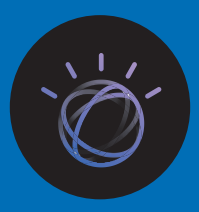
CAMBRIDGE TRADES

CAMBRIDGETRADES IBM-SMART_CONTRACT

CAMBRIDGETRADES IBM-SMART_CONTRACT

IBM Leadership

#1 AI for business
20,000+ IBM Watson client engagements across 20 industries.



#1 in hybrid cloud
47 of the Fortune 50 rely on IBM Cloud. Revenue for IBM Cloud topped $19 billion in 2018.

#1 in enterprise services
IBM Services, with end-to-end cloud and AI capabilities, closed 47 client agreements worth more than $100 million each in 2018.

#1 in enterprise security
IBM Security manages 70 billion cybersecurity events per day for clients in more than 130 countries.

#1 in enterprise systems
IBM Z is at the heart of world commerce with 30 billion transactions per day, including 87 percent of all credit card transactions.

#1 in blockchain
IBM Blockchain Platform was ranked number one by analyst firms Juniper Research and Everest Group.

#1 in U.S. patents for the 26th consecutive year
IBM inventors received a record 9,100 patents, including more than 3,000 in AI, cloud and quantum computing.

#1 and #2 fastest supercomputers in the world
Built by IBM for the U.S. Department of Energy, based on IBM POWER9 CPUs tuned for AI workloads.

That is why businesses moving to Chapter 2 will need to embrace a new, hybrid cloud approach. It is one that will allow them to more easily move data and scale AI and other applications across public, private and on-premise IT in their enterprises, with consistent management and security protocols, using open source technology.

For example, BNP Paribas, a leading European bank, is working with IBM to speed and scale the launch of new digital and AI customer services across the cloud, while protecting the security and confidentiality of customer data. Similarly, global telecom leader Vodafone Business is partnering with IBM to innovate the way it delivers multicloud and digital capabilities—including AI, edge computing, 5G and software-defined networking solutions—to its customers.

> "We are ready for this moment of moving clients to Chapter 2 of their digital reinventions with our unique integration of innovative technology, industry expertise and a reputation for trust and security earned over decades."

IBM Services provides end-to-end cloud integration capabilities and is helping thousands of businesses migrate, integrate and manage applications and workloads seamlessly and securely across any cloud environment. Industry experts from IBM Services are co-creating cloud-enabled solutions with clients in our IBM Garages. Using design thinking and agile methods, we are helping clients implement new ways of working, such as rapid prototyping and iteration to more quickly move technology projects from pilot to production at scale.

We are ready for this moment of moving clients to Chapter 2 of their digital reinventions with our unique integration of innovative technology, industry expertise and a reputation for trust and security earned over decades. IBM is now moving the world's major enterprises to the next era, an effort that will be enhanced by our planned acquisition of Red Hat.

Chapter 2 of Trust and Responsible Stewardship
We recognize that our clients and the consumers they serve expect more than groundbreaking innovation and industry expertise. They want to work with technology partners they can trust to protect their data and handle it responsibly. They want to work with partners who know how to bring new technologies into the world safely and help society benefit from them. And they want their partners to create inclusive workplaces and communities where diversity thrives.

CAMBRIDGE TRADES

CAMBRIDGETRADES IBM-SMART_CONTRACT

IBM Quantum

CAMBRIDGETRADES Quantum understanding

ExxonMobil's vice president for Research and Development, Vijay Swarup, is leading the company's exploration of quantum computing.

Every energy company's dual challenge:

Provide access to scalable, affordable energy

Reduce the risks of climate change

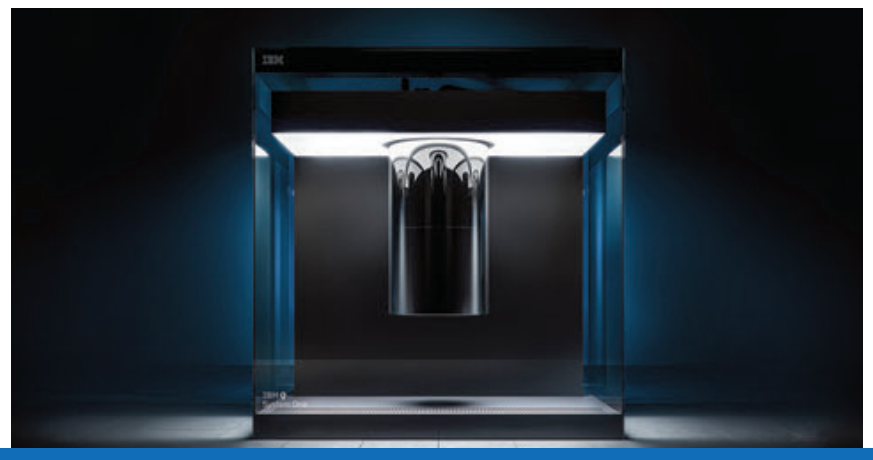
Vijay Swarup, ExxonMobil vice president for Research and Development, says energy research requires curiosity, optimism, patience and dissatisfaction. Dissatisfaction because he believes things can be better. But what, exactly, can be better? Nothing less than our understanding of the world.

Researchers now have a new tool to explore new ways to solve problems: quantum computing. And Vijay's quite precise about the trouble with our current understanding. "There are some problems so big, all we can do is approximate," he says. Whether he's in a business suit or the lab coat he wears at ExxonMobil's expansive New Jersey research facility, Vijay clearly enjoys trying to solve what he calls today's pressing dual challenge: ensuring that people have access to scalable, affordable energy, and doing so in the context of climate change and the need for sustainable solutions. This is where IBM Q comes into the picture. Quantum computers have long been considered theoretical. But today, they're becoming a reality, with huge potential for energy companies like ExxonMobil. That said, using a quantum computer also calls for significant change in how researchers think about approaching their work. "Computation has always been an integral part of the research we've done here, but quantum's radically different," Vijay explains. "Now, we must first figure out which problems are most suited to a quantum approach and only then can we answer a more interesting question: How can you program a quantum computer to solve energy problems?"

ExxonMobil joins a group of global corporations partnering with IBM to work side-by-side on IBM's fully functional quantum computers. As Vijay says, quantum's a priority that requires pairing the "best minds with the best minds." So ExxonMobil has a team that will meet regularly with IBM's quantum researchers. Barclays has its own team working on quantum, as do Samsung and Daimler. Working as part of the IBM Q Network alongside global universities and national research labs, these corporations see the potential of a massive shift in how computers can help solve some of the most enduring challenges—issues that, once solved, could transform entire industries.
"IBM Q System One is the world's first integrated universal quantum computing system designed for scientific and commercial use," says Dario Gil, director, IBM Research. "We are at the beginning of an exciting journey. Our research, systems and business teams—along with our IBM Q Network partners—have a bold vision. They are thinking big. These are the true pioneers."

Nature is no longer estimated but predicted and understood. That's the goal. So when IBM unveiled its quantum machines, companies like ExxonMobil saw great promise. But when you talk to Vijay about promise, his thoughts turn to the great needs that are facing the world. "Our global population is increasing from 7 billion to 9 billion and, all across the world, a growing middle class requires more resources and, especially, more energy."
Quantum might be well suited to solve super-complex problems, such as advanced models which could lead to better approaches to carbon capture and lower emissions sources of energy. But what excites Vijay most is that the collaboration with IBM researchers could lead to a fresh ability to predict and anticipate how nature operates—which could lead to an understanding of what's *actually* happening, as opposed to an approximation of what *might* be happening. "With a little curiosity, patience and not settling for the status quo, I know we can get there," he says.

IBM Q System One is the world's first integrated quantum computing system for commercial use.



CAMBRIDGETRADES IBM-SMART_CONTRACT

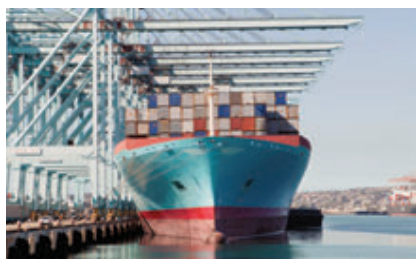
More clients are partnering with IBM to write the next chapters of their digital reinventions.

Belron applied **IBM Watson** Visual Recognition to its Autoglass Body Repair business to speed up insurance processing, move repairs along quickly and help its customers get back on the road fast.

Thought Machine, a London-based fintech startup, has built Vault, a new, cloud-native core banking infrastructure launching on **IBM Cloud**. It has also partnered with **IBM Services** to provide advisory and delivery capabilities to its clients.

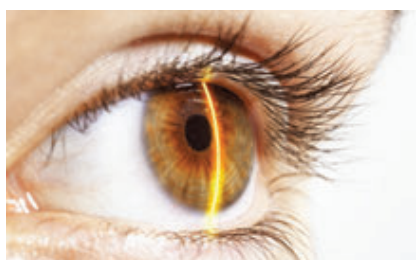
Travelport, a travel commerce platform, is working with **IBM Watson** to integrate disparate information sources and make stronger corporate travel recommendations. As a result, finding the lowest travel costs for a company will be quicker and easier.

Japan Airlines is using an **IBM Watson**-powered chatbot, Makana-chan, to answer customers' questions about its popular Tokyo-to-Honolulu flights. Makana-chan eases the burden on live agents and is very popular with passengers.



Maersk, the container logistics giant, is using **IBM Blockchain** to create TradeLens, a global blockchain solution for the shipping ecosystem. This global transformation will lead to faster delivery times, lower costs and a noticeable difference in the way we get the things we use every day.

KMD, Denmark's largest technology company, is dedicated to connecting its clients to the latest technologies. The company is using **IBM Services** to provide a critical foundation of servers, networks and other technologies that help it handle large volumes of data with high levels of security.



Bausch + Lomb simplified the service and maintenance process for its high-tech Stellaris Elite Vision Enhancement System for cataract and retina surgery. Using **IBM Cloud**, the company can now pinpoint or respond to technical and service requests and limit or minimize downtime.

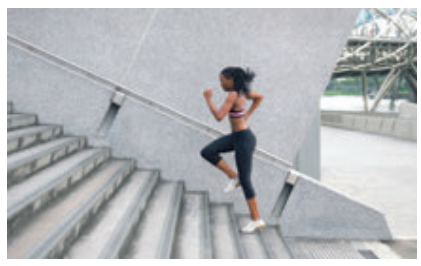
Fluor Corporation builds mega-projects across the globe. Data generated by these projects has been harnessed by working with **IBM Research** and **IBM Services**. Fluor recently introduced two new AI-powered systems to uncover and predict how unmitigated trends could affect key project indicators.

BNP Paribas is accelerating its digital transformation and improving its operational efficiency. The bank will now integrate **IBM Cloud**-hosted data centers dedicated to the bank, and will strengthen its hybrid cloud "as a service" capabilities while ensuring the security and confidentiality of their customers' data—including not using public clouds for hosting any customer or other production environments with sensitive information.

Whirlpool Corporation is using **IBM Cloud** to help manage all the data from its manufacturing of connected home appliances. Whirlpool will be using the cloud to manage critical enterprise applications, which will give it more flexibility to scale and innovate.

Telefónica turned to **IBM Blockchain** to capture call data in real time and save it in a format that's trusted, traceable and accessible to network providers and carriers worldwide, making international phone calls feel seamless despite all the technological leaps they require.

Smart Dubai, working with **IBM Blockchain** and **IBM Cloud**, has launched the region's first government-endorsed blockchain service: Dubai Blockchain Platform. It is designed to make the technology more accessible to the Dubai government, the UAE national government and private companies.



Suunto, creator of the Movesense microsensor, launched a Movesense development community enabled in the **IBM Cloud**. This let Suunto dramatically scale its offerings. Today, more than 800 developers are working with Movesense, helping Suunto bring the device to new customers all over the world.

KPMG is using **IBM Watson** to power a contract analysis solution for its clients. The solution examines contracts, breaks them into their component parts and interprets each part with a high degree of accuracy. It's faster and less expensive than manual methods, while freeing up skilled resources to perform more productive tasks.

Krungsri Bank, one of Thailand's largest financial institutions, is working with **IBM Services** to lay the foundation for its future. An **IBM Blockchain** pilot is in progress, and the bank is planning to develop new services for its customers.

Profility, a post-surgery rehabilitation solutions provider, needed to integrate large volumes of data as well as meet stringent HIPAA regulations. They chose **IBM Cloud** because of its flexible software and secure, dedicated hardware. Their system is widely used and has resulted in shorter rehab stays and fewer hospital readmissions.

The Australian Federal Government has set its sights on being one of the world's top three digital governments by 2025. In July 2018, it announced a five-year agreement that covers solutions from **IBM Cloud**, **IBM Watson**, **IBM Security**, **IBM Research** and the **IBM Q** quantum computing initiative.

View these stories and more at ibm.com/annualreport

Responsible stewardship and trust have been hallmarks of IBM's culture—from our labs to the boardroom—for more than a century.

IBM is recognized as one of the World's Most Ethical Companies by the Ethisphere Institute, highlighting our influence in driving positive change in business and society around the world.

Data Responsibility

At IBM, we've always followed straightforward principles to act responsibly and earn trust. Today, our principles include:

- The purpose of new technologies is to augment—not replace—human intelligence.
- Data and insights belong to their owner.
- New technology, including AI, must be transparent and explainable.

Recent actions demonstrate our principles at work, including:

- **Advocating for public policies to protect the privacy and security of data** and working with governments worldwide on strategies that will ensure privacy and responsible handling of data, without undermining innovation.

- **Partnering with STOP THE TRAFFIK**, law enforcement and financial services institutions to stop human trafficking by using IBM software analytics to identify suspicious trends, hotspots and financial transactions.

Modern slavery, a $150 billion business, has a new foe: an AI data hub on the IBM Cloud.

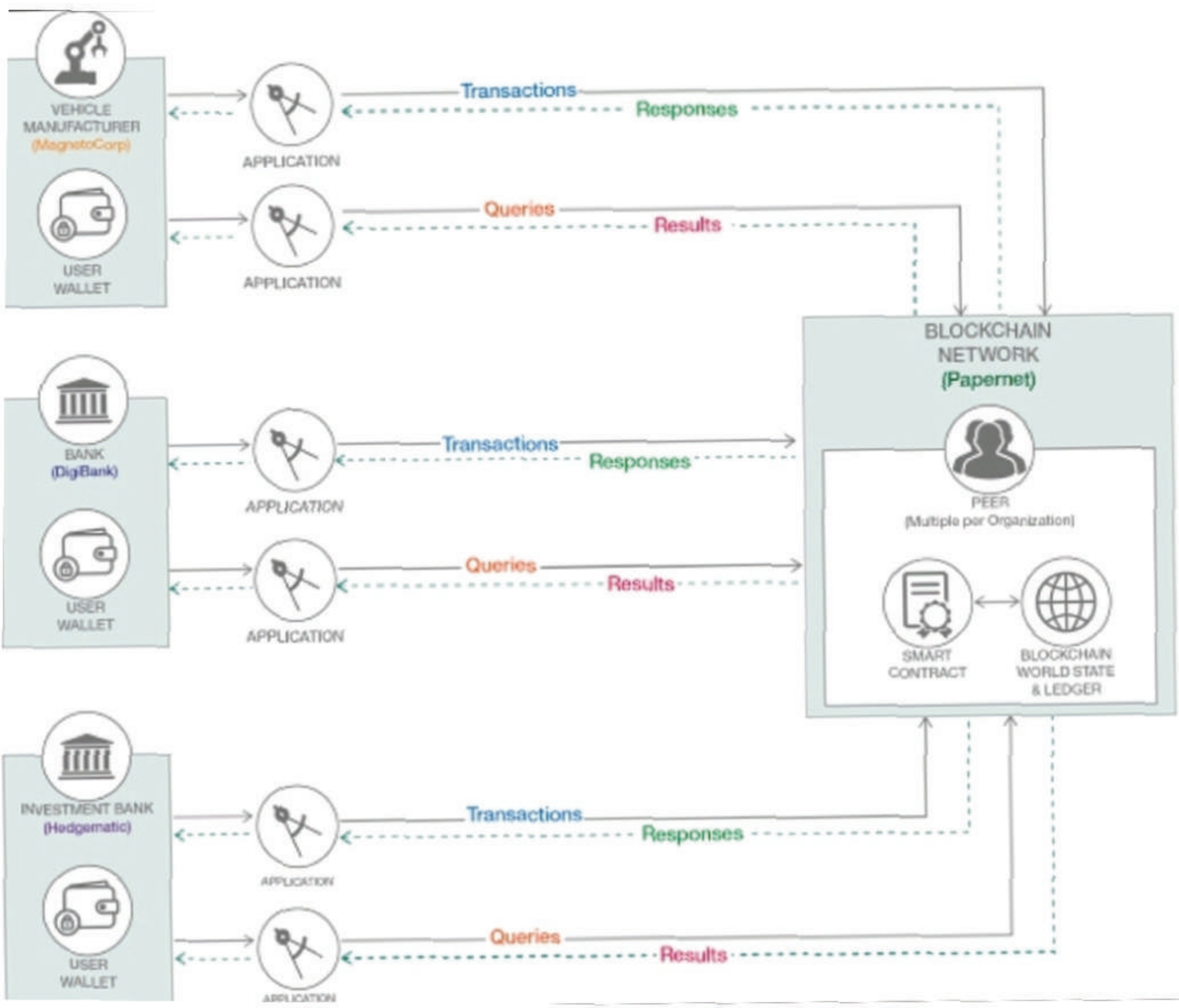
- **Launching AI Fairness 360**, an open source software toolkit to help developers actively detect and reduce bias in datasets and AI.

- **Releasing Diversity in Faces, a first-of-its-kind dataset**, to help reduce bias in facial recognition systems, making them fairer and more accurate.

1 million annotated human facial images

CAMBRIDGE TRADES

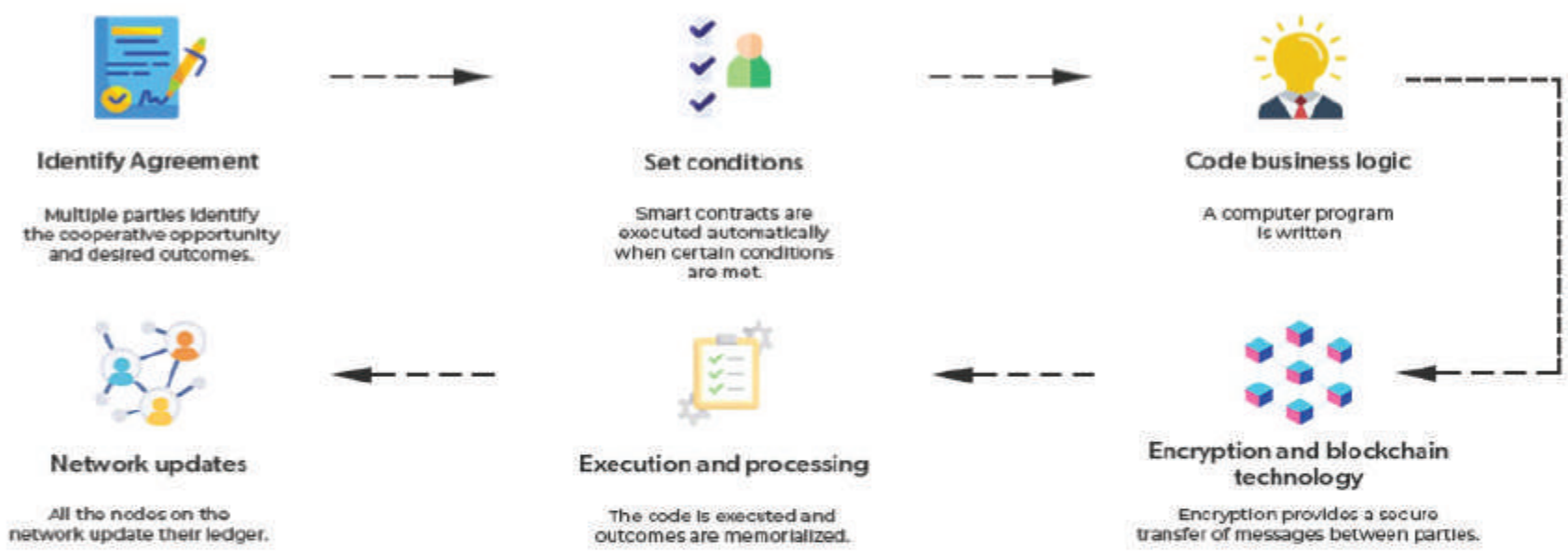
CAMBRIDGETRADES IBM-SMART_CONTRACT



CAMBRIDGE TRADES

CAMBRIDGETRADES IBM-SMART_CONTRACT

How does a Smart Contract Work?



SMART CONTRACT

Table IV. Comparison of Smart Contract Platforms

	Ethereum	**Fabric**	**Corda**	**Stellar**	**Rootstock**	**EOS**
Execution environment	EVM	Docker	JVM	Docker	VM	WebAssembly
Language	Solidity, Serpent, LLL, Mutan	Java, Golang	Java, Kotlin	Python, JavaScript, Golang and PHP, etc.	Solidity	C++
Turing Completeness	Turing complete	Turing complete	Turing incomplete	Turing incomplete	Turing complete	Turing complete
Data model	Account-based	Key-value pair	Transaction-based	Account-based	Account-based	Account-based
Consensus	PoW	PBFT	Raft	Stellar Consensus Protocol (SCP)	PoW	BFT-DPOS
Permission	Public	Private	Private	Consortium	Public	Public
Application	General	General	Digital currency	Digital currency	Digital currency	General

i.e., much safer than those systems independent of blockchains since it runs on top of Bitcoin. However, it can cause extra burden on Bitcoin blockchain. How to resolve this problem is crucial to RSK.

6) EOS: EOS [96] is designed to enable the scalability of decentralized applications. Instead of using one type of consensus algorithms only, EOS combines Byzantine Fault Tolerance (BFT) and Delegated Proof of Stake (DPOS), thereby obtaining the advantages of both consensus algorithms. At each round, delegates (*i.e.*, block producers) will be selected by stake holders to produce a new block and BFT will proceed among those selected delegates to make the block irreversible. Similar to Bitcoin, EOS is also account-based but it also allows all accounts to be referenced by human readable names. Instead of customizing a virtual machine for code execution like Ethereum, EOS chooses to use WebAssembly (Wasm) so that it is possible to write a smart contract in various languages as long as it can be compiled into Wasm (*e.g.*, EOS supports C++).

B. Comparison of Smart Contract Platforms

Table IV compares Ethereum, Fabric, Corda, Stella, Rootstock (RSK) and EOS from the following aspects such as execution environment, supporting language, Turing completeness, data model, consensus protocols, permission and application. We next summarize the main characteristics of these representative smart contract platforms as follows.

- *Execution Environment*. Contracts in Ethereum are executed in EVM. Similarly, Corda and Rootstock adopt JVM and RSK virtual machines, respectively. In contrast, Fabric and Stellar run smart contracts on top of Docker containers, consequently reducing the overhead while sacrificing the isolation of applications. EOS chooses to use Wasm to support more smart contract languages.
- *Supported Languages*. Ethereum supports Solidity, Serpent and Mutan, which are specially designed for Ethereum. Fabric currently supports Java and Golang while Corda adopts Java and Kotlin. Stellar can support a diversity of languages such as Python, Javascript, Golang and PHP. To be compatible with Ethereum, RSK adopts Solidity as the contract language while EOS currently only supports C++.
- *Turing completeness*. Smart contracts on Ethereum, EOS, Fabric and RSK are all Turing complete while Corda and Stellar are Turing incomplete. Turing-complete contracts are typically more expressive than Turing-incomplete contracts. However, the Turing completeness also brings the potential software bugs being susceptible to malicious attacks (as illustrated in Section III).
- *Data Model*. Corda adopts the unspent transaction output (UTXO) model as Bitcoin does. In UTXO model, each payment has to specify the previous unspent transaction as the input. Then the specified transaction becomes *spent*. The changes will be made on new unspent transactions. Ethereum, Stellar, EOS and RSK adopt account-based model, in which the balance of an address is recorded directly instead of calculating all the unspent transaction amounts. Fabric exploits key-value model, in which data is represented in key-value pairs stored in blockchains.
- *Consensus Algorithms*. Ethereum and RSK adopt PoW, in which the validation of the trustfulness of a block is equivalent to the solution of a computationally difficult problem (*i.e.*, a puzzle). PoW consensus algorithms are typically computational-intensive. Fabric chooses to PBFT consensus algorithm [24], in which several rounds of voting among authenticated nodes are taken to reach the consensus. Therefore, PBFT is network-intensive. In contrast, Corda adopts a simple consensus algorithm namely Raft to achieve the consensus between different sectors at the level of individual deals instead of a global system. Similarly, Stellar develops a simply consensus algorithm named SCP to reach the consensus. EOS uses the combination of BFT and DPOS.
- *Permission*. Ethereum, EOS and RSK are public (*i.e.*permissionless) smart contract platforms and each user can arbitrarily join the network while Corda and Hyperledger are private platforms only allowing authenticated users to access. Stellar sitting between public and private blockchains is a consortium blockchain across different enterprise sectors (or organizations).
- *Applications of smart contract*. Unlike Corda, Stellar and RSK only support digital-currency while Ethereum and Fabric cater for a wider diversity of applications ranging

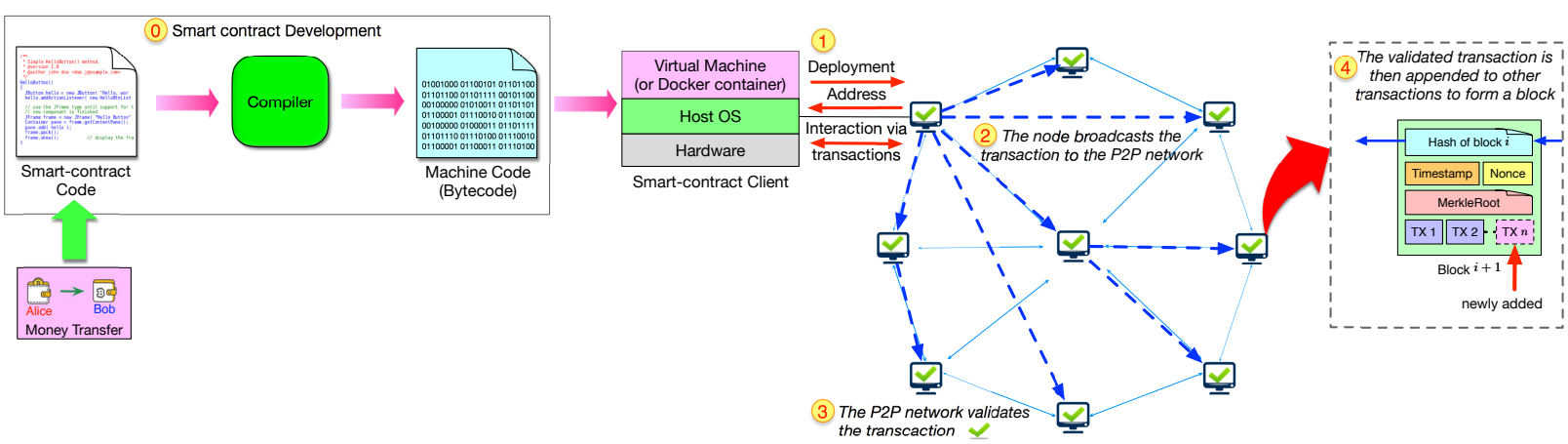


Figure 5. Workflow of a smart contract

from digital currency, digital-asset management, capital investment, public sector to sharing economy. In the future, Corda, EOS, Stellar and RSK and their derivatives may support more general applications.

C. Example of developing a smart contract

We next show how to develop and deploy a smart contract. Take a contract of money transfer between Alice and Bob as an example as shown in Figure 5. After several rounds of negotiations, the agreement between Alice and Bob reaches. Then the agreement is implemented by a smart contract language (*e.g.*, Solidity in Ethereum and Golang in Fabric). The smart contract code is next compiled via a compiler (*e.g.*, solc for Solidity), which generates machine code (or bytecode) running on top of either virtual machines (*e.g.*, EVM, JVM) or Docker containers at a smart contract client. The smart contract client is essentially connected through a peer-to-peer network. After the smart contract is deployed across the blockchain network, a unique contract address is returned to the client to support the future interactions. Thereafter, users can interact with the blockchain network via executing transactions in the smart contract (*e.g.*, deducting the specified amount of money from Alice's digital wallet and increasing the corresponding amount of money in Bob's wallet). It is worth mentioning that each transaction needs to be validated across the blockchain network via the consensus algorithms as shown in Figure 5. The validated transaction is then appended to the list of transactions. Since every node has a copy of the updated blockchain, it is difficulty to falsify the blockchain data.

Coding Sample. The syntax of Solidity is similar to JavaScript and it also supports inheritance and user-defined types. Figure 6 shows an example of a smart contract written in Solidity.

```
// mortal.sol
pragma solidity ^0.4.0;
contract mortal {
   /* Define variable owner of the type address
       */
   address owner;
   /* This function is executed at
       initialization */
    constructor() internal { owner =
        msg.sender; }
   /* Function to send 500 wei to receiver's
       address; 10^18 wei=1 ether; */
   function fundtransfer(address receiver)
       public { if (msg.sender == owner)
       {receiver.transfer(500);} }
}
```

Figure 6. Example of smart contract written in Solidity in Ethereum

V. Applications of smart contract

Smart contracts have a broad spectrum of applications ranging from Internet of Things to sharing economy. In particular, we roughly categorize major smart contract applications into six types as shown in Figure 7. We next describe them in details.

A. Internet of Things

Internet of things (IoT) that is one of the most promising technologies can support numerous applications including supply chain management, inventory control systems, retailers, access control, libraries, e-health systems, industrial Internet [97], [98], [99]. The main initiative of IoT is to integrate "*smart*" objects (*i.e.*, "things") into the Internet and to provide various services to users [100]. IoT has been proposed to automate various business transactions in an implicit way.

With the integration with smart contracts, the potentials of IoT can be unleashed. Take industrial manufacturing as an example. Most current manufacturers maintain their IoT ecosystems in a centralized manner. For instance, firmware updates can only be obtained at the central server *manually* by various IoT devices through querying from devices to the server. Smart contracts offer an automatic solution to this problem [101]. Manufacturers can place firmware update hashes on smart contracts deployed on blockchains distributed throughout the whole network. Devices can then obtain the firmware hashes from smart contracts automatically. In this way, resources are greatly saved.

Smart contracts can also bring benefits to IoT e-business model. For example, the traditional e-business model often requires a third party serving as an agent to complete the payment. However, this centralized payment is costly and cannot

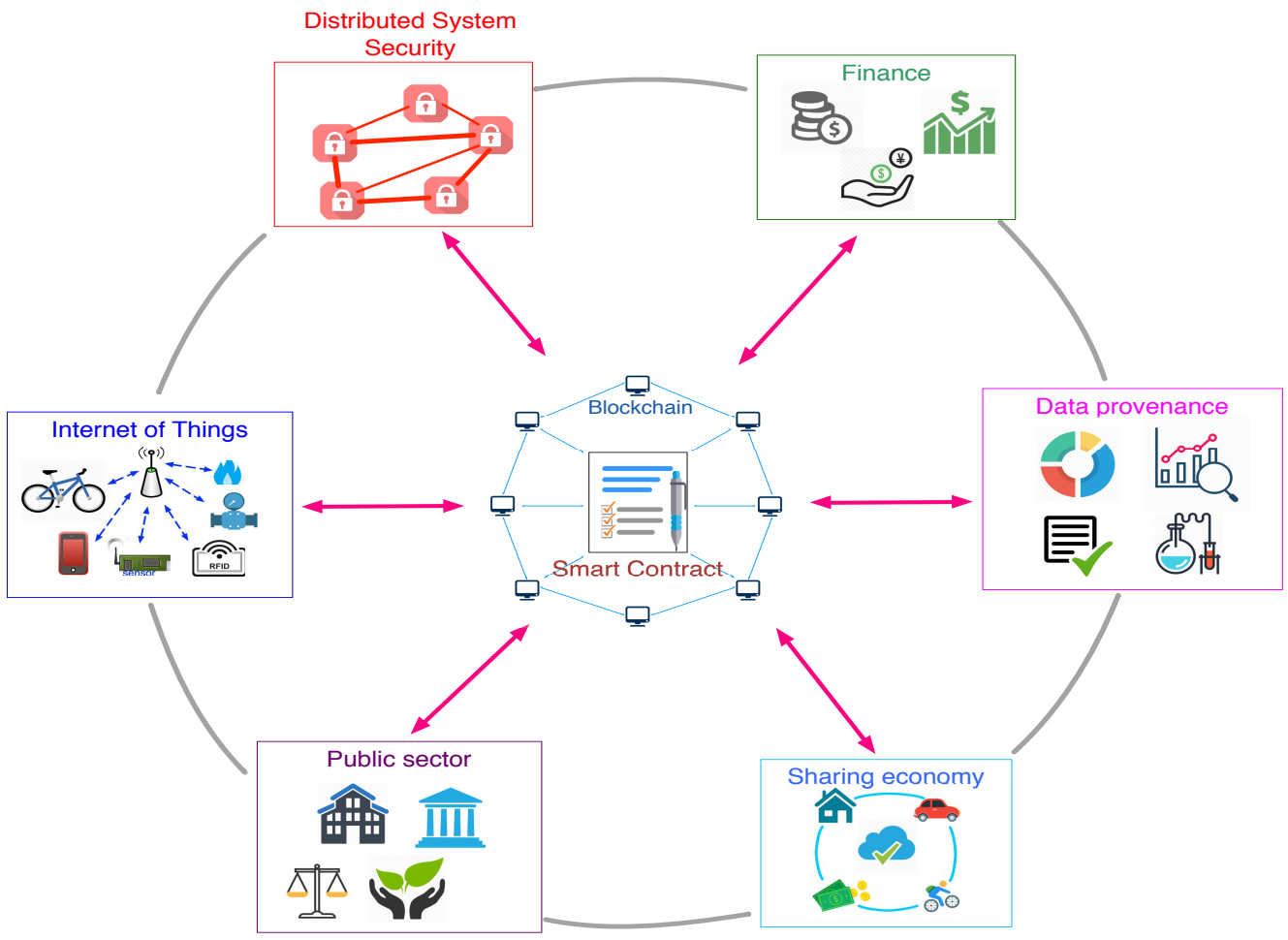


Figure 7. Smart contract applications

fully utilize advantages of IoT. In [4], Distributed autonomous Corporations (DACs) were proposed to automate transactions, in which there are no traditional roles like governments or companies involved with the payment. Being implemented by smart contracts, DACs can work automatically without human intervention. Moreover, smart contracts can also help to speed up conventional supply chains. For example, the marriage of supply chains with smart contracts can automate contractual rights and obligations during the payment and the delivery of goods while all the parties in the whole process are trustful.

B. Distributed system security

Smart contracts can bring benefits in improving the security of distributed systems. Distributed Denial-of-Service (DDoS) attacks are one of major security threats in computer networks. Attackers flood the targeted machine with superfluous requests to overload systems, consequently interrupting or suspending Internet services [102]. Recently, a collaborative mechanism was proposed to mitigate DDoS attacks [103]. Compared with traditional solutions, this scheme that is based on smart contracts can tackle the attacks in a fully decentralized manner. In particular, once a server is attacked, the IP addresses of attackers will be automatically stored in a smart contract. In this manner, other nodes will be informed of the addresses of attackers. Furthermore, other security polices will be immediately enforced, *e.g.*, filtering the traffic from the malicious users.

Cloud computing is a promising technology to offer a ubiquitous access of a shared pool of computing and storage resources to users [104]. Generally, users can purchase cloud services from trustful cloud service providers (CSPs). However, how to verify the trustfulness of CSPs becomes a challenge since CSPs often collude with each other to earn more profits. Dong *et al.* [105] proposed a solution based on game theory and smart contracts. The main idea of this approach is to let a client ask two cloud servers to compute the same task. During this process, smart contracts are used to stimulate tension, betrayal and distrust between the clouds. In this way, users can easily determine the rational clouds that will not collude and cheat. Experiments based on the contracts written in Solidity on the official Ethereum network were also conducted to verify the effectiveness of this proposal.

Moreover, brokers are typically used in cloud computing. Users' requests are checked by a broker to match with providers' services. However, both users and service providers must trust the broker. Once the broker is hijacked or compromised, both the parties become untrustful. Recently, Scoca *et al.* [9] proposed to use smart contracts to avoid the usage of brokers. The main idea of their approach is to use distributed Service-Level-Agreements for Clouds (dSLAC) [106] to specify the needs via smart contracts. Meanwhile, a utility function that evaluates the agreements according to both parties' preferences was proposed to solve the mismatching problem.

www.cambridgetrades.ltd