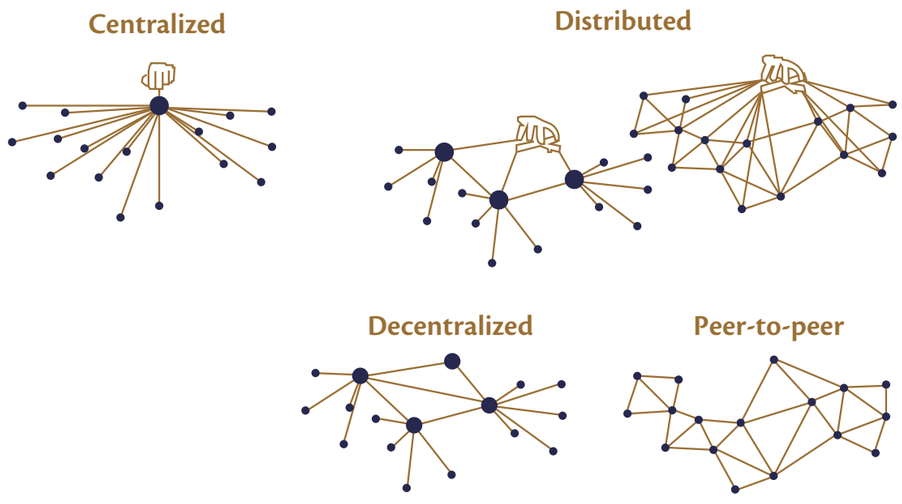


Figure 2. Centralized, Distributed and Decentralized Networks

A group of computer scientists and programmers calling themselves the Cypherpunks came together in the 1980s to establish a distributed and independent monetary system, based on the utopian values of the early internet. Over two decades, this group assembled the building blocks of a decentralized, distributed, anonymous and tamper-proof digital exchange (Figure 2).

The global financial crisis of 2008 gave new urgency to their mission. On October 31st, 2008, a person or group of persons by the name of Satoshi Nakamoto released a white paper outlining a cryptocurrency operated on a blockchain platform. It had no central authority or mint, was run on a peer-to-peer authentication platform and featured anonymous participation. The Cypherpunks' dream was realized in Bitcoin.

Before Bitcoin, there were several earlier attempts at cryptocurrency in the 1990s with varying degrees of success, most notably eCash and b-money.

The success of any currency pivots on trust. Users must believe that the currency will be accepted as tender for goods and services and that the marketplace has enough controls to keep fraud out. Bitcoin's early challenge was to earn the public's trust while demonstrating that its currency was reliably redeemable. It remains to be seen if Bitcoin is either a stable store of value or reliably redeemable.

Bitcoin's legacy is not its digital currency but rather the blockchain network that supports it. When the price of Bitcoin surged in 2017, blockchain technology had its global moment. Blockchain is now part of the international conversation on new technologies. And, everyday more people are getting exposed to its potential and possibility to transform digital transactions and record keeping systems.

1. INTRODUCTION & OVERVIEW

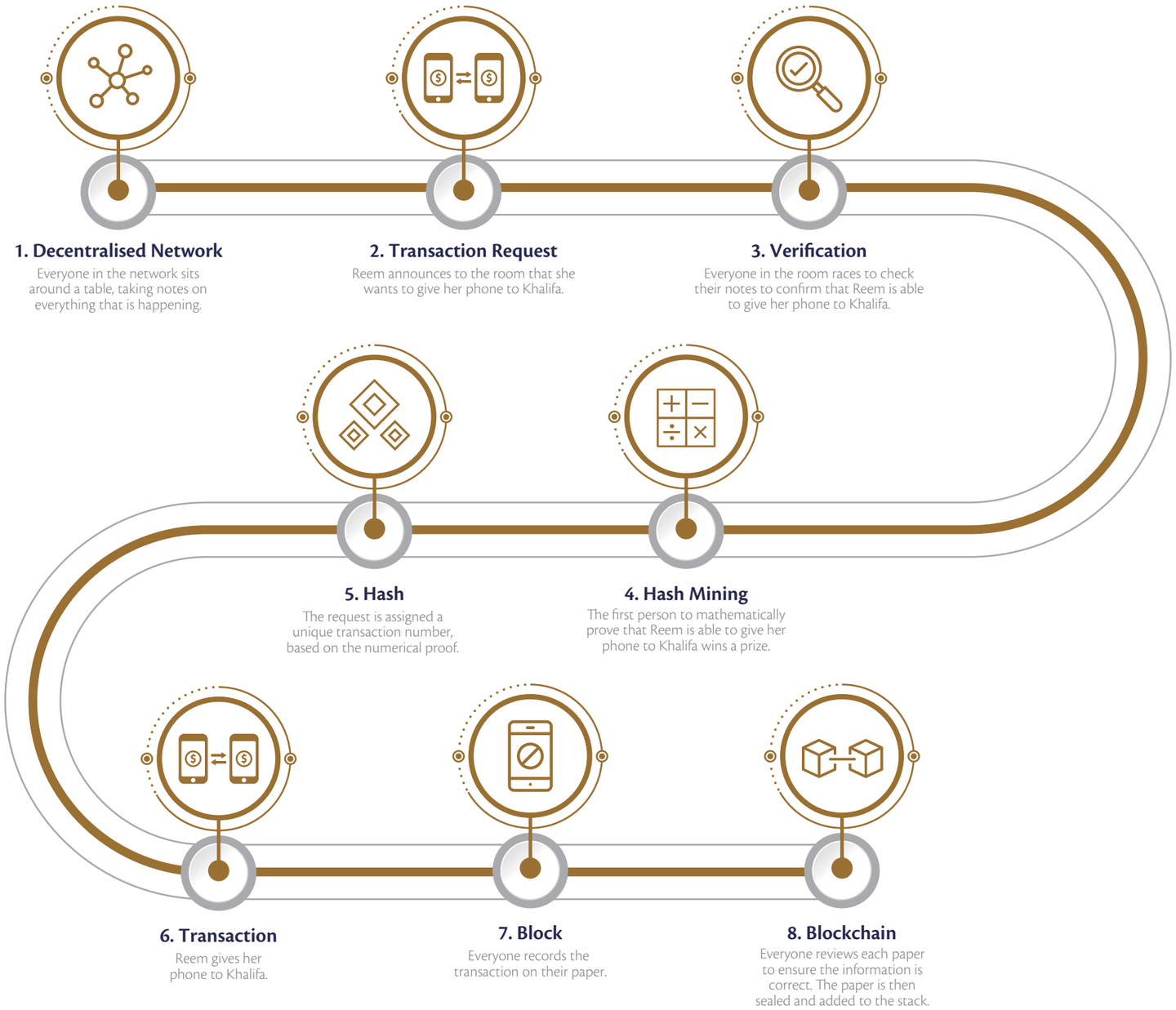


Figure 3. How Blockchain Works

1.2 KNOW YOUR BLOCKS AND CHAINS

Blockchain is a type of data structure, where data is arranged into groups of "blocks" containing information. Each block stores a reference of the block that came before it, forming a "chain". This chain of data is replicated amongst many participants, thus forming a distributed, and resilient shared store of information. It is a technology that enables the development of decentralized and distributed applications in a trustless environment.

While there are myriad applications for blockchain beyond cryptocurrency, unpacking a Bitcoin transaction is a useful starting point to understand how blockchain works.

For a Bitcoin, the first step is mining or creating a coin (Figure 3). Once a computer is connected to the Bitcoin network and generated a bitcoin wallet address, it can start mining. Mining happens any time a bitcoin transaction is requested on the network. In order to complete the transaction, a unique hash needs to be assigned to each request. To create that hash, every computer connected to the network competes to solve a math problem.

With bitcoin in hand, it is time to spend it on something. The first step is to set up a personal wallet. The wallet is a unique ledger protected through a public key infrastructure to keep the owner's identity anonymous. The ledger tr acks how many bitcoins the owner — and everyone else on the network — has to spend by recording every transaction ever made. Functionally, it is similar to a traditional cheque book, except that it is readable by everyone on the network.

Every exchange of bitcoin begins with a transaction request. When a transaction is requested, a new 'block' is created that contains all of the details of the transaction. Blocks are made up of many transactions. Block creation is tied to units of time (about every 10 minutes). In this important sense, a Bitcoin blockchain block is not really

1. INTRODUCTION & OVERVIEW

like a row in a cheque book because the block is comprised of lots of transactions from multiple users. The block is assigned a new hash that is mathematically verifiable as unique. Blocks can also be limited in size (Bitcoin blocks, for example, are 2MB). This is one of the inherently limiting functions of Bitcoin's slow transaction processing time and the high fees on the network. A feud over the block size led to the hard fork and the creation of Bitcoin Cash, which has a larger block size to speed transaction processing times.

Once a block is created, each participant in the network verifies that all of the details for the transaction are correct. This is done by comparing the hashes of all of the previous transactions on the ledger (for example, when money was first deposited in a wallet). This is the step that ensures the owner has enough bitcoin to complete the transaction, and that the party funds are being transferred to is able to receive them.

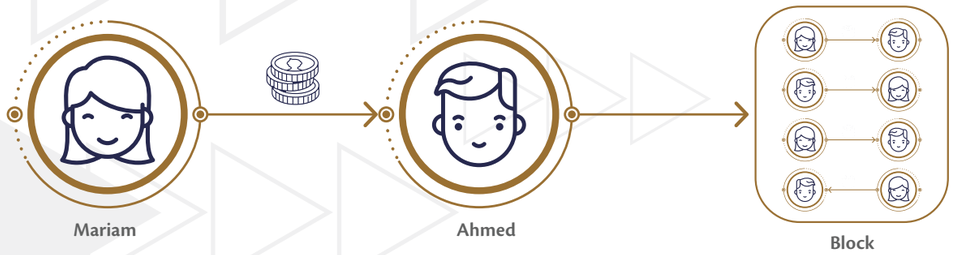
Once the network verifies the transaction, it is cleared to proceed. The funds change accounts, and the public ledger is updated accordingly. That ledger is viewable by everyone in the network, and it is made up of all of the blocks of every transaction that has ever taken place on the network. This public ledger of connected blocks bearing the complete and indelible transaction history of the network is called "the blockchain".

HASHING

The hash pointer connecting blocks of data is created by a cryptographic hash function, which takes any string of input and turns it into a unique 64-digit string of output (Figure 4). There are several varieties of hash functions that are used in different blockchains, but the principle is largely the same. The hash of each block contains the hash of the previous block; preventing any previous block tampering. If someone were to try to change the details of a past transaction, the hash of the affected block and all subsequent blocks would change (because the data changes). A change to a blockchain record is only possible if the majority (51% in case of Bitcoin) of the network agrees to the alteration, at which point a fork happens and a new chain is started.

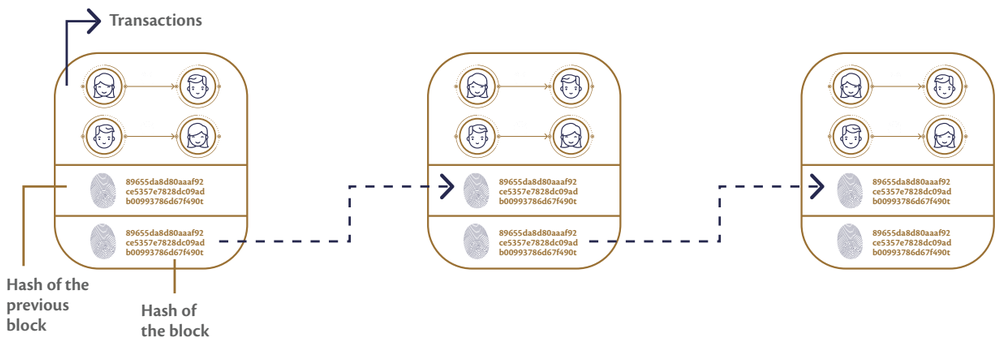
Figure 4. Hashing Algorithm

1. INTRODUCTION & OVERVIEW



Mariam sending Ahmed AED 100 is an example of a transaction in a block.
A block can contain hundreds of transactions.

A hash, like a fingerprint for the data in a block, is created and it is always unique to every block in the Blockchain. When the data in a block changes, the hash will also change.



A block also contains the **hash of the previous block**. Hence forming a chain structure.

Figure 5. Blockchain Creation
Source: Hackernoon.com

BLOCK CREATION

A blockchain is comprised of blocks of data chained together in a ledger that, taken together, maintains a complete and proven transaction history (Figure 5). For Bitcoin, that data is related to monetary transactions, but for other blockchain applications, the data could be virtually anything. Blockchains build a transaction history over time by preparing blocks of data that are cryptographically linked to the preceding and subsequent blocks. New blocks to confirm the digital signature of previous blocks to quite literally build the blockchain. One block of data wouldn't be able to stand on its own two feet because it needs to be chained to another block of data that can confirm its digital signature. Altering just one block in the blockchain invalidates all following blocks. It is important to note the role of hashing or hash function in encryption. A hash function enables encryption using an algorithm and no key. This is known as a one-way hash function because there is no way to reverse the encryption. In other words, you can't get the input from the output.

CONSENSUS MECHANISMS

Because there is no central authority in blockchain technology, establishing a general agreement on any update made to the blockchain is critical. The consensus mechanism is the process by which participants in the network are synchronized and agree on which transactions are legitimate and should be added to the blockchain. Common consensus mechanisms include **Proof of Work (PoW), Proof of Stake (PoS),** and **Proof of Authority (PoA).**

For a **Proof of Work (PoW)** mechanism, mining computers in the network compete to solve mathematically intensive puzzles that require a lot of computational power. The answer to the puzzle is called the hash, and it becomes the proof that the transactions in a block are verified and a new block can be formed. Bitcoin and Ethereum (original consensus) use PoW, and it is therefore the most widely deployed mechanism. PoW is also more vulnerable to attack because an attacker would only need to hold 51% of the mining resources to launch an attack. Recently, a successful attack on Bitcoin Cash was carried out using this strategy.

Proof of Stake (PoS) mechanisms assign the creator of the next block using a statistically randomized selection process that is tied to each participant's

1. INTRODUCTION & OVERVIEW

stake in the network. The assumption is that an individual with a higher stake in the network will have more interest in its success. Instead of having miners do the heavy lifting, PoS uses these specially tasked validators to ensure transactions are verified. However, since PoS does not take into account the validator's relative stake, it is possible that incentives are imbalanced.

Proof of Authority (PoA) attempts to address the inherent challenges of PoW and PoS mechanisms by linking stake to identity. Individuals compete to become validators. It is thought that since individual reputations are on the line, there is less incentive for foul play. PoA is also much faster since validators can use automated processes that don't require them to be constantly monitoring the verification process. Due to its speed, PoA can scale easier than the previous methods and thus has many applications for everyday blockchain use such as smart contracts and blockchain for business.

PUBLIC AND PRIVATE BLOCKCHAINS

A public blockchain is completely open and anyone can participate (Figure 6). Bitcoin is the primary example of a public blockchain. A private blockchain allows authorised entities to participate. It is a closed network and often referred to as a permissioned blockchain. Hyperledger and Enterprise Ethereum are examples of a private blockchain because it is a closed network that grants certain rights and restrictions to participants on the blockchain.

PUBLIC BLOCKCHAIN

Permissionless

Open, all participants have the same rights and same access to the information. This determines the validity of transactions and the consensus process.

High level of security as a consensus Protocol makes it impossible mathematically to falsify or reverse a transaction.

PRIVATE BLOCKCHAIN

Permissioned

Network owners have control over those who participate in the network. Members get different levels of authority based on protocols.

Overall Blockchain security is only as good as the honesty of companies checking transactions.

ACCESS LEVEL	SECURITY	TRANSACTION SPEED

Figure 6. Types of Blockchain

DISTRIBUTED LEDGER TECHNOLOGY (DLT)

Of the many innovations taking place inside the blockchain community, distributed ledger technology (DLT) is critical. Borrowing aspects such as cryptography from public blockchains, DLT is used in the corporate world to help upgrade older systems with modern ledger operations. Some larger

1. INTRODUCTION & OVERVIEW

companies are using this blockchain-like technology to upgrade their bookkeeping. The benefits of choosing DLT systems over traditional options include the fact that various compliance requirements are easier to achieve, given their robustness and flexibility to accommodate different scenarios.

SMART CONTRACTS

As interest in blockchain's power grew with the rise of Bitcoin, developers discovered new applications for the technology: contracts. Blockchain technology can be used to oversee the exchange of any contract of record. As long as the exchange could be put on a ledger and stored, blockchain can be applied. The title deed of a new home, the sale of a used car, the execution of a will, a driver's license — even a ballot vote.

This has critical implications for the business sector as well. Governments can use smart contracts to streamline the organisation of information, which in turn can air automation processes and transformations. Financial records that require a high level of security can be stored securely in smart contracts. Consider how smart contracts can revitalise public private partnership agreements and data sharing situations. The possibilities are nearly endless.

Blockchain makes the process more streamlined and reduces the need for a middleman because the contract is enforced through a cryptographic code. Not only can a blockchain record the exchange of these contracts on an indelible ledger, it can, through a decentralised network, automatically execute "contracts" as they were intended by both parties.

Consider the process of purchasing a new home. Most home buyers will take out a mortgage, which means they will need to have the mortgage loan pre-approved from the bank before making an offer on a prospective property, and the bank will require a credit score from a third-party credit-rating firm. They will likely be closing with a real estate broker, not the current homeowner.

Once an offer is made, the validation process will proceed in duplicate with the brokers and bankers on each side of the transaction filling forms and reports, and there are any number of inspections that the new owners have the right to request. These inspections will need to be approved, conducted, and recorded. When the home buyers finally reach the settlement stage, local government will step in to record the transition of ownership. Then begins the lengthy process of registering for various utilities, phone lines, internet, cable, updating addresses with the postal service, and even updating addresses for food delivery apps.

A real estate application on blockchain, utilising self-executing smart contracts, can condense this process to just a handful of steps, with banks, brokers, and the local government participating in a decentralised blockchain network with a distributed ledger. This process can't be replicated by normal digital transactions methods because trust is ensured by cryptographic proofs on a blockchain. The need for a trusted third party for verification is removed by cryptographic proofs.

1.3 DATA PROTECTION BASICS

More data is being created now than at any other time in human history. Technological advances will entail the creation of even more data. Ensuring that data is handled in a trusted and secure manner is one of the most important challenges today. Blockchain's first use case, Bitcoin, used cryptographic means to secure trust in monetary systems. Blockchain can perform similar functions for the exchange, storage and integrity of data.

Since data is not stored at a central location but spread across a network in a blockchain, the system has built-in safeguards. This decentralised nature ensures that information is unalterable, which is the first line of defence in any form of data protection. Every transaction that takes place is traceable, trackable, and accessible to anyone on a blockchain. If data is stored in a centralised server, and it is comprised in any way, then the data protection defences have essentially failed. On a blockchain network, by contrast, attackers need to compromise the majority of stakeholders on the network as opposed to one central authority to manipulate data.

Instead of storing data on private servers that render the data, the commodity of whoever owns the servers, blockchain platforms distribute the information over a peer-to-peer network in which no single computer or server can claim ownership.

2. BLOCKCHAIN TODAY

2. BLOCKCHAIN TODAY

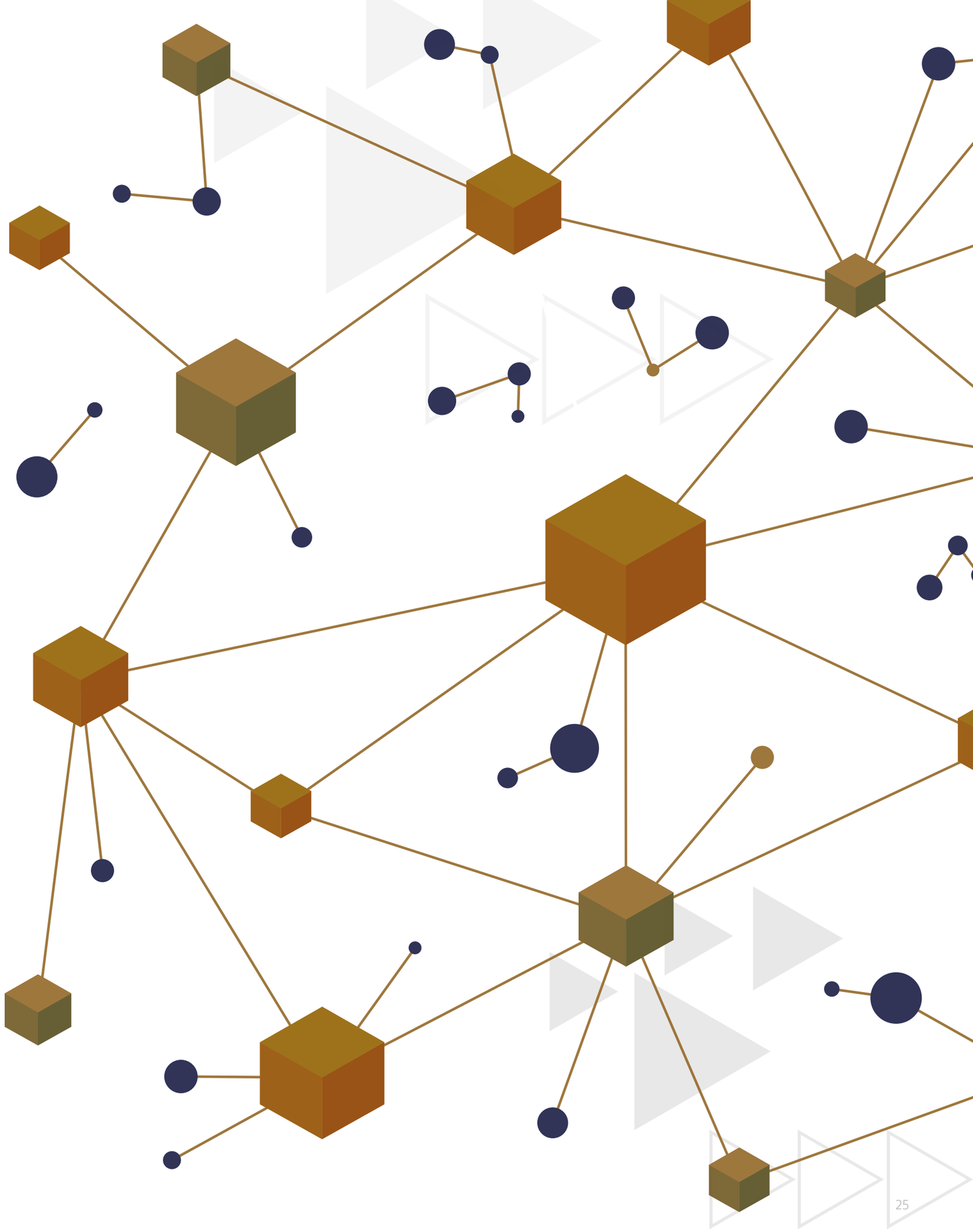
While blockchain technology was being explored several years prior by startups, corporates, and governments alike, it wasn't until the price of Bitcoin skyrocketed in 2017 that the global economy began paying real attention to the cryptocurrency and the technology underpinning it. Major financial publications now dedicate special sections to reporting on blockchain. The world's largest financial institutions have announced their own projects and consortia focused on the numerous possibilities for blockchain to transform areas such as payments, clearing and settlement, trade finance, and more.

As blockchain gained popularity, many began to take note of the projects underway before the Bitcoin price surge. The UAE Government's blockchain strategy, for example, was recognised for being ahead of the curve when the international community woke up to the power and potential of blockchain in 2017.

2.1 HOW MANY DIFFERENT BLOCKCHAIN SYSTEMS EXIST?

Given the ubiquity of Bitcoin, one could be mistaken to think that there is only one type of blockchain. In fact, there are a plethora of platforms and networks in the blockchain ecosystem (Figure 7). The original bitcoin blockchain was created in 2009 and because it was open source, the protocol was available to anyone to modify the code and start their own blockchains and cryptocurrencies.

Indeed, with the advent of the ERC20 standard for implementing tokens on Ethereum, hundreds of new coins flooded in the market in 2017 in the wake of the Bitcoin price spike. As more and more people adopted blockchain fundamentals and smart contracts to their own needs, new projects took shape that reached many other applications beyond cryptocurrency.



2. BLOCKCHAIN TODAY

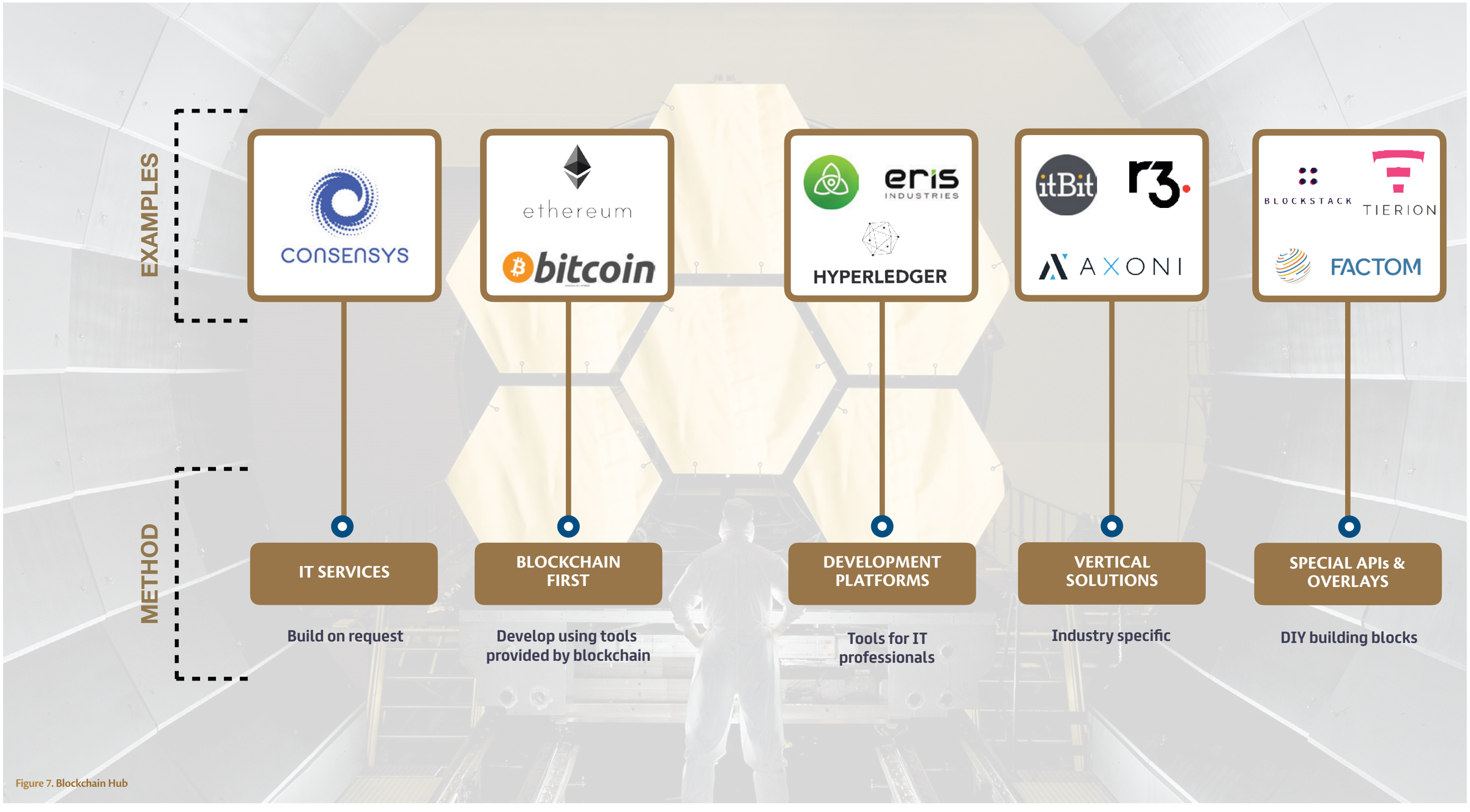


Figure 7. Blockchain Hub

2. BLOCKCHAIN TODAY

In addition to public blockchains like the one that upholds bitcoin, there are private blockchains and federated blockchains. Federated blockchains are normally used by private sector companies in the banking, energy or insurance fields among others. They operate under the leadership of a group (and are not open source like public blockchains). As such, they don't allow just any person with internet access to join the process of verifying transaction on the ledger. They are faster and more secure because of the closed contours of their programming, but they aren't used in the same widespread capacity as public blockchains. Private blockchains are further isolated and restricted to one organization or group of people. Private blockchains are a way of taking advantage of blockchain technology by setting up groups of participants who can verify transactions internally.

2.1.1 BITCOIN

Bitcoin was the original application employing blockchain technology. It was designed to enable peer-to-peer online payments through a distributed network, without the need for a financial institution acting as an intermediary. There are a finite number of bitcoins, which are mined by computers that verify the transactions and thus maintain the system as a whole. Bitcoin is an example of a public or permission-less blockchain in which anyone can participate on the blockchain.

2.1.2 ETHEREUM

Considered the second most recognized blockchain in the world, Ethereum is focused on smart contracts. Ethereum is an open source software platform built on a blockchain that facilitates decentralised applications. Ethereum is analogous to Apple's App Store, but for smart contracts on a distributed network.

Blockchain-enabled websites and platforms known as DApps facilitate the execution of smart contracts. A DApp or a decentralised application is an application that runs on a peer-to-peer network of computers instead of a single computer (Figure 8). To execute a smart contract on Ethereum's blockchain, a DApp must be completely open source, its data and records of the operation must be cryptographically stored, it must use a cryptographic token, and must generate tokens.

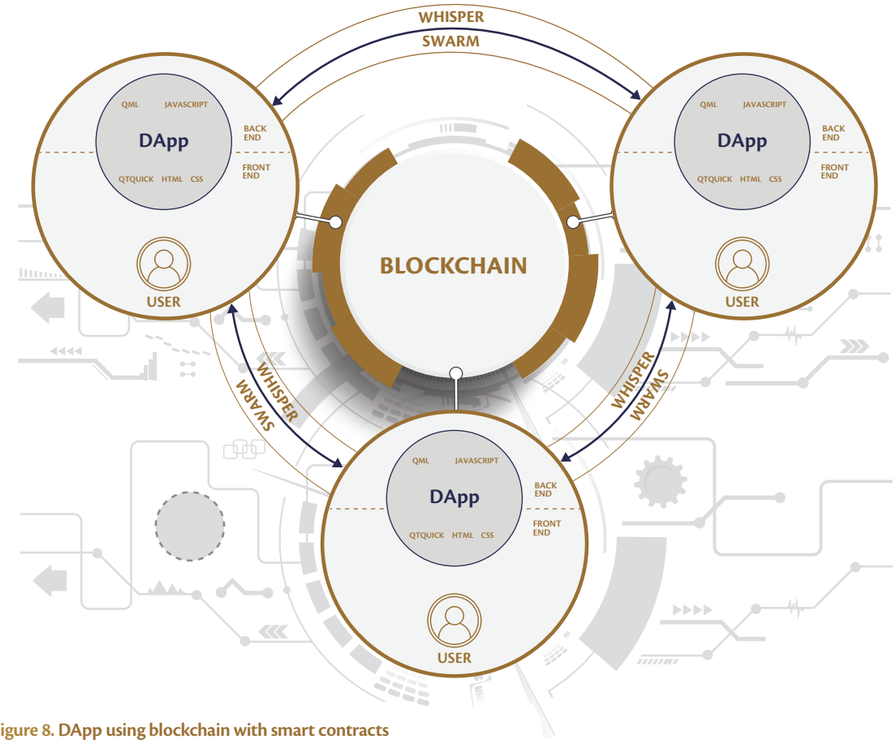


Figure 8. DApp using blockchain with smart contracts
Source: Ethereum Stack exchange

2. BLOCKCHAIN TODAY

2.1.3 HYPERLEDGER

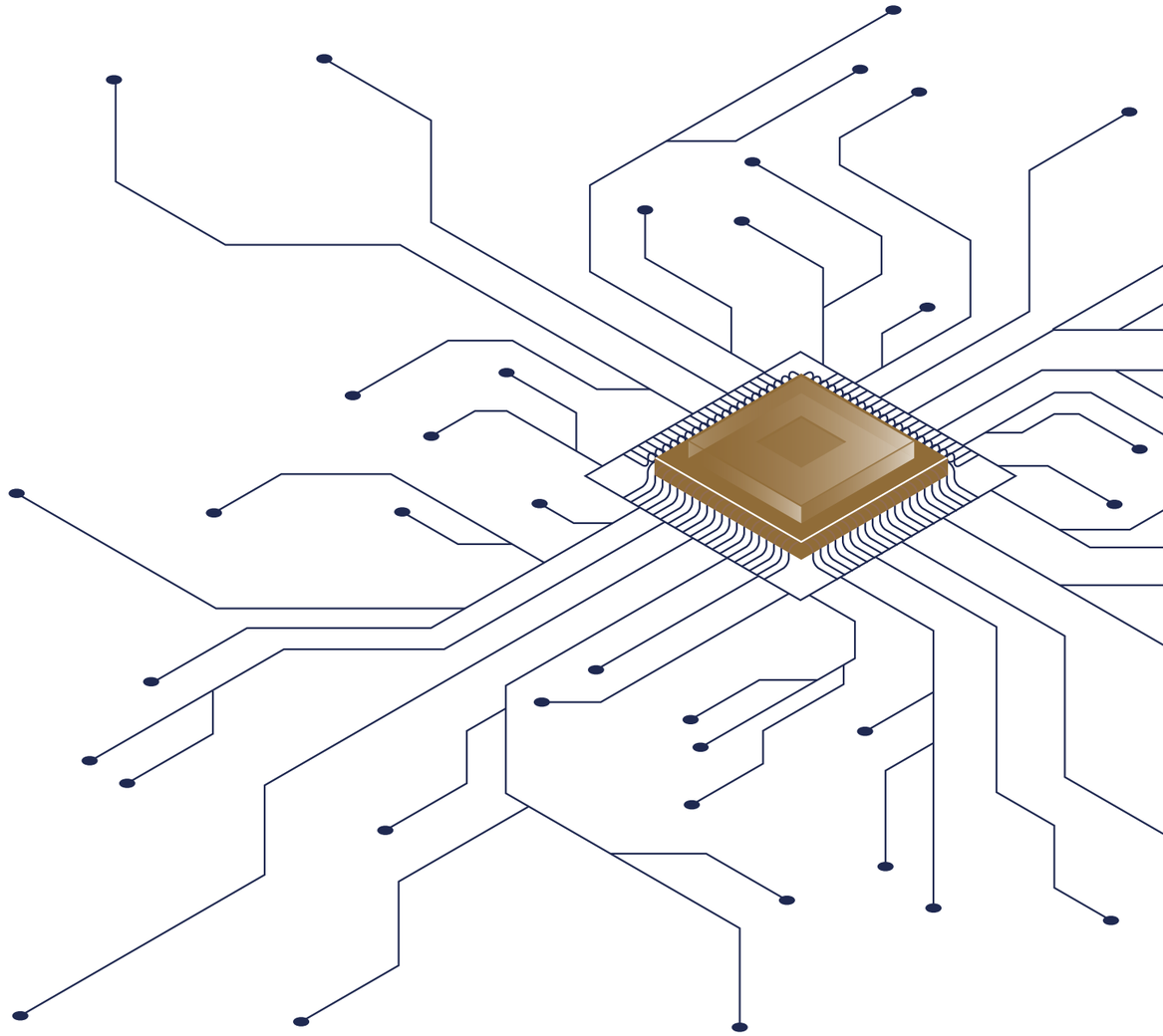
Hyperledger is an opensource blockchain hosted by The Linux Foundation on a permissioned blockchain in which only authorised parties can participate. Hyperledger enables a range of different applications from banking, finance, Internet of Things, and manufacturing. It is an open-source distributed ledger framework that can be used for industry-specific applications, platforms and hardware systems to support business transactions. By creating an enterprise-grade, open source distributed ledger framework and code base, Hyperledger is enabling businesses to harness the full power of blockchain.

Many companies contribute to the Hyperledger project. One of the companies is working on developing a blockchain called Hyperledger Sawtooth, which tests the functionality of a new consensus mechanism called Proof of Elapsed Time (PoeT) and which allows an enterprise to run and maintain distributed ledgers without a central authority. If applied to the seafood supply chain, for example, the blockchain can help track a fish's journey from sea to table.

2.1.4 OTHER PLATFORMS

Among the many other platforms to consider in this section, Quorum and Corda highlight the division between task-oriented and general purpose blockchains. In a task-oriented blockchain, the technology is used for a narrowly defined process. General purpose blockchains can be used for a wide variety of solutions, including large scale cryptocurrencies. Quorum, a commercial blockchain service operated by JPMorgan, is an enterprise-class distributed ledger that facilitates the creation of smart contracts, among other actions. The fully managed blockchain suite was recently integrated into Microsoft's Azure, as part of Microsoft's push into the blockchain ecosystem.

Corda is another platform geared toward businesses. Corda claims to have started the third wave of blockchain technology that allows a variety of applications to interoperate on one global platform, where only interacting parties can see the data within an agreement or transaction. While smart contracts are an important leap forward in business applications of blockchain, the second wave of blockchain platforms came with restrictions that prevented broad adoption by businesses. Corda declares that it delivers better privacy, transaction finality, identification standards, and the ability to scale to billions of daily transactions.



2. BLOCKCHAIN TODAY

2.2 APPLICATION OF BLOCKCHAIN

While Bitcoin deserves its reputation as a premier blockchain use case, cryptocurrencies are only the beginning of the possible applications for blockchain.

Even today, people are finding new ways to use blockchains that will have a profound impact across industries and geographies.

Determining when to use a blockchain for a business doesn't need to be a difficult task. Outlined in Figure 9 called "blockchain checklist", one must start by asking a set of simple questions based on guidelines created by the World Economic Forum.

For example, are you trying to remove intermediaries or brokers? Are you working with digital assets as opposed to physical assets? If the answer is yes, then you need to ask a second set of questions as the visual lays out. How important is trust in your

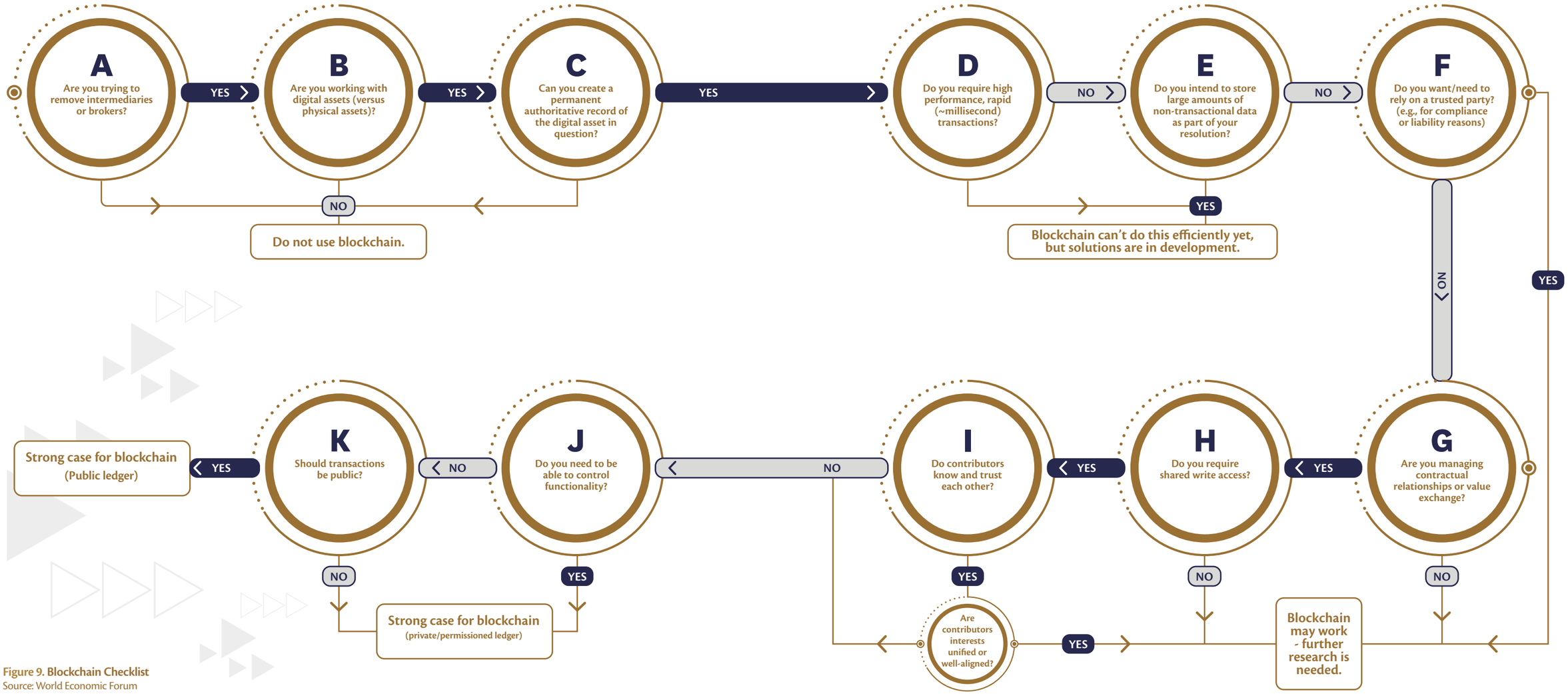


Figure 9. Blockchain Checklist
Source: World Economic Forum

2. BLOCKCHAIN TODAY

estimation? Do you need rapid transaction speeds? Again, if the answer is yes, then the case for a blockchain becomes stronger. Ultimately once one finds themselves with a strong case for a public or private blockchain depending on their specific use case, further consultation is required to ensure best outcomes.

2.2.1 GOVERNMENT

From Canada to Kenya, governments around the world are using blockchain technology to make government services more streamlined, transparent, and effective. In countries like Japan, the government has strongly backed favourable regulation for cryptocurrencies. While others, such as Spain and Australia, have invested in blockchain initiatives to help the finance sector. The government of Estonia uses blockchain to achieve 100% electronic billing in healthcare.

While blockchain information is protected by a secure and decentralised network, it also adds the benefit of having government data available to be accessed quickly with much flexibility. This can help in boosting the efficiency of governmental work and increase the efficiency by reducing the resistance when accessing information across different branches of government and private entities.

The UAE's interest in blockchain technology indicates how and why blockchain has a role to play in the future of government. In early 2016, a group of information and financial technologists and public officials convened on the sidelines of the World Government Summit in Dubai to discuss a new technology that had the potential to disrupt the digital landscape of the city – blockchain. With momentum behind the platform having reached a tipping point, the Global Blockchain Council was formed.

The council soon launched Dubai Blockchain Strategy with the aim of developing a local blockchain industry with global reach. The Smart Dubai Office, the government entity charged with overseeing Dubai's Blockchain ambitions, set itself the goal of making Dubai the Blockchain capital of the world by 2020. A goal it reached 13 months later, where in November 2017, Dubai was named the "First Smart City on the Blockchain" by the Smart City Expo and World Congress in Barcelona.

The Blockchain Challenge, hosted in 2017 by Smart Dubai in collaboration with the Washington, D.C.-based start-up accelerator 1776, attracted 20 teams from all over the world, while the government's Dubai Future Accelerators programme has had 13 government and private entities join the programme for the purpose of bringing cutting-edge startups to Dubai to explore emerging technologies such as blockchain. Led by these two initiatives, Dubai has positioned itself as the testbed for global blockchain solutions: designed in Dubai, made for the world.

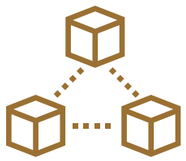
The Blockchain Challenge continued as an annual event in 2018 and 2019. The latest edition of the event received 700 applications from 79 countries. The growth of the event is a testament to the UAE's central position as a world hub for blockchain technology.

Dubai's Crown Prince Sheikh Hamdan bin Mohammed has issued a challenge to Smart Dubai to move all viable government transactions to blockchain by 2020, effectively turning the government paperless. Meanwhile, the Dubai Blockchain Strategy aims to establish more than 1,000 new businesses and solutions using the technology, thereby cementing Dubai's position as a global hub.

The UAE Government launched the UAE Blockchain Strategy 2021 (Figure 10) in April 2018. The goal is to move 50% of government transaction onto a blockchain platform by 2021, which will save an estimated AED 11 billion in transaction and document costs, 398 million printed documents annually, and 77 million working hours annually.

Dubai has already passed several milestones on its blockchain path.

2. BLOCKCHAIN TODAY



50%

Government transactions on federal level will use blockchain technology by 2021.

AED11

billion saved annually

Document transactions and documents

77

million saved annually

Hours of work

389

million

Reduction in number of government documents

1.6

billion

Reduction in kilometres spent driving

Figure 10. UAE Blockchain Strategy

In an effort to improve tracking and visibility in one of the world's busiest ports, Abu Dhabi port has locally built SILSAL, the first blockchain-based solution in the ports industry. Built on a blockchain using digital technology and smart contracts, SILSAL enables the tracking of cargo without point-to-point integration.

The UAE is also using blockchain to sharpen the financial regulation industry. The Abu Dhabi Global Market, one of the Middle East's leading financial centres, created one of the industry's first Know Your Customer (KYC) utility projects built on a blockchain. The project will streamline the regulation process by giving all parties information about the customer.

In 2017, Abu Dhabi Securities Exchange became the first financial market in the Middle East and North Africa to use blockchain technology in its services. Blockchain allows companies to share information such as statements with investors in real time and enables simultaneous e-voting through the internet from any location in the world.

All eyes will be on Dubai when it hosts the World Expo in 2020, with more than 20 million visitors expected. Here, Dubai is looking to radically streamline the experience for Expo visitors by collaborating with international partners to move much of the immigration and arrival process onto blockchain.

Dubai has already passed several milestones on its blockchain path. Six Dubai Government entities taking part in the Dubai Paperless Strategy reduced their paper usage by 57% as part of phase one of the project. In addition to limiting the government's use of paper, Smart Dubai launched the payment reconciliation and settlement system in September 2018 to enable a blockchain-powered upgrade to Dubai's financial system.

Blockchain technology is also being introduced into the Dubai Department of Finance so that staff members no longer have to physically go through payments collected from various portals and manually reconcile them. In this case, blockchain is a promising technology to yield huge time savings, and offer flexibility to accommodate various scenarios and requirements.

2. BLOCKCHAIN TODAY

One of the most interesting examples of the UAE's approach to incorporating Blockchain technology is at the Dubai Land Department (DLD). The government entity is using blockchain to improve service, collaboration with other parties involved with the real estate market and create secured assets. One such example in action is the ability of DLD to write end-to-end property transactions on to a real estate blockchain so that all participants involved in a given transaction have access to the pertinent information.

With blockchain implementations well underway, the UAE government is focused on the governance and legislation standards needed to effectively promote and regulate blockchain solutions. The opening of a new World Economic Forum (WEF) Centre for the Fourth Industrial Revolution (C4IR) in Dubai is a testament to how far the UAE is along in building its knowledge economy with blockchain at its core. The think tank focuses on blockchain logistics and how best to incorporate the technology in the work of governance and legislation. It also focuses on how to lead on legal issues related to blockchain in the global context.

WEF has created several think tanks in Japan, China, the United States, India and the UAE study the Fourth Industrial Revolution (4IR) and consider the societal impact of the shift. Dubai's centre is the latest member of the team, and it will focus on the impact of blockchain and AI on the UAE and the Middle East by working closely with governments, businesses, academics, and other organisations.

The Dubai Blockchain Center brings together thought leaders, developers, investors, and educators to advance blockchain development and adoption in the UAE. It also provides specialised courses in Arabic and English on blockchain technology. The centre is one of several educational outlets in the UAE preparing, educating, and training the next generation of blockchain pioneers. It is a vital part of the UAE's development as a leading knowledge economy.

2.2.2 CRYPTOCURRENCY

By far, the most popular and common application of blockchain technology is cryptocurrency. At their core, cryptocurrencies like Bitcoin are digital currencies that use cryptography for security. Cryptography is the established practice of writing and/or solving codes. In the modern application, cryptography is used to secure transactions, verify the transfer of assets, and maintain the overall security of a blockchain through unbreakable forms of verification. There are currently thousands of cryptocurrencies on the market with an overall market capitalization of hundreds of billions of dollars.

The UAE and Saudi Arabia are cooperating on the creation of a cryptocurrency through "Aber" project. The cross-border digital currency will be strictly targeted to banks during the pilot phase. The project aims better understand the implications of blockchain technology for facilitating cross-border payments. The project will also determine the impact of a central currency on monetary policies.

As part of its smart city vision for Dubai, the Emirate announced a partnership with Fantom, a distributed ledger technology stack that is highly skilled at scalable smart contract execution. The partnership will help Fantom create an open-source, scalable platform that will enable highly reliable infrastructure with real-time transactions and data sharing.

2. BLOCKCHAIN TODAY

2.2.3 LOGISTICS AND SUPPLY CHAIN

Due to its immutable and distributed ledger, blockchain is also transforming how logistics are conducted. As an electronic transaction processing and record keeping system that enables all parties to track information through a secure network, logistics operators from the port of Dubai to Aramex's international shipping network are moving towards blockchain systems. Blockchain pilots are underway in the timber industry, the international shipping industry, the fishing industry (Figure 11), and in the agriculture industry to track goods from provenance to their final destination.

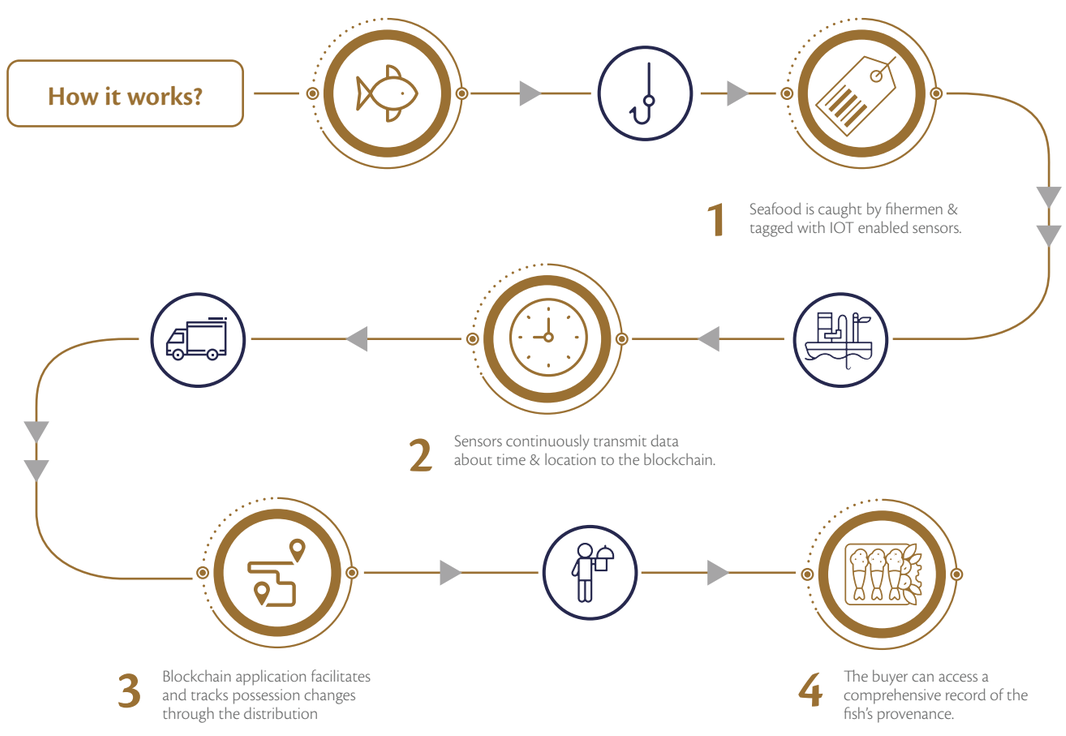


Figure 11. Smart Contract Example: Logistics and Supply Chain

The Dubai Electricity and Water Authority is working to find ways to use blockchain to innovate creatives solutions that will disrupt current electricity and water utility business models.

2.2.4 HEALTHCARE

Health records stored on a blockchain could translate to life or death (Figure 12). Imagine if individual health data was easily accessible for any doctor that might need it. This could be critical if someone walked into a hospital for an emergency, and their entire medical history was instantly available for the doctor on call. On a blockchain, life-saving medical information could be securely and safely shared across the medical sector.

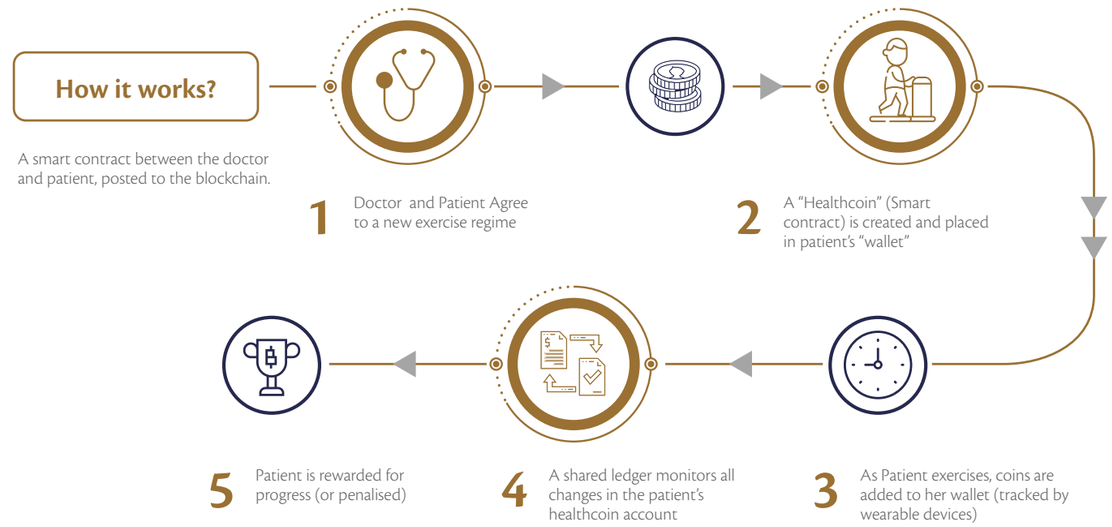


Figure 12. Smart Contract Example: Healthcoin

2. BLOCKCHAIN TODAY

2.2.5 IDENTITY SYSTEMS

From governments to private businesses, blockchain facilitates better, more efficient and secure identity systems (Figure 13). As with other applications of blockchain, identity systems benefit from the security and access credentials of the blockchain system. Major companies are working towards developing a decentralized approach to identity management systems, and to give individuals and organizations more control over their identity.

As part of the effort to digitize and completely automate the residence visa experience in the UAE across visa application, issuance and renewal, the General Directorate of Residency and Foreigners Affairs (GDRFA) has partnered with Blinking, a blockchain-based digital ID solution provider. The new authentication tool gives users complete control over their data. It is a platform for secure digital identity management, providing biometric authentication, service authorization, shareable KYC, secure data storage and private data regulatory compliance.

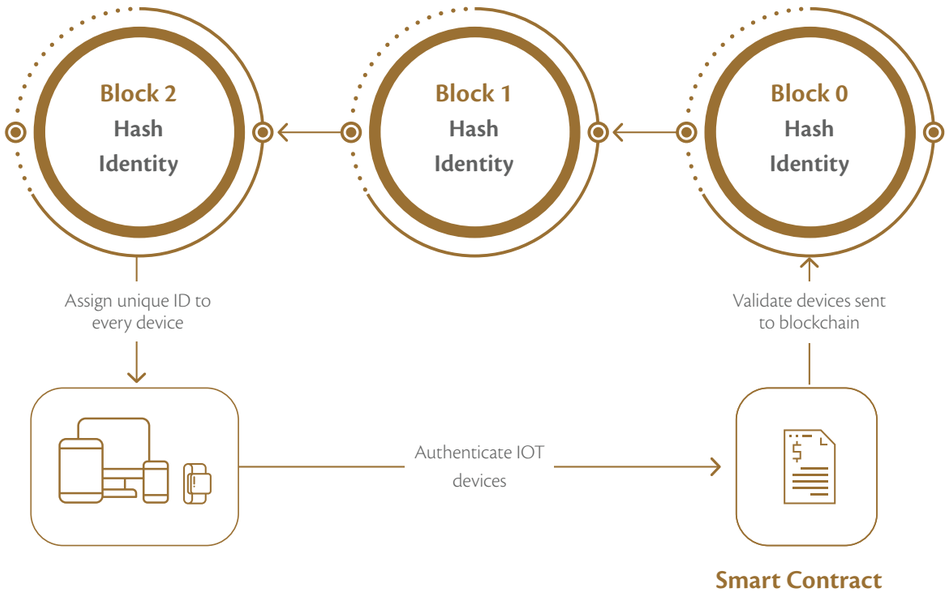


Figure 13. Smart Contract Example: Identity Management System

2.2.6 FINANCIAL SERVICES AND INSURANCE

Since blockchain went mainstream, the financial services sector has embraced blockchain technology in a big way. From creating their own cryptocurrencies to shifting critical systems to blockchain, the possibility for disruptive change is profound.

Blockchain technology promises immutability, decentralization, and transparency. In financial services, this means financial data can be effectively exchanged and managed between parties, significantly reducing reconciliation costs. Customers are able to perform financial transactions more quickly and access more of their data more easily. Similar benefits apply in the insurance industry, where administrators will also have access to data regarding premiums and rates that are automatically updated and verified using blockchain.

Emirates National Bank of Dubai (Emirates NBD) announced a unique Blockchain pilot in spring 2017. As a developing region, many of the bank's customers still prefer to transact via cheque. Rather than enforce a new consumer behaviour, Emirates NBD is piloting an integration for blockchain that allows customers to continue to write cheques, but enables the bank to instantly store the cheque data on the blockchain as soon as the cheque is deposited. Once a digital copy of the cheque is made — usually after it is deposited into a cheque deposit machine (CDM) — the bank reads the details of the cheque and stores it on the 'Cheque Chain', creating a record of the transaction.

Telecom provider Etisalat has partnered with leading blockchain solution providers Settlemint and Tradefin to innovate blockchain business-to-business solutions that will reduce transaction costs in processes between banks, government, and private entities. SettleMint provides licensed, enterprise-grade, middleware to make building blockchain applications and integrating blockchain into existing applications easy for IT teams. Tradefin provides a business to business payment and financing network on blockchain. Through partnerships such as these, Etisalat aims to reduce costs by 40% over the next five years through the use of blockchain technology.

3. CHALLENGES FACING BLOCKCHAIN

3. CHALLENGES FACING BLOCKCHAIN

The first blockchain was not perfect. Hobbyist programmers spent years tinkering with Bitcoin's blockchain to defeat bugs and improve the system. As the technology proliferated, early limitations were overcome, technological advancements made, and new applications discovered. However, blockchain remains a nascent technology, and technological and practical challenges remain.

3.1 EDUCATION AND CAPABILITIES

As terms such as "blockchain", "bitcoin", and "cryptocurrency" began emerging throughout the business world, the media did its part in publishing explainers about blockchain and cryptocurrency. Government initiatives led awareness campaigns outlining the power of blockchain to change how government functions.

Blockchain is still closely identified with cryptocurrency. While misconceptions about cryptocurrency have subsided, many still don't fundamentally understand how blockchain works, and the powerful effects technology can have in everyday life. This lack of awareness even extends to most lawmakers around the world, which is problematic because blockchain - as a new technology - needs fresh regulations to ensure that its power is used in a constructive way for society.

Because blockchain is a new field of technology, there are few individuals who understand how it works, and distinguish it from cryptocurrencies. Not to mention, there are even fewer talented enterprise-level blockchain software developers. Without proper training programs, that matches different levels (i.e. students, engineers, managers, and senior executives), there will be doubt of adoption and development in the technology even if it matures and progresses steadily.

3.2 INTEROPERABILITY

With the creation of so many types of blockchains, there is additional concern about interoperability moving forward. No standard is there to ensure that different types of blockchains can be compatible with each other and work in harmony, and lack of this standard is what raising this interoperability issue. On Github alone there is more than 6500 active blockchain projects using different languages, platforms, consensus mechanisms, and protocol schemes. This disconnection between different blockchains will add to the confusion and challenge in development and adoption of the technology, and would make decision makers think and doubt twice.

3.3 SCALABILITY

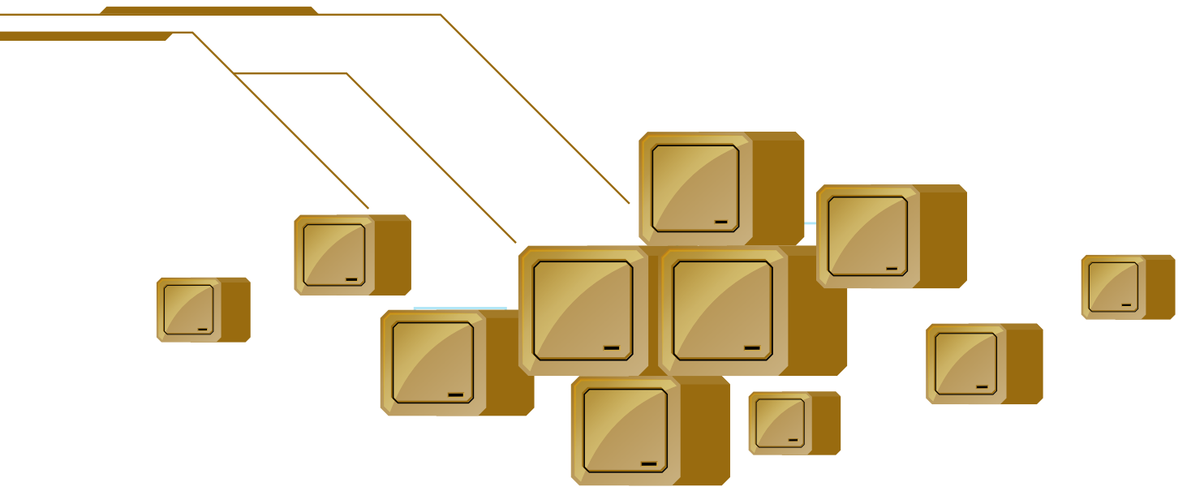
Scalability remains a critical challenge for companies and governments. The creation of scalable blockchain platforms that can adapt to the growing needs of a company or government can pose challenges with regard to implementation, cost, and training of employees. Indeed, investing in a blockchain technology today, only to have to change it afterwards due it being incapable of handling the growth of a company's transactions will halt the technology's progression. What needs to be considered here is that scalability is an inherent technological challenge for blockchains. With every transaction, the blockchain adds one more block to its ladder of transactions, and every block increases the chain size with data as the chain will contain the history of the blocks before it. As more users join the networks and the transaction histories of individual coins grow, the current system is in danger of buckling. For comparison, Bitcoin can handle approximately 60 transactions per second, while Visa's peak rate of 47,000 per second. Many solutions are being considered and tested to overcome this challenge, such as Sharding or off-chain transaction (i.e. lightning network), but one has to keep in mind that there is no free meal in this game.

3. CHALLENGES FACING BLOCKCHAIN

3.4 REGULATORY CLARITY

Considering the borderless nature of blockchain networks and their global impact, lack of consistent regulatory clarity and differences between jurisdictions may prove a challenge for burgeoning networks. As the technology advances ahead of regulations, risks and uncertainties will continue to arise. Many regulators still lack the necessary understanding of blockchain and cryptocurrencies and remain unprepared to apply a cohesive approach towards answering regulatory concerns.

Indeed, the current regulations over cryptocurrency are inconclusive and scattered. In some places, cryptocurrencies are banned completely, while others regulate their use by regulating exchanges. There are no unified international standards, and this will continue to be a challenge for the short and medium term. There are additional concerns about how best to regulate data and data ownership, but so far, there are no internationally accepted standards or codes of conduct. The efforts of the UAE and WEF to establish global standards for blockchain are a welcome move and signal how the technology is maturing.



3.5 GOVERNANCE

Governance is the establishment of policies, and continuous monitoring of their proper implementation, by the members of the governing body of an organization. It includes the mechanisms required to balance the powers of the member, and their primary duty of enhancing the prosperity and viability of the organization.

Each blockchain has its own mechanisms to modify and shape its network in order to adapt and change overtime. Because blockchain is relatively a new technology, governing it is in reality an experiment that we do not know the best recipe for yet. Moreover, adding to the problem, blockchain governance is rooted in the fact that the interests of a network's stakeholders change as they interact with and generate value from the network.

Governments and industries would need to be open and prepared to address change when needed in a way that ensures the benefit of all stakeholders without comprising the blockchain network. For example, deciding when to switch to a new consensus protocol, how to set rules for organizations joining and leaving the network, whether block sizes should be increased or not, or whether an off-chain solution should be adopted.

Different solutions are being considered and tested, mainly separated into on-chain and off-chain governance schemes (i.e. DAO). However, the core of this challenge remains in deciding the governing entities selection and classifying stakeholders. In short, it is a social problem in the digital era.

Governments and industries would need to be open and prepared to address change when needed.

4. BLOCKCHAIN'S FUTURE

4. BLOCKCHAIN'S FUTURE

By 2024, blockchain could become around an $8 Billion industry. The average person will never interact with blockchain, yet soon, blockchain could underwrite every transaction. Blockchain might be embedded within nearly every organisation on the planet in the next decade. Business, by definition, is the exchange of goods or services in fulfilment of a contract. Blockchain can regulate every step of that equation. Every stage of a business lifecycle in any sector can be enhanced by smart contracts on blockchain.

Businesses of all sizes should investigate the potential role of Blockchain in their organisation, and be ready to embrace the technology as it matures. Mass adoption will come sooner than you think.

4.1 INTERNET OF TRANSACTIONS

Take a look at the myriad applications of smart contracts. Smart contracts in the music industry can be deployed by artists to ensure their IP is protected, and to make sure they receive payment for their work whenever an album or song is downloaded. A British recording artist has emerged as a blockchain pioneer and evangelist, working to introduce the benefits of an indelible ledger and self-executing smart contracts to the music industry. Through smart contracts, musicians can automatically receive payments for a song and, as the artist has done, automatically share royalties with everyone who contributed to the making of the song.

In the art world, blockchain can be deployed to open a digital market for investors and artists, simultaneously assessing and validating the worth of an artwork, and recording the exchange of possession between artist and buyer. As forgery techniques become even more advanced, blockchain can be applied to verify the origins of artwork, helping would-be investors differentiate between an original Monet and an Artificial Intelligence copy.

Self-executing contracts on the blockchain can also dramatically reduce payment turn-around times for client work. Companies in service, design, and consulting fields who have entered into a smart contract with a client can receive payment for services within moments of the client signing a delivery note, reducing the payment processing period from weeks to seconds. And because the contract terms and transaction history are permanently stored on the blockchain, the audit trail is tamper-proof.

Businesses of all sizes should investigate the potential role of blockchain in their organisation and be ready to embrace the technology as it matures. Mass adoption is coming soon.

This is all possible because as blockchain technology matures, it will drift to the middle. It has already matured from the vision of the early internet pioneers and the libertarian Cypherpunks into something more palatable to business and government. Given its use case, it will only continue to do so.

4. BLOCKCHAIN'S FUTURE

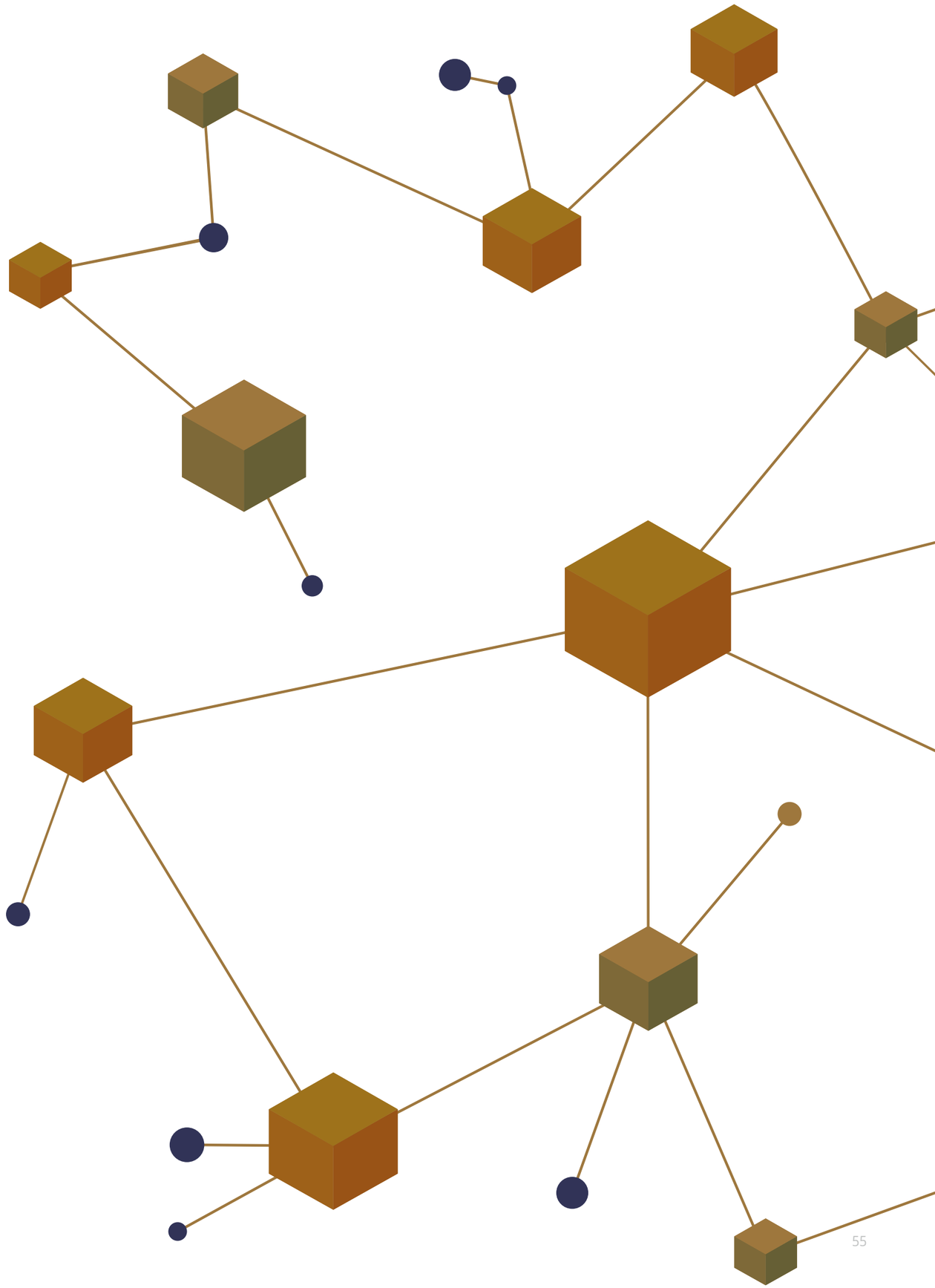
4.2 CONVERGENCE

The world is awash in data. From smartphones to the Internet of Things (IoT) devices, data fuels contemporary life and is fast becoming as valuable as oil. As the internet expands, increasing amounts of data will be required to sustain new innovation. Artificial Intelligence programmes requires massive amounts of data to function properly.

How will data be securely organised in a manner that provides quick and easy access? As the technology that enables cryptocurrencies such as Bitcoin, blockchain offers a promising new approach to digital transactions that meet contemporary requirements for a shared, verifiable, and immutable record of transactions. This is just the beginning of the wave of changes that blockchain will facilitate.

Consider the overlap in how blockchain, IoT devices, and artificial intelligence technologies can work together. An example of AI and blockchain working together is AI DAO. AI DAO could be a decentralised organisation entirely run by machines with no or limited human intervention, effectively utilizing AI, blockchain, and IoT as its building blocks.

Above all else, blockchain can put the keys to personal data back in the hands of users by demonstrating who accessed their data and when. And that is the message that blockchain can deliver: putting control back in the hands of users to enable a new era of trust in the internet. In today's connected world, trust is one of the most valuable currencies in the marketplace and blockchain just might be the new gold standard.



5. GLOSSARY

5. GLOSSARY

BLOCKCHAIN
A decentralized, distributed, and digital ledger that is used to record transactions across many computers so that any involved record cannot be altered retroactively, without the alteration of all subsequent blocks.

CRYPTOCURRENCY
A digital asset designed to work as a medium of exchange that uses cryptography to secure financial transactions, control the creation of additional units, and verify the transfer of assets.

ORACLE
Oracles are used in smart contract blockchain application. A blockchain oracle is a third-party information source that has the sole function of supplying data to blockchains which permit for the creation of smart contracts.

SIDE CHAIN
A sidechain is a separate blockchain that is attached to its parent blockchain using a two-way peg. The two-way peg enables interchangeability of assets at a predetermined rate between the parent blockchain and the sidechain. The original blockchain is usually referred to as the 'main chain', and all additional blockchains are referred to as 'sidechains'.

ON-CHAIN
On-chain transactions refer to transactions which occur on the blockchain - that is, on the records of the blockchain - and remain dependent on the state of the blockchain for their validity.

OFFCHAIN
An off-chain transaction is the recording of data or movement of value outside of the blockchain.

PERMISSIONED
Also known as private blockchains, Permissioned blockchains maintain an access control layer to restrict access and rights to certain identifiable participants.

PERMISSION-LESS
A public blockchain that is accessible to anyone.

WALLET
A cryptocurrency wallet is a software program that stores private and public keys and interacts with various blockchain to enable users to send and receive digital currency and monitor their balance.

CONSENSUS
A consensus mechanism is a fault-tolerant mechanism that is used in computer and blockchain systems to achieve the necessary agreement on a single data value or a single state of the network among distributed processes or multi-agent systems.

AI.GOV.AE

CRYPTOGRAPHY
The practice and study of techniques for secure communication in the presence of third parties

HASH FUNCTION
A hash function is any function that can be used to map data of arbitrary size onto data of a fixed size. The values returned by a hash function are called hash values, hash codes, digests, or simply hashes.

DISTRIBUTED LEDGER
A distributed ledger is a database that is consensually shared and synchronized across multiple sites, institutions or geographies. It allows transactions to have public "witnesses," thereby making a cyberattack more difficult. The participant at each node of the network can access the recordings shared across that network and can own an identical copy of it.

DECENTRALISED
The decentralized nature of blockchain technology means that it doesn't rely on a central point of control.

SMART CONTRACTS
Smart contracts are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. The code and the agreements contained therein exist across a distributed, decentralized blockchain network.

BLOCKCHAIN NETWORK/NODES
Nodes form the infrastructure of a blockchain. All nodes on a blockchain are connected to each other, and they constantly exchange the latest blockchain data with each other, so all nodes stay up to date.

DAO
A DAO (Decentralized Autonomous Organization) can be seen as the most complex form of a smart contract, where the bylaws of the decentralized organization are embedded into the code of the smart contract, using complex token governance rules.

DAPP
DApp is an abbreviated form for decentralized application. A DApp has its backend code running on a decentralized peer-to-peer network. Contrast this with an app where the backend code is running on centralized servers.

IOT
The Internet of things (IoT) is the extension of Internet connectivity into physical devices and everyday objects.

ICO
An Initial Coin Offering (ICO) is the cryptocurrency space's rough equivalent to an IPO in the mainstream investment world. ICOs act as fundraisers of sorts; a company looking to create a new coin, app, or service launches an ICO.

البرنامج الوطني للذكاء الاصطناعي

NATIONAL PROGRAM FOR ARTIFICIAL INTELLIGENCE

United Arab Emirates

AI.GOV.AE