Preprint Cambridge Centre for Computational Chemical Engineering ISSN 1473 – 4273

# Blockchain Technology in the Chemical Industry

Xiaochi Zhou[1], Markus Kraft[1,2,3]

released: October 7, 2021

[1] Department of Chemical Engineering
and Biotechnology
University of Cambridge
Philippa Fawcett Drive
Cambridge, CB3 0AS
United Kingdom

[2] CARES
Cambridge Centre for Advanced
Research and Education in Singapore
1 Create Way
CREATE Tower, #05-05
Singapore, 138602

[3] School of Chemical
and Biomedical Engineering
Nanyang Technological University
62 Nanyang Drive
Singapore, 637459

Preprint No. 282

*Keywords:* Blockchain, Smart contract, Chemical industry, IoT, Industry 4.0, P2P energy trading, emission trading, Smart city, Knowledge graph

**Edited by**
Computational Modelling Group
Department of Chemical Engineering and Biotechnology
University of Cambridge
Philippa Fawcett Drive
Cambridge, CB3 0AS
United Kingdom

**E-Mail:** mk306@cam.ac.uk
**World Wide Web:** `https://como.ceb.cam.ac.uk/`

## Abstract

This paper presents a review of the application of blockchain and blockchain-based smart contracts in the chemical and related industries. We introduce the basic concepts of blockchain and smart contracts and explain how some of their features are enabled. We review a number of typical or novel publications on blockchain and smart contract technologies and their enabling concepts and underlying technologies. We classify the selected contributions into five categories and discuss their motivations and technical designs. We recognise that the trend of decentralisation creates a need for using blockchain and smart contracts to implement trust and distributed control mechanisms. We also speculate on future applications of blockchain and smart contracts. We believe that, in future, blockchains with different consensus will be studied and applied to achieve more efficient and practical decentralised systems. Also, blockchain-based smart contracts will be more widely applied to enhance autonomous distributed controls in decentralised systems.


## Highlights

- Detailed introduction to blockchain and smart contract implementation
- Systematic review of works applying blockchain and smart contract technologies in the chemical industry.

# Contents

# 1 Introduction

In many industries, including the chemical industry, there is a common trend of transforming large-scale systems from centralised architectures into decentralised architectures. To cope with some shortcomings of decentralised systems, blockchain technologies are widely applied in those systems.

Current technologies and concepts which are closely related to the chemical industry, especially the Internet of Things (IoT) [8, 111] and Industry 4.0 [19, 126], are installing millions of devices to industrial systems and are empowering them with more computing power and awareness of the surrounding physical world. In addition, devices and systems are being connected and are cooperating with each other more closely than ever. As a result, an enormous amount of data are being created, processed, and transferred each second. Also, the needs for computing and other services are also rapidly growing. Consequently, it is challenging for centralised systems to ensure high availability and low latency, due to the limitations of communication channels or network congestion and their vulnerability to single-point-failure. Naturally, decentralised systems are becoming ever more favoured.

Typical decentralised systems often adopt a peer-to-peer (P2P) communication model [106], where all peers or nodes directly exchange information with each other and distribute local information to the system. Without central commands, the nodes aggregate information locally and act upon local information to contribute to the collective, complex behaviour.

A decentralised industrial system has several advantages. Firstly, decentralised systems are robust against single-point-failure as they do not depend on one single central control. As a result, high availability of the system is ensured. Energy trading is an area where high availability and system robustness are vital [27, 129]. Therefore, many decentralised P2P energy markets are proposed, where users directly trade energy without a central authority.

Secondly, with the access to other local devices within the same system or located nearby, the communication latency can be improved. One example is the concept of fog computing [132], which utilises a huge number of heterogeneous and local devices (*e.g.* end devices, routers, *etc.*) in a decentralised network to offer computing storage and task processing services without the control of third parties. The main feature of fog computing is a low requirement on bandwidth and low latency [132]. It can also make good use of idle capacity and prevent waste [78].

Scalability is another feature of decentralised systems as a single node can join or leave the decentralised system freely without having a major impact on the overall system. However, high scalability is only possible if the decentralised system is permission-less and trust-less. To integrate a large number of nodes in a network, it is costly to validate the identity of a new node, permit its entrance, and regulate its behaviour. As a result, scalable decentralised systems are inevitably open, permission-less, and trust-less. Consequently, for large decentralised systems, trust between nodes is a vital issue.

Within a permission-less, trust-less, and decentralised environment, the application of blockchain technology is recognised as the most effective way to ensure trust among peers [38]. A blockchain is a form of database implemented on top of P2P networks, where the data are stored in a distributed way and managed in a decentralised way. Nodes on a blockchain network can keep a local replica of the database and the integrity and consistency of this local replica can be guaranteed. The consensus mechanisms also prevent malicious behaviours from other nodes. Also, due to its cryptographic and P2P nature, privacy can be effectively preserved during the communication between nodes. In addition, blockchain-based smart contracts, which are code published on a blockchain, can serve as trustworthy and autonomous nodes. Those autonomous nodes enabled by smart contracts can then react to and enforce activities on the blockchain [21, 113].

As a result, in fields that are revolutionising the modern chemical industry [49, 83, 86], including IoT, smart manufacturing, smart supply chain management, smart city, P2P energy trading, emission trading, and knowledge graphs, are adopting blockchains and smart contracts to implement and improve their decentralised systems. The application of blockchains are in aspects including but not limited to data sharing, trading, transactions, record keeping and tracing, and privacy preserving. Smart contracts are applied in aspects including market clearing, transaction settlement, identity management, access control, and so on.

In this paper, we present a systematic literature review on the application of blockchain and smart contract technologies in the chemical industry and other closely related fields. Our study and analysis focuses on the motivation for these fields to utilise blockchain and smart contract technologies and how these technologies are used in their systems. In addition, although blockchain technology, especially its features, has been widely discussed in both industry and academia, the details of how the features are enabled are less well known. Therefore, this paper also gives a detailed introduction to the enabling technologies of blockchain and smart contracts.

The rest of this paper is organised as follows. Section 2 introduces the implementation of blockchain and smart contracts. In section 2.3, we introduce some important or novel implementations of blockchains and their features. Section 3 introduces our literature review methodology and presents a statistical analysis of the literature. Section 4 discusses several selected works that apply blockchain and smart contracts in different fields. In section 5 we specifically introduce the application of blockchain and smart contracts in knowledge graphs. Finally, section 6 concludes our findings and our insights on the future directions.

# 2 Basics on blockchain and smart contracts

In this section, we explain the fundamentals of blockchain and smart contracts in detail and elaborate how some of their features are enabled.

## 2.1 Blockchain

A typical blockchain is a database, managed in a decentralised way and can store any information, including transactions, records, events, and even scripts in a distributed fashion. A blockchain is formed by a sequence of blocks, linked with each other. A block usually contains information including a nonce (abbreviation for "number only used once"), some data, the hash of the previous block, and the hash of the block itself. As a new block always contains the hash of the previous block, the blocks form a chain-like structure and hence are called "blockchain". Figure 1 presents an example of two linked blocks.

### 2.1.1 Hash function

The hashes are generated via cryptographic hash functions [101]. A cryptographic hash function, for example, Secure Hash Algorithm-256 bit (SHA-256), takes any information as input and produces a unique 64-digit hexadecimal number. In an ideal hash function, the hash of any information can be easily produced but it is difficult to derive the inputs from the hash. In addition, any minor changes in the inputs will result in significant and seemingly uncorrelated changes to the resultant hash. As a result, it is easy to verify whether the hash is produced from the known inputs but it is expensive, in the sense of computation power, to find the inputs that produce a known hash [121].

### 2.1.2 Tamper-proof

The hash of a block is usually generated via a hash function using three inputs: the nonce, the data, and the previous hash. Some blockchain requires the hash to meet certain conditions. For example, the hash must begin with four zeros. As a result, to calculate the hash, one must try different nonces in iterations to generate a hash that meets the requirement. This requirement is referred to as a target. The process of finding a nonce that generates a valid hash is called mining and a user that does the mining is referred to as a miner.

As mentioned before, any changes in the inputs will lead to significant changes in the hash. Therefore, if any data is modified in a block, the newly calculated hash will not meet the requirements. Also, as this new hash is the previous hash for the next block and it is one of the inputs for generating the hash in the next block, the hash in the next block will become invalid as well. Consequently, the tampered block and all blocks after it will have invalid hashes. The propagation of hash invalidity is demonstrated in Figure 2. To make these blocks valid again, one must mine the tampered block and all subsequent blocks. As mentioned before, it is expensive to find the valid nonce. Therefore, it consumes substantial computing power to tamper with data on a blockchain and fix the hashes.

### 2.1.3 Public and private key pair

A typical blockchain also integrates a public and private key pair mechanism. For each user, one or more pairs of public and private keys are generated. Assume User A has a private key and a public key, User A can create a message signature from the private key and the message. User B can use User A's public key and the message signature to verify the message was created by the owner of the paired private key - User A. In addition, User B can encrypt a message using User A's public key and only User A can decrypt the message using its private key.

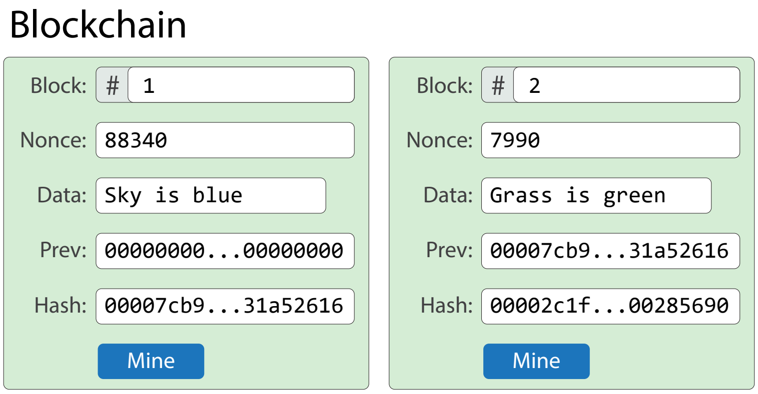


**Figure 1:** *An example of a blockchain containing two blocks.*

### 2.1.4 P2P network and consensus mechanism

A blockchain is implemented on top of a peer-to-peer (P2P) network, with no centralised authority. For a blockchain such as the Bitcoin blockchain, anyone can join the network without any permission. Each user is considered a node on the network and can hold a full copy of the entire blockchain. To guarantee the local copies on the nodes are synchronised throughout the network and ensure that all the nodes agree on the content of the blockchain, different types of consensus mechanisms are implemented. Prevailing consensus mechanisms include Proof-of-Work (PoW) [90], Proof-of-Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), and *etc.* [1]. The most used consensus mechanisms are PoW and PoS [10].

When a user makes a transaction, the message will be broadcast in the P2P network and each node can receive it. In a PoW mechanism, transactions will be processed as follows:

- Each miner creates a candidate block containing all the valid transactions from among all the transactions it received. The valid transactions are transactions compatible with the rest of the chain.
- Mine this new block until the nonce that produces a hash that meets the target (*e.g.* minimum amount of leading zeroes) is found.
- Broadcast the new block to the network.
- Other nodes on the network will start to verify the proof-of-work of this chain and append the new block to their local chain.
- In case multiple miners finish mining simultaneously and broadcast their block, the chain will be temporarily split into two or more branches (forks). The nodes will work on the first new block they received but save other new blocks in case they grow longer. When another valid new block is broadcast by one of the competing miners, who found the next proof-of-work, the tie is broken. Since another block

is added to one of the branches, this branch becomes the longest chain. Any nodes working on a different branch will accept and switch to this branch.

In a PoS mechanism, competing miners are replaced by a chosen "validator". The node to create the next block in the chain is selected by a random process. In this random process, nodes who want to be validators stake their tokens. The chance of being selected is proportional to the number of tokens staked. If a validator is found doing wrong in creating the block, they will lose their stake.

### 2.1.5 Incentives

The PoW mechanism consumes substantial computation power. As a result, incentive mechanisms are implemented to compensate miners. Each transaction has a transaction fee, which will be rewarded to the miner. As a result, miners will prioritise transactions with higher transaction fees and hence these transactions will be accepted faster. The PoS mechanism works differently by punishing wrong-doings and hence indirectly provides incentives for honest behaviour.

### 2.1.6 Attacks

A "51% percent attack", or a majority attack, happens when one or a group of dishonest miners can continuously generate blocks faster than all other nodes combined. Consequently, a fraudulent chain can be the longest chain. Since other nodes always accept the longest chain, the fraudulent chain becomes the valid chain and the attackers control the blockchain. Then malicious actions such as double-spending by reserving transaction records become possible. However, in a PoW-based blockchain, it requires a vast amount of computation capability to achieve a "51% percent" attack in a major blockchain and makes a "51% attack" practically infeasible.

In a PoS blockchain, it requires controlling more than half of the cryptocurrency tokens on this blockchain to achieve a "51% attack". Firstly, considering the market value of the major cryptocurrencies, it is very difficult to control this vast amount of tokens. Secondly, if a blockchain is attacked, it will be considered vulnerable and the market value of its token will drop. Since the attacker is the biggest holder of this cryptocurrency, the attacker will bear a significant financial loss. Lastly, as the attack has staked the majority of the tokens on the blockchain, their loss due to the wrong-doing will always be worth more than their gain from the attack.

Sybil attack [31] refers to obtaining disproportional control or influence in P2P networks by maliciously creating a large number of identities. When identities can be cheaply generated in a system, this system is more vulnerable to Sybil attacks. In the two major consensus mechanisms: PoS and PoW, the influence of users must be backed by either the holding of tokens or computation power. As a result, it is costly to create effective identities in the network.

## 2.2 Smart contract

A smart contract is essentially a piece of script published on a blockchain, for the purpose of enabling more complex decentralised and distributed applications. The two major platforms supporting smart contracts are the Bitcoin blockchain [90] and the Ethereum blockchain [21], which are both PoW blockchains. Some PoS blockchains, including Cardano [22] and NEO [34], also support the implementation of smart contracts. We will explain blockchain-based smart contracts using the Ethereum smart contract as an example.

As mentioned above, any information can be published on blockchains. On the Ethereum blockchain, some bytecodes are published via transactions. The same as other information published on the chain, these bytecodes are tamper-proof and each node can have a local copy of those codes. The code, together with their states (data), which are also stored on the blockchain, are referred to as smart contracts.

The Ethereum blockchain provides Ethereum Virtual Machines (EVMs), which can be installed locally on the nodes and execute the local copies of the smart contracts. The EVMs serve as sandboxes and ensure the results of running the smart contracts are consistent over different nodes. The tamper-proof code and data of the smart contracts together with the EVMs, make it possible to implement functions that can not be intervened with.

Smart contracts can also be seen as a type of Ethereum account and are assigned with blockchain addresses. Therefore, smart contracts have a balance of tokens and can make transactions over the network. Data can also be "stored" in smart contracts as variables declared in the smart contracts are assigned with addresses on the blockchain. If a node has permission to access a variable, it then can read the variable locally via smart contracts and update the variable via transactions.

As a result, smart contracts serve as trustworthy yet autonomous nodes, which can react to and enforce activities on the blockchain.

Currently, Solidity [25] is the mainstream programming language for implementing Ethereum smart contracts. Vyper [120] is another language for Ethereum smart contracts but deliberately has less feature than Solidity to make contracts more secure and easier to audit.

## 2.3 Implementation

In this section, we will discuss the features of some influential or technically novel implementations of blockchains.

### 2.3.1 Bitcoin

Bitcoin is the first and the most well-known digital currency. The blockchain hosting Bitcoin is also the largest blockchain so far. As of October 2021, there are more than 703,000 blocks with a blockchain larger than 355 gigabytes and around 12,000 active nodes [17]. A new block is created and appended to the chain roughly every 10 minutes, containing 2,759 transactions on average [15].

The Bitcoin blockchain adopts a PoW consensus mechanism. In 2021, it takes from 8 USD to 60 USD to make a transaction, the value changes rapidly due to the fluctuation of the value of Bitcoin. The current estimated total hash rate in the Bitcoin blockchain is $1.47 \times 10^{20}$ hashes per second [15]. It means it is estimated that the total mining computation power on the Bitcoin blockchain can make $1.47 \times 10^{20}$ guesses to find the proof-of-work every second. In 2020, Gallersdörfer et al. estimates that mining on the Bitcoin blockchain consumes energy at a rate of 4.3 gigawatts while Digiconomist [28] derives 7.9 gigawatts, which is 166.76 terawatt-hour annually [28].

The Bitcoin blockchain supports the implementation of smart contracts. Smart contracts are coded in a language named "Script", which is intentionally Turing-incomplete and does not support logical loops [16, 91].

### 2.3.2 Ethereum

Ethereum [21] is the other most important blockchain, which hosts its cryptocurrency "ether". As of October 2021, The Ethereum blockchain contains 13,319,122 blocks. The time for a new block to be added to the chain is between 10 to 20 seconds and 13.43 on average [131]. In 2021, the peak number of nodes in the Ethereum network was 12,472 and then dropped to around 3,600 in October [36].

The main blockchain of Ethereum also adopts a PoW mechanism. As of October 2021, the average network hash rate of Ethereum is about $7.1 \times 10^{14}$ hash per second [37]. The latest average transaction fee on Ethereum is about 3.82 USD. The estimated power consumption rate of Ethereum is about 0.719 gigawatts [45]. Digiconnomist estimates that the annual energy consumption is 74.64 terawatt-hour [28].

The support for smart contracts is a major feature of Ethereum. Solidity is the most active and maintained language for Ethereum smart contracts [25]. Different from Script, Solidity is Turing-complete and can support more complex functions [57].

### 2.3.3 Others

**Cardano** is the first blockchain to be established on peer-reviewed research. Cardano adopts a PoS consensus mechanism and hosts its cryptocurrency ADA. Based on the market capitalisation of ADA, Cardano is the largest PoS-based blockchain. It is claimed that Cardano only consumes 6 gigawatt-hour per year [20].

Cardano started to support smart contracts from September 2021 and their smart contracts support two programming languages, Marlowe and Plutus [22].

**The NEO network** adopts a decentralised Byzantine fault-tolerant (dBFT) consensus mechanism together with a set of centrally approved nodes. One of its major features is the ability to support over 10,000 transactions every second. It also supports smart contracts [34].

**Tezos** is another PoS blockchain. Its main feature is that it supports amendment of the protocol if an upgrade proposal passes voting within the community [5].

**The Ripple** blockchain hosts its own cryptocurrency, XRP. Rather than PoW or PoS, Ripple adopts relies on a set of bank-owned servers, to confirm transactions. Therefore, Ripple features instant and low-cost international payments.

**MultiChain** is an open-source blockchain platform for building and deploying blockchain applications and provides convenient interfaces [46]. It also allows the use of various programming languages such as Python, C#, PHP, Ruby or JavaScript.

# 3 Literature analysis

In this section we review the literature on blockchain and smart contracts. We do this by systematically searching through Scopus, which is Elsevier's abstract and citation database launched in 2004. Scopus covers nearly 36,377 titles from approximately 11,678 publishers. Two lists of keywords are defined to create keywords combinations for the search. List 1 contains keywords for blockchain and smart contract technologies: "Blockchain", "Distributed ledger", "Smart Contract", and "Decentralised Application". List 2 includes keywords in the field of chemical engineering: "Chemical engineering", "Chemical industry", "Energy", "Energy industry", "Power industry", "Chemical", "Smart city", "Industrial parks" "Process industry", "Smart industry" and "Chemistry". On top of these two keywords lists, 44 keywords combinations are generated. These keywords are then searched in Scopus. Scopus returned 2,527 unique results.

On top of the 2,527 articles, we analysed their publication year and geographical distribution as shown in Figure 3. In the aspect of publication year, it is evident that the number of works is increasing annually. From the geographical distribution of the publications, it can be seen that although China, the United States, and India are leading the number of publications, other countries also made significant contributions.

# 4 Selected works

From these articles, 158 of them that present typical or novel applications of blockchain or smart contracts are selected and reviewed. Articles that are highly cited or newly published are prioritised. Some works are also added to the review during the writing of this paper. Among them, 82 are discussed in this paper. It is found that an overwhelming majority of the reviewed articles belong to 5 fields: Internet of Things, Industry 4.0, P2P energy markets, emission trading, and smart cities. Unfortunately, there is a very limited number of works that directly discuss applying blockchain and smart contracts in chemical engineering. However, the aforementioned 5 fields are core enabling technologies and concepts for the chemical industry. In each field, a table of works will be presented. Table 1 for the Internet of Things, table 2 for Industry 4.0, table 3 for P2P energy markets, table 4 for emission trading, and table 5 for smart cities.

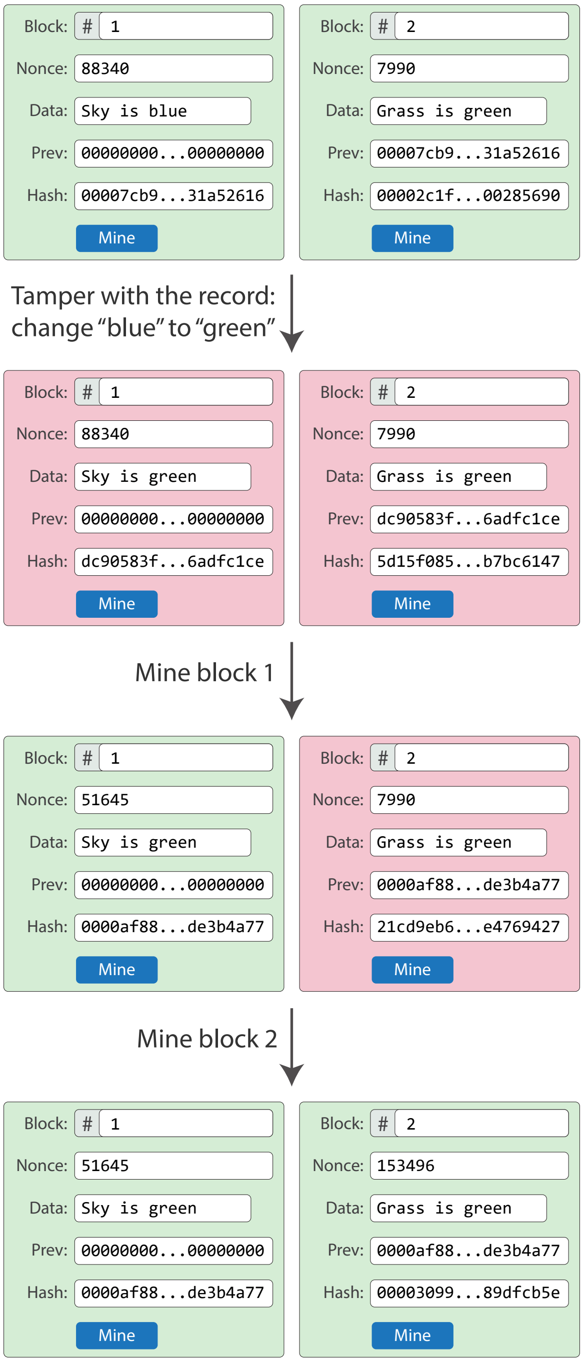


**Figure 2:** *Before tampering with the data in block 1, both blocks have valid hashes and therefore are green. When the data in block 1 is changed, both blocks turned red as neither of them has a valid hash. In block 1, the original nonce and the tampered data generates a hash that doesn't meet the requirements. In block 2, due to the change of the previous hash, its hash has become invalid. To make the blocks valid again, both of the blocks need to be mined again.*

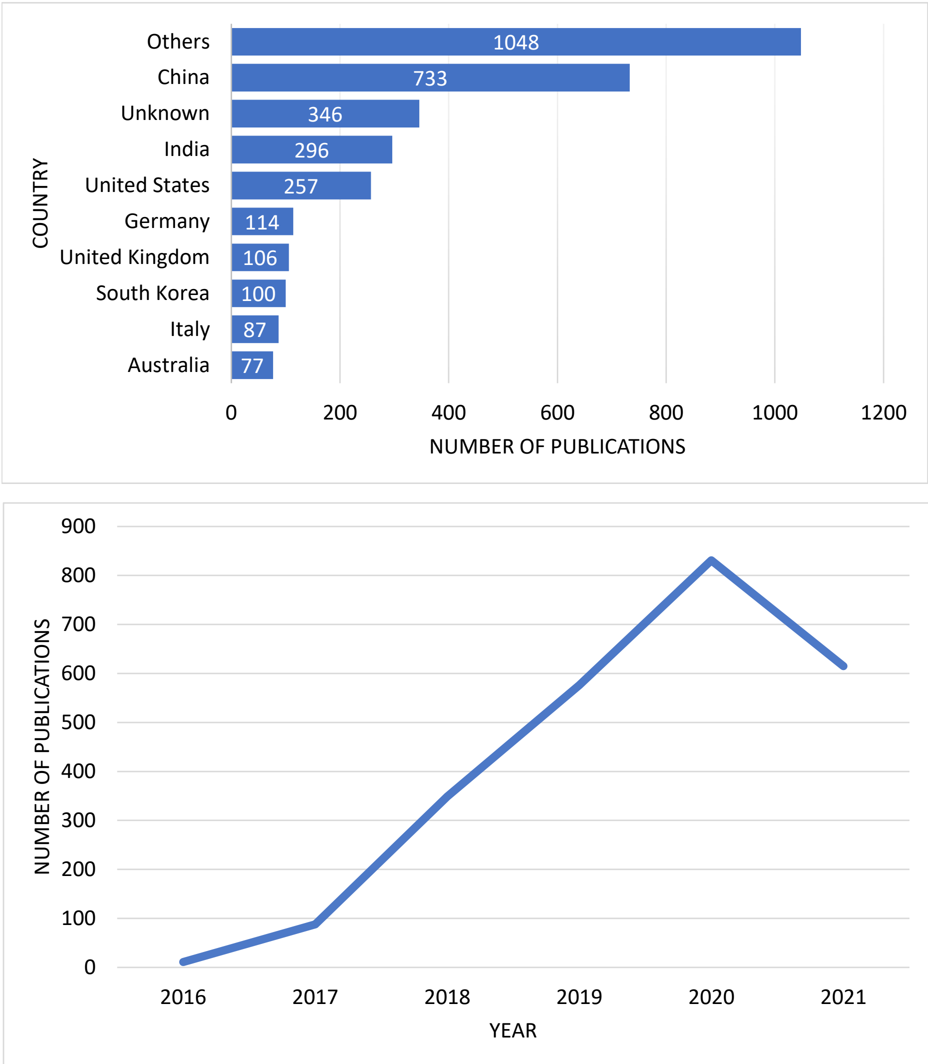


**Figure 3:** *Number of publications by country and number of publications by year.*

## 4.1 Internet of Things

Security is a major concern in the IoT community, as accidental or malicious interference of data can lead to serious consequences. However, the rapid growth of the number of devices introduces a substantial number of untrusted devices to the IoT network. Since the integrity of data stored on blockchains can be rather easily verified, many works [30, 48, 58–60, 79, 102, 114, 116, 127] have adopted blockchain technology to implement a trust layer among untrusted devices.

For example, Yazdinejad et al. proposed a design that incorporates a software-defined networking (SDN) controller and blockchain to monitor the integrity of data in the IoT network. There are also works that use blockchain as a transaction layer for IoT networks. For example, Zhang and Wen proposed an E-business platform where paid data can be traded within the IoT network using blockchain as the transaction layer. Muthanna et al. proposed to use blockchain to ensure decentralisation of IoT networks in a trustful manner.

In the IoT community, blockchain-based smart contracts are often used for enabling an authentication and authorisation mechanism and implementing a trust layer. For example, Xu et al. proposed an identity-based capability token management strategy, which uses smart contracts for registration, propagation, and revocation of the access authorisation. Nakamura et al. proposed a decentralised and trustworthy Capability-Based Access Control (CapBAC) scheme by using the Ethereum smart contract technology.

In addition, due to the rapid growth of the number of devices in the IoT networks, the IoT community is adopting a decentralised computing architecture: fog computing. Fog computing utilises local devices and computation power to handle tasks that require fast response times. At the same time, fog computing leverages cloud computing to handle heavy tasks when the local devices do not have sufficient computation or data storage power. However, it is challenging to implement conventional centralised authentication and access control mechanisms in fog computing while guaranteeing low response time and high availability, mainly when the network contains many devices. As a result, many works propose the use of smart contracts to handle the authentication and access control in such a network. Khalid et al. proposed a decentralised authentication mechanism for fog computing in IoT systems on top of smart contracts. In this mechanism, smart contracts are used to verify the identity of devices by comparing their identity information with the registration information stored in the blockchain. Sharma et al. used smart contracts to check whether tasks can be performed on a certain machine.

## 4.2 Industry 4.0

Industry 4.0 has widely adopted blockchain technology in many aspects, including supply chain management and manufacturing [19].

Due to the tamper-proof nature of data stored on a blockchain, blockchain technology is used to ensure the integrity of supply chain records, enable traceability of the products, and eliminate fraud. For example, Feng Tian proposed a blockchain-based supply chain traceability system that covers several processes of a supply chain to guarantee food safety. Take their cold chain distribution system as an example, an on-vehicle safety

**Table 1:** *Internet of Things*

| Author | Title | Year |
|---|---|---|
| Zhang and Wen | The IoT electric business model: Using blockchain technology for the internet of things | 2017 |
| Dorri et al. | Blockchain for IoT security and privacy: The case study of a smart home | 2017 |
| Teslya and Ryabchikov | Blockchain-based platform architecture for industrial IoT | 2017 |
| Khan and Salah | IoT security: Review | 2018 |
| Hammi et al. | Bubbles of Trust: A decentralized blockchain-based authentication system for IoT | 2018 |
| Roy et al. | BlockChain for IoT Security and Management: Current Prospects | 2018 |
| Tapas et al. | Blockchain-Based IoT-Cloud Authorization and Delegation | 2018 |
| Machado et al. | IoT Data Integrity Verification for Cyber-Physical Systems Using Blockchain | 2018 |
| Xu et al. | BlendCAC: A Blockchain-Enabled Decentralized Capability-Based Access Control for IoTs | 2018 |
| Sharma et al. | A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT | 2018 |
| Muthanna et al. | Secure and Reliable IoT Networks Using Fog Computing with Software-Defined Networking and Blockchain | 2019 |
| Nakamura et al. | Exploiting Smart Contracts for Capability-Based Access Control in the Internet of Things | 2020 |
| Kamran et al. | Blockchain and Internet of Things: A bibliometric study | 2020 |
| Yazdinejad et al. | An Energy-Efficient SDN Controller Architecture for IoT Networks With Blockchain-Based Security | 2020 |
| Khalid et al. | A decentralized lightweight blockchain-based authentication mechanism for IoT systems | 2020 |

monitoring system constantly uploads real-time environmental data of products, including temperature and humidity, and their GPS coordinates to the blockchain. Feng Tian later upgraded their system to cover all processes in a supply chain. Tse et al. involves the government in the tracking, monitoring, and auditing of the supply chain in their blockchain-based supply chain tracking system. The work from Kshetri focuses on using blockchain to increase the transparency and accountability of supply chain records. Kuhi et al. proposed a system to ensure performance measurement integrity in logistics using blockchain. Mondragon et al. discussed the applicability of leveraging blockchain technology in the supply chain of the composite material industry, where semi-finished materials such as pre-impregnated materials require temperature-controlled transportation.

In manufacturing, some works use blockchain to provide tamper-proof records of product manufacturing, provenance, transportation, handling and storage[69]. Ko et al. discussed how blockchain technology can help the manufacturing industry in achieving real-time transparency and cost-saving.

Some works also use blockchain to handle data exchange between participants in a decentralised, secured, and scalable way. Vatankhah Barenji et al. proposed a cloud manufacturing (CMfg) architecture incorporating two types of blockchain networks. The public blockchain allows end-users to select available services from existing cloud manufacturing systems and make payments for these services, while a private blockchain is used for the shop level and handles data receiving and gathering for machines.

In the field of supply chains, the work from Dolgui et al. uses smart contracts to trigger rescheduling in the supply chain upon the detection of a delay. Wang et al. built a decentralised application (DApp) based on the Truffle framework to carry out the process of product registration, transferring, and tracking through the collaboration of smart contracts. Chang et al. proposed a private-chain design to enhance the transparency and distributed collaboration of supply chain processes.

In the field of manufacturing, Angrish et al. proposed a system that uses smart contracts to facilitate the sharing of data between various participants in the manufacturing process. Three types of smart contracts are designed. The Global Registrar Contract (GRC) maps each participant, including humans, agents, and machines, to their blockchain address identity and manages the identity data. The Participant Historical Event Contract (PHEC) allows participants to retrieve historical events of the manufacturing history related to the participants. The Participant Relationship Contract (PRC) creates entries representing the relationship and its status between participants. For example, the relationship between a client and a service provider. Rožman et al. proposed a Shared Manufacturing Protocol (SMP). In this protocol, functions including service discovery, the negotiation between service providers and consumers, transactions, and service evaluation, are implemented on top of smart contracts. This protocol enables a scalable solution for shared manufacturing in accordance with the nature of shared manufacturing concepts.

**Table 2:** *Industry 4.0*

| Author | Title | Year |
|---|---|---|
| Feng Tian | An agri-food supply chain traceability system for China based on RFID and blockchain technology | 2016 |
| Feng Tian | A supply chain traceability system for food safety based on HACCP, blockchain and Internet of things | 2017 |
| Tse et al. | Blockchain application in food supply information security | 2017 |
| Kshetri | 1 Blockchain's roles in meeting key supply chain management objectives | 2018 |
| Kuhi et al. | Ensuring performance measurement integrity in logistics using blockchain | 2018 |
| Mondragon et al. | Exploring the applicability of blockchain technology to enhance manufacturing supply chains in the composite materials industry | 2018 |
| Ko et al. | Blockchain Technology and Manufacturing Industry: Real-Time Transparency and Cost Savings | 2018 |
| Vatankhah Barenji et al. | Blockchain Cloud Manufacturing: Shop Floor and Machine Level | 2018 |
| Angrish et al. | A Case Study for Blockchain in Manufacturing: "FabRec": A Prototype for Peer-to-Peer Network of Manufacturing Nodes | 2018 |
| Wang et al. | Smart Contract-Based Product Traceability System in the Supply Chain Scenario | 2019 |
| Chang et al. | Supply chain re-engineering using blockchain technology: A case of smart contract based tracking process | 2019 |
| Bodkhe et al. | Blockchain for Industry 4.0: A Comprehensive Review | 2020 |
| Dolgui et al. | Blockchain-oriented dynamic modelling of smart contract design and execution in the supply chain | 2020 |
| Kurpjuweit et al. | Blockchain in Additive Manufacturing and its Impact on Supply Chains | 2021 |
| Rožman et al. | Scalable framework for blockchain-based shared manufacturing | 2021 |

## 4.3 P2P energy markets

In a peer-to-peer (P2P) energy market, customers equipped with distributed energy resources (DERs) both produce and consume power. More importantly, they directly trade and share energy with each other. This P2P energy market enables localised energy systems, which are self-managed and robust cells for larger energy systems. However, P2P energy markets have a high diversity of power generation and demand profiles of customers. DERs are subject to a variety of types, features, capacities, locations, and ownership and are spread all over the edges of the power systems. As a result, it is challenging to manage such a system in a centralised way, as it requires acquiring and processing a large amount of data by one party and it may violate the privacy of the users.

A blockchain, which is inherently built and managed in a decentralised way without coordinators, naturally fits the architecture of the P2P energy market [115]. The decentralised nature of data storage also makes the system robust to a single-point failure. In addition, as data in a blockchain are protected by cryptography mechanisms, user privacy is preserved. As a result, a considerable number of works [2, 52, 53, 82, 96, 104, 110, 122] have started to adopt blockchain as the backbone of a P2P energy market.

To improve the efficiency of energy trading, Noor et al. proposed using blockchain to enhance a game theory-based model for demand-side management within micro-grid networks. In this case, blockchain is used to handle micro-transactions along with the exchange of energy and information, creating a transparent energy market. Wang et al. propose a decentralised distribution energy system that uses smart contracts to facilitate the automated or manual sale of surplus energy from users to the grid. Li et al. propose a hierarchical framework for energy demand-side management through blockchain-enabled real-time information exchange in energy markets.

Among the many P2P energy markets designed on top of a blockchain, other than improving the efficiency of the trades, blockchains mainly play the role of protecting privacy and ensuring the security of the trade.

With respect to protecting users privacy, Laszka et al. propose Privacy-preserving Energy Transactions (PETra), which keeps the anonymity of users for communication, bidding, and trading in transactive micro-grids, leveraging the anonymous nature of blockchain. Aitzhan and Svetinovic also presents a blockchain-based design where users communicate via anonymous messaging streams.

Securing the trading in a P2P market is another important role for blockchain [62] as there is no regulatory authority to prevent malicious, dishonest, or unfair actions from users. For example, Li et al. implemented a timed-commitment-based mechanism to guarantee verifiable fairness during energy trading, which utilises the verifiable nature of data on blockchains. Sheikh et al. utilised the advantage of how consensus is reached in blockchain networks and proposed a P2P energy trading mechanism on top of a Byzantine-based blockchain. Huh and Kim also proposed a system that adopts an Hyper Delegation Proof of Randomness (HDPoR) algorithm-based blockchain to make the P2P network robust to attacks.

**Table 3:** *P2P energy market*

| Author | Title | Year |
|---|---|---|
| Sikorski et al. | Blockchain technology in the chemical industry: Machine-to-machine electricity market | 2017 |
| Mannaro et al. | Crypto-trading: Blockchain-oriented energy market | 2017 |
| Sabounchi and Wei | Towards resilient networked microgrids: Blockchain-enabled peer-to-peer electricity trading mechanism | 2017 |
| Peck and Wagman | Energy trading for fun and profit buy your neighbor's rooftop solar power or sell your own-it'll all be on a blockchain | 2017 |
| Horta et al. | Novel market approach for locally balancing renewable energy production and flexible demand | 2017 |
| Laszka et al. | Providing privacy, safety, and security in IoT-based transactive energy systems using distributed ledgers | 2017 |
| Hou et al. | Applying the blockchain technology to promote the development of distributed photovoltaic in China | 2018 |
| Aggarwal et al. | EnergyChain: Enabling Energy Trading for Smart Homes using Blockchains in Smart Grid Ecosystem | 2018 |
| Wang et al. | Blockchain-Assisted Crowdsourced Energy Systems | 2018 |
| Noor et al. | Energy Demand Side Management within micro-grid networks enhanced by blockchain | 2018 |
| Aitzhan and Svetinovic | Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams | 2018 |
| Kim and Huh | A Study on the Improvement of Smart Grid Security Performance and Blockchain Smart Grid Perspective | 2018 |
| Huh and Kim | The Blockchain Consensus Algorithm for Viable Management of New and Renewable Energies | 2019 |
| Wang et al. | Blockchain-based smart contract for energy demand management | 2019 |
| Li et al. | Design and management of a distributed hybrid energy system through smart contract and blockchain | 2019 |
| Li et al. | Blockchain-Enabled Secure Energy Trading With Verifiable Fairness in Industrial Internet of Things | 2020 |
| Sheikh et al. | Secured Energy Trading Using Byzantine-Based Blockchain Consensus | 2020 |
| Teng et al. | A comprehensive review of energy blockchain: Application scenarios and development trends | 2021 |

## 4.4 Emission trading

Blockchain is also widely applied for enhancing environmental sustainability [94]. One prevailing topic is to use blockchain technology to establish or facilitate the emission trading platforms for CO2 or other Green House Gases (GHGs) [95, 99]. For example, Kim and Huh propose the use of a blockchain to measure carbon emission rights among the UN-SDGs' (United Nations Sustainable Development Goals') 17 tasks and hence make the transactions more reliable.

Hartmann and Thomas provide an insightful summary of applying blockchain to carbon markets. The authors put existing blockchain-based carbon markets into four categories: "Networked carbon markets" [56, 80, 125], "Industry 4.0-based carbon markets" [44, 61], "Technolibertarian" [4], and "Voluntary Offset" [72, 73]. In a "networked carbon market", smaller markets form a larger global carbon market. Smaller carbon markets connect and trade with each other through an overarching blockchain. "Industry 4.0-based carbon markets" refer to markets focusing on using smart devices for automated monitoring, reporting, and verification (MRV) and leverage blockchain to match the automated nature of the market. The "Technolibertarian" carbon market aims to use blockchain technology to protect the privacy and security of the market participants and attract participants that have privacy and security concerns. In the "Voluntary Offset" carbon markets, the Ethereum blockchain is used to create Decentralised Autonomous Organisations (DAOs), which host voluntary carbon credit offset projects. In their design, universities manage the DAOs, and the DAOs raise capital through Initial Coin Offerings (ICOs). When participants in this carbon market successfully offset carbon emissions, the DAOs will issue carbon credits to them in the form of cryptocurrency.

Saraji and Borowczak proposed a blockchain-based carbon credit ecosystem. In this ecosystem, carbon credits will be converted into digital tokens and distributed to carbon credit generators (*e.g.* wind farms, CO2 sequestration projects, *etc.*) after their projects are validated by validators.

Yan and Grid proposed a blockchain for transacting energy and carbon allowance in networked microgrids. The two types of participants are microgrids (MGs) [76] and distribution system operators (DSOs) [12, 32]. The system implements two types of smart contracts: market-clearing contracts and transaction settlement contracts. The market-clearing contracts serve as interfaces for MGs to submit energy and carbon trade data to DSOs. These contracts also have a schedule to collect and deliver the trading data to the DSO. After the DSOs clear the market by calculating the optimal dispatch and payoff allocations among MGs based on the data, the market-clearing contract will automatically broadcast the clearing results to all MGs. The transaction settlement contracts would query smart meters to get real-time data, such as carbon allowance generation or consumption, and compare them with the market clearing results provided by the market-clearing contract. According to whether the MGs have fulfilled their commitments, transactions or penalties will be automatically executed by the transaction settlement contract. This design leverages smart contracts to provide automated yet fair market clearing and transaction settlement.

Another trend in incorporating blockchain into emission trading markets is to integrate distributed energy markets with emission markets. Hua et al. propose a blockchain-based peer-to-peer trading framework to exchange energy and carbon allowances. He et al. propose a novel mechanism that integrates the blockchain-based distributed photovoltaic power generation market and the blockchain-based carbon market, where carbon credits and electricity can be traded with each other, enabled by cross-chain transaction technology. This design allows the two markets to adopt independent blockchain implementations.

## 4.5 Smart cities

The smart city concept deeply integrates the concept of IoT and information and communication technology (ICT). IoT networks, services, and the flow of massive amounts of data support the daily operation of a smart city. Similar to IoT networks, decentralised architectures are widely adopted in smart cities to couple with the vast scale of systems.

An important application of blockchain technology in smart cities is to implement decentralised authentication and authorisation mechanisms [100], which are essential for smart cities [71]. Due to their vast size and ever-growing nature [64], smart cities inevitably need to adopt a multi-tenant deployment model that integrates various infrastructure systems. Different systems have their own set of security policies and identity management mechanisms. These policies and identity management mechanisms must be available to other systems to enable cooperation between systems. However, the response will be slow if the access control policies and identity attributes are stored within a centralised database owned by a trusted third party. Also, the system will be vulnerable to single-point-failure and insider attacks. It will be more efficient if a local copy of all the valid security policies and identity attributes is available. However, it is challenging to keep consistent replicas of records within the context of an asynchronous system. Also, it is challenging to guarantee the integrity of the data. Blockchain technology offers a solution to this problem [134]. On the one hand, a blockchain uses distributed consensus algorithms tolerant of crashing and byzantine failures. Therefore, the consistency of replicated data on the local copies is guaranteed, even if the environment is distributed and asynchronous. On the other hand, the tamper-proof nature of blockchains ensures the integrity of the data on the blockchain. Esposito et al. propose a very practical implementation that enables localised and decentralised management of authentication and authorisation in smart cities, incorporating blockchains with the existing authentication and authorisation mechanisms from the FIWARE platform [6]. Vivekanandan et al. presents a blockchain-based IoT device-to-device authentication protocol for smart city applications using 5G technology. Ferreira et al. develop API Gateways for IoT devices to sign, identify, and authorise messages, which use keys and essential characteristics of the devices registered in blockchains in advance.

It is also evident that data is the cornerstone of a smart city. As a result, many works aim to leverage blockchain to facilitate and secure the transition, management, and utilisation of data, with a focus on protecting privacy. Ramachandran Gowri et al. present a proof-of-concept decentralised data marketplace, where buyers and sellers can directly trade IoT data with each other. Smart contracts are used for sellers to register their products and for buyers to discover them. A Streaming Data Payment Protocol (SDPP) [97] will transmit data to the buyer upon blockchain-based transaction. Lastly, a rating smart contract

**Table 4:** *Emission trading*

| Author | Title | Year |
|---|---|---|
| Al Kawasmi et al. | Bitcoin-Based Decentralized Carbon Emissions Trading Infrastructure Model | 2015 |
| Macinante | Networking Carbon Markets : Key Elements of the Process | 2016 |
| Jackson et al. | Networked Carbon Markets: Permissionless Innovation with Distributed Ledgers? | 2017 |
| Li et al. | Networked Microgrids for Enhancing the Power System Resilience | 2017 |
| Leonhard | Developing the Crypto Carbon Credit on Ethereum's Blockchain | 2017 |
| Leonhard | Forget Paris: Building a Carbon Market in the U.S. Using Blockchain-Based Smart Contracts | 2017 |
| Khaqqi et al. | Incorporating seller/buyer reputation-based system in blockchain-enabled emission trading application | 2018 |
| Fu et al. | Blockchain Enhanced Emission Trading Framework in Fashion Apparel Manufacturing Industry | 2018 |
| World Bank Group | Blockchain and Emerging Digital Technologies for Enhancing Post-2020 Climate Markets | 2018 |
| Patel et al. | Carbon Credits on Blockchain | 2020 |
| Kim and Huh | Blockchain of carbon trading for UN sustainable development goals | 2020 |
| Richardson and Xu | Carbon Trading with Blockchain | 2020 |
| Hartmann and Thomas | Applying Blockchain to the Australian Carbon Market | 2020 |
| Du and Li | A Hierarchical Real-Time Balancing Market Considering Multi-Microgrids With Distributed Sustainable Resources | 2020 |
| Hua et al. | A blockchain based peer-to-peer trading framework integrating energy and carbon markets | 2020 |
| He et al. | Joint Operation Mechanism of Distributed Photovoltaic Power Generation Market and Carbon Market Based on Cross-Chain Trading Technology | 2020 |
| Parmentola et al. | Is blockchain able to enhance environmental sustainability? A systematic review and research agenda from the perspective of Sustainable Development Goals (SDGs) | 2021 |
| Saraji and Borowczak | A Blockchain-based Carbon Credit Ecosystem | 2021 |
| Yan and Grid | Blockchain for Transacting Energy and Carbon Allowance in Networked Microgrids | 2021 |

allows sellers and buyers to rate each other. Yu et al. propose a data auditing blockchain (DAB) that stores auditing proofs of big data and uses Practical Byzantine Fault Tolerance (PBFT). Biswas and Muthukkumarasamy present a blockchain-enabled framework for secure communication between smart devices in the context of smart cities.

To ensure trust and protect privacy in data sharing, Sun and Zhang propose a decentralised blockchain-based trust service for sharing government information resources in the context of a smart city. Shen et al. develop a privacy-preserving mechanism for sharing blockchain encrypted IoT data for Support Vector Machine (SVM) model training in the context of smart cities. PrivySharing [81] is designed to ensure privacy in sharing data via blockchain and also to use smart contracts to implement access control of data.

Some services in smart cities also benefit from blockchain technology. Lin et al. propose a trading mechanism for vehicles to trade their idle computer capability via blockchain, which preserves privacy and ensures transaction security. Zhang et al. presents a crowd-sourcing system, which is built on top of smart contracts for smart cities. A crowd-sourcing service is an essential part of an informational city. However, it is also a vulnerable service to malicious or dishonest behaviours and lacks a trust-ensuring mechanism. Therefore, this crowd-sourcing system uses smart contracts to monitor and control each step of the crowd-sourcing service preventing malicious behaviours such as submitting substandard results and refusing to pay even when the tasks are fulfilled. Liao and Wang design a decentralised lottery system for smart cities, where smart contracts ensure fairness, transparency, and privacy.

# 5 Knowledge graphs and blockchain

Knowledge graphs (KGs) have been identified as a promising technology for chemical engineering [9, 11, 40, 85]. The World Avatar Knowledge Graph (TWA) [33] is an example of applying KG technology to the chemical engineering domain.

Knowledge graphs utilise Semantic Web technology [13, 47] to represent information in a machine-readable way, where concepts, entities, and the relations between them are formally defined and connected. Through the links between instances, it is convenient to retrieve and navigate through related data within a KG.

More importantly, by applying the Linked Data principals [18] and linking knowledge from different domains, KGs interconnect previously isolated datasets. For example, the instance of a power plant can be connected to a city instance via an "isLocatedIn" location, while another connection between the instance of natural gas can be connected to this power plant by the "hasPrimarilyFuel" relation. Further, the physical and chemical properties of natural gas, such as its molecular weight, can be also connected to the instance of natural gas. As a result, a KG provides a common ground for accessing data from different domains or multiple levels [88] and guarantees that related data can be easily queried. For example, the TWA integrates geospatial data [23], datasets for quantum calculation [66], datasets for chemical kinetic reaction mechanisms [39], power systems [26], *etc.*

Agents are introduced into TWAs to update the TWAs over time. Taking a city as an example, the real-time weather data is dynamic. Therefore, a weather agent is implemented

**Table 5:** *Smart city*

| Author | Title | Year |
|---|---|---|
| Biswas et al. | Securing Smart Cities Using Blockchain Technology | 2016 |
| Rivera et al. | How digital identity on blockchain can contribute in a smart city environment | 2017 |
| Liao and Wang | Design of a Blockchain-Based Lottery System for Smart Cities Applications | 2017 |
| Zhang et al. | Cyber-Physical-Social Systems: The State of the Art and Perspectives | 2018 |
| Ramachandran et al. | Towards a Decentralized Data Marketplace for Smart Cities | 2018 |
| Radhakrishnan et al. | Streaming Data Payment Protocol (SDPP) for the Internet of Things | 2018 |
| Shen et al. | Privacy-Preserving Support Vector Machine Training Over Blockchain-Based Encrypted IoT Data in Smart Cities | 2019 |
| Yu et al. | Decentralized Big Data Auditing for Smart City Environments Leveraging Blockchain Technology | 2019 |
| Alonso et al. | An Identity Framework for Providing Access to FIWARE OAuth 2.0-Based Services According to the eIDAS European Regulation | 2019 |
| Laufs et al. | Security and the smart city: A systematic review | 2020 |
| Sun and Zhang | Research on the application of block chain big data platform in the construction of new smart city for low carbon emission and green environment | 2020 |
| Makhdoom et al. | PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities | 2020 |
| Kirimtat et al. | Future Trends and Current State of Smart City Concepts: A Survey | 2020 |
| Zahed Benisi et al. | Blockchain-based decentralized storage networks: A survey | 2020 |
| Lin et al. | Blockchain-based On-Demand Computing Resource Trading in IoV-Assisted Smart City | 2020 |
| Esposito et al. | Blockchain-based authentication and authorization for smart city applications | 2021 |
| Ferreira et al. | IoT Registration and Authentication in Smart City Applications with Blockchain | 2021 |

to update the weather attributes of this city dynamically. To enable the automated discovery, composition, and execution of agents, the semantic description of agents are created and integrated into TWA [137]. The integration between semantic agents and the KG makes it possible to obtain dynamic properties of instances in TWA.

With the common ground for accessing data in KGs and the agents to provide real-time information, it is possible to efficiently implement applications demanding complex data inputs. For example, to simulate the real-time dispersion of emissions from all power plants within a city, which requires the geographical and building model of the city, the locations and operation details of all the power plants in this city, the type of emission of the plants, the real-time weather in this city, *etc.*

Similar to a smart city, the implementation of KG is an integration of many components from heterogeneous sources, due to its vast scale and cross-domain nature. The data is provided by different parties or different IoT networks, agents are implemented by different service providers and are of different quality. Due to its vast scale, validation and management of participants, and the data or agents they provide, in a centralised way is highly inefficient. One prominent problem is how to ensure or verify the quality of service (QoS) [84] of the agents.

When TWA is applied in a production environment, the quality of service of the agents is vital. Moreover, some proprietary agents will charge users for usage. As a result, it is necessary to implement a marketplace of agents on top of the KG that can provide trust for the QoS of the agents and provide means to automatically settle the payment for using the agents.

In the context of establishing such an agent marketplace, there several advantages of blockchain technology. Firstly, blockchain can provide tamper-proof record-keeping without a centralised authority. Secondly, automated, secured, and unbiased payment settlement mechanisms and other mechanisms can be implemented on top of blockchain-based smart contracts.

As a result, blockchain technology, especially the blockchain-based smart contract, is applied to build a decentralised agent marketplace [138], which deeply integrates knowledge graph technology.

Firstly, semantic descriptions of the agents, especially their I/O signatures, are stored in TWA. As a result, any participants can then discover the agents by specifying the I/O signatures of the agents they want through an off-chain agent discovery system. The schema of the inputs and outputs of the agents is also provided by their description.

An agent registry and lookup system is implemented on top of Ethereum smart contracts, where developers of the agents can register their agents and store the IRIs, URLs, and prices of the agents in the Etheruem blockchain. After an agent is registered on the blockchain, it will be assigned a unique address on the blockchain. This address will be updated to the semantic description of this agent in TWA. A reputation system is also implemented on top of smart contracts, where smart contracts independently analyse the performance of agents and update QoS ratings of agents to the blockchain. In addition, a smart contract-based payment system is also implemented, which automatically settles payments after an agent is invoked and rated.

The workflow of this agent marketplace is as follows: when a user discovers an agent from TWA, the user goes to the smart contract-based agent registry and lookup system to find the agent address on the blockchain. Via the agent registry and agent reputation smart contracts, the user then obtains the agent rating and price. According to the rating and price, the user can make their choice.

The user then submits the agent address and input data to the agent marketplace, which will invoke the agent for the user. After the result is returned, smart contracts will carry out performance evaluations and update the performance ratings of the agents in the blockchain. With the performance score of this particular invocation, the payment amount is calculated by the smart contracts. Then the smart contract will make the payment to the developer with credits topped up by the user.

The processes of obtaining the agent ratings, the invocation, the evaluation of the agent performance, the updating of the agent ratings, and the payment settlement, are all managed by smart contracts and therefore are not vulnerable to outside or inside attacks. With its decentralised architecture, this agent marketplace requires no central administration and therefore it is scalable and cost-effective.

# 6 Conclusion

In this paper, we introduced the implementation of blockchain and blockchain-based smart contracts and elaborated on how their features are enabled. 2,527 articles are collected and 158 of them are reviewed. The articles are categorised into 5 fields: Internet of Things, Industry 4.0, P2P energy markets, emission trading, and smart cities. From this review, we notice the common trends of establishing decentralised systems in these 5 fields, which create very practical motivations for applying blockchain and smart contracts. Blockchains are generally used to implement a trust layer in a permission-less, trust-less, and anonymous environment. Smart contracts are often applied to provide distributed and autonomous control and management in those decentralised systems.

With the proliferation of blockchain technology, more and more new types of consensus mechanisms are introduced and enable new types of blockchains with different features. One prominent example is to use PoS blockchain instead of PoW to address the energy consumption problem. As a result, it can be seen that some works are trying new types of blockchains to design decentralised systems that suit their scenarios better. We also recognise a trend that smart contracts are more and more frequently leveraged to build complex decentralised applications, to enhance the self-managing nature of the decentralised systems.

# Acknowledgements

This project is supported by CMCL Innovations and the National Research Foundation(NRF), Prime Minister' s Office, Singapore under its Campus for Research Excellence and Technological Enterprise(CREATE) programme. Markus Kraft acknowledges the support of the Alexander von Humboldt foundation. The authors would also like to thank Andrew Charles Breeson for proofreading and making figures.

# References


[1] S. Aggarwal and N. Kumar. Chapter eleven - cryptographic consensus mechanisms. In S. Aggarwal, N. Kumar, and P. Raj, editors, *The Blockchain Technology for Secure and Smart Applications across Industry Verticals*, volume 121 of *Advances in Computers*, pages 211–226. Elsevier, 2021. doi:https://doi.org/10.1016/bs.adcom.2020.08.011.

[2] S. Aggarwal, R. Chaudhary, G. S. Aujla, A. Jindal, A. Dua, and N. Kumar. EnergyChain: Enabling Energy Trading for Smart Homes using Blockchains in Smart Grid Ecosystem. In *Proceedings of the 1st ACM MobiHoc Workshop on Networking and Cybersecurity for Smart Cities*, pages 1–6, Los Angeles CA USA, 2018. ACM. doi:10.1145/3214701.3214704.

[3] N. Z. Aitzhan and D. Svetinovic. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE Transactions on Dependable and Secure Computing*, 15:840–852, 2018. doi:10.1109/TDSC.2016.2616861.

[4] E. Al Kawasmi, E. Arnautovic, and D. Svetinovic. Bitcoin-Based Decentralized Carbon Emissions Trading Infrastructure Model. *Systems Engineering*, 18(2):115–130, 2015. doi:10.1002/sys.21291.

[5] V. Allombert, M. Bourgoin, and J. Tesson. Introduction to the Tezos Blockchain. In *2019 International Conference on High Performance Computing & Simulation (HPCS)*, pages 1–10. IEEE, 2019. doi:10.1109/HPCS48598.2019.9188227.

[6] A. Alonso, A. Pozo, J. Choque, G. Bueno, J. Salvachua, L. Diez, J. Marin, and P. L. C. Alonso. An Identity Framework for Providing Access to FIWARE OAuth 2.0-Based Services According to the eIDAS European Regulation. *IEEE Access*, 7:88435–88449, 2019. doi:10.1109/ACCESS.2019.2926556.

[7] A. Angrish, B. Craver, M. Hasan, and B. Starly. A Case Study for Blockchain in Manufacturing: “FabRec”: A Prototype for Peer-to-Peer Network of Manufacturing Nodes. *Procedia Manufacturing*, 26:1180–1192, 2018. doi:10.1016/j.promfg.2018.07.154.

[8] L. Atzori, A. Iera, and G. Morabito. The Internet of Things: A survey. *Computer Networks*, 54(15):2787–2805, 2010. doi:10.1016/j.comnet.2010.05.010.

[9] S. Auer, V. Kovtun, M. Prinz, A. Kasprzik, M. Stocker, and M. E. Vidal. Towards a Knowledge Graph for Science. In *Proceedings of the 8th International Conference on Web Intelligence, Mining and Semantics*, pages 1–6, New York, NY, USA, 2018. ACM. doi:10.1145/3227609.3227689.

[10] L. M. Bach, B. Mihaljevic, and M. Zagar. Comparative analysis of blockchain consensus algorithms. In *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pages 1545–1550. IEEE, 2018. doi:10.23919/MIPRO.2018.8400278.

[11] J. Bai, R. Geeson, F. Farazi, S. Mosbach, J. Akroyd, E. J. Bringley, and M. Kraft. Automated Calibration of a Poly(oxymethylene) Dimethyl Ether Oxidation Mechanism Using the Knowledge Graph Technology. *Journal of Chemical Information and Modeling*, 61(4):1701–1717, 2021. doi:10.1021/acs.jcim.0c01322.

[12] L. Bai, J. Wang, C. Wang, C. Chen, and F. Li. Distribution Locational Marginal Pricing (DLMP) for Congestion Management and Voltage Support. *IEEE Transactions on Power Systems*, 33(4):4061–4073, 2018. doi:10.1109/TPWRS.2017.2767632.

[13] T. Berners-Lee, J. Hendler, and O. Lassila. Semantic web. *Sci. Am.*, 284(5):34–43, 2001. URL http://www.jstor.org/stable/26059207.

[14] K. Biswas and V. Muthukkumarasamy. Securing Smart Cities Using Blockchain Technology. In *2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, pages 1392–1393, Sydney, Australia, 2016. IEEE. doi:10.1109/HPCC-SmartCity-DSS.2016.0198.

[15] Bitcoin Explorer. Bitcoin explorer, 2021. URL https://www.blockchain.com/explorer. Last accessed 01 October 2021.

[16] bitcoin wiki. Script, 2016. URL https://en.bitcoin.it/w/index.php?title=Script&oldid=61707. Last accessed 01 October 2021.

[17] bitnodes. Global bitcoin nodes distribution, 2021. URL https://ycharts.com/indicators/reports/ethereum_statistics. Last accessed 01 October 2021.

[18] C. Bizer, T. Heath, and T. Berners-Lee. Linked Data - The Story So Far. *International Journal on Semantic Web and Information Systems*, 5(3):1–22, 2009. doi:10.4018/jswis.2009081901.

[19] U. Bodkhe, S. Tanwar, K. Parekh, P. Khanpara, S. Tyagi, N. Kumar, and M. Alazab. Blockchain for Industry 4.0: A Comprehensive Review. *IEEE Access*, 8:79764–79800, 2020. doi:10.1109/ACCESS.2020.2988579.

[20] R. Browne. Bitcoin's wild ride renews worries about its massive carbon footprint, 2021. URL https://www.cnbc.com/2021/02/05/bitcoin-btc-surge-renews-worries-about-its-massive-carbon-footprint.html. Last accessed 01 October 2021.

[21] V. Buterin. Ethereum: A next-generation smart contract and decentralized application platform, 2013. http://ethereum.org/ethereum.html last accessed: October 7, 2021.

[22] Cardano. Cardano developer portal, 2021. URL https://developers.cardano.org/. Last accessed 01 October 2021.

[23] A. Chadzynski, N. Krdzavac, F. Farazi, M. Q. Lim, S. Li, A. Grisiute, P. Herthogs, A. von Richthofen, S. Cairns, and M. Kraft. Semantic 3D City Database — An enabler for a dynamic geospatial knowledge graph. *Energy and AI*, 6:100106, 2021. doi:10.1016/j.egyai.2021.100106.

[24] S. E. Chang, Y.-C. Chen, and M.-F. Lu. Supply chain re-engineering using blockchain technology: A case of smart contract based tracking process. *Technological Forecasting and Social Change*, 144:1–11, 2019. doi:10.1016/j.techfore.2019.03.015.

[25] C. Dannen. *Introducing Ethereum and Solidity*. Apress, Berkeley, CA, 2017. doi:10.1007/978-1-4842-2535-6.

[26] A. Devanand, G. Karmakar, N. Krdzavac, R. Rigo-Mariani, Y. Foo Eddy, I. A. Karimi, and M. Kraft. OntoPowSys: A power system ontology for cross domain interactions in an eco industrial park. *Energy and AI*, 1:100008, 2020. doi:10.1016/j.egyai.2020.100008.

[27] M. L. Di Silvestre, P. Gallo, J. M. Guerrero, R. Musca, E. Riva Sanseverino, G. Sciumè, J. C. Vásquez, and G. Zizzo. Blockchain for power systems: Current trends and future applications. *Renewable and Sustainable Energy Reviews*, 119:109585, 2020. doi:10.1016/j.rser.2019.109585.

[28] Digiconomist. Bitcoin energy consumption index, 2020. URL `https://digiconomist.net/bitcoin-energy-consumption`. Last accessed 01 October 2021.

[29] A. Dolgui, D. Ivanov, S. Potryasaev, B. Sokolov, M. Ivanova, and F. Werner. Blockchain-oriented dynamic modelling of smart contract design and execution in the supply chain. *International Journal of Production Research*, 58(7):2184–2199, 2020. doi:10.1080/00207543.2019.1627439.

[30] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram. Blockchain for IoT security and privacy: The case study of a smart home. In *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pages 618–623, Kona, HI, 2017. IEEE. doi:10.1109/PERCOMW.2017.7917634.

[31] J. R. Douceur. The sybil attack. In P. Druschel, F. Kaashoek, and A. Rowstron, editors, *Peer-to-Peer Systems*, pages 251–260, Berlin, Heidelberg, 2002. Springer Berlin Heidelberg.

[32] Y. Du and F. Li. A Hierarchical Real-Time Balancing Market Considering Multi-Microgrids With Distributed Sustainable Resources. *IEEE Transactions on Sustainable Energy*, 11(1):72–83, 2020. doi:10.1109/TSTE.2018.2884223.

[33] A. Eibeck, M. Q. Lim, and M. Kraft. J-Park Simulator: An ontology-based platform for cross-domain scenarios in process industry. *Computers & Chemical Engineering*, 131:106586, 2019. doi:10.1016/j.compchemeng.2019.106586.

[34] E. Elrom. NEO Blockchain and Smart Contracts. In *The Blockchain Developer*, pages 257–298. Apress, Berkeley, CA, 2019. doi:10.1007/978-1-4842-4847-8_7.

[35] C. Esposito, M. Ficco, and B. B. Gupta. Blockchain-based authentication and authorization for smart city applications. *Information Processing & Management*, 58(2):102468, 2021. doi:10.1016/j.ipm.2020.102468.

[36] ether nodes. Ethereum mainnet statistics, 2021. URL `https://ethernodes.org/`. Last accessed 01 October 2021.

[37] ether scan. The ethereum blockchain explorer, 2021. URL `https://etherscan.io/`. Last accessed 01 October 2021.

[38] X. Fan, L. Liu, R. Zhang, Q. Jing, and J. Bi. Decentralized Trust Management. *ACM Computing Surveys*, 53(1):1–33, 2020. doi:10.1145/3362168.

[39] F. Farazi, J. Akroyd, S. Mosbach, P. Buerger, D. Nurkowski, M. Salamanca, and M. Kraft. OntoKin: An Ontology for Chemical Kinetic Reaction Mechanisms. *Journal of Chemical Information and Modeling*, 60(1):108–120, 2020. doi:10.1021/acs.jcim.9b00960.

[40] F. Farazi, M. Salamanca, S. Mosbach, J. Akroyd, A. Eibeck, L. K. Aditya, A. Chadzynski, K. Pan, X. Zhou, S. Zhang, M. Q. Lim, and M. Kraft. Knowledge Graph Approach to Combustion Chemistry and Interoperability. *ACS Omega*, 5(29):18342–18348, 2020. doi:10.1021/acsomega.0c02055.

[41] Feng Tian. An agri-food supply chain traceability system for China based on RFID & blockchain technology. In *2016 13th International Conference on Service Systems and Service Management (ICSSSM)*, pages 1–6. IEEE, 2016. doi:10.1109/ICSSSM.2016.7538424.

[42] Feng Tian. A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things. In *2017 International Conference on Service Systems and Service Management*, pages 1–6. IEEE, 2017. doi:10.1109/ICSSSM.2017.7996119.

[43] C. M. S. Ferreira, C. T. B. Garrocho, R. A. R. Oliveira, J. S. Silva, and C. F. M. d. C. Cavalcanti. IoT Registration and Authentication in Smart City Applications with Blockchain. *Sensors*, 21(4):1323, 2021. doi:10.3390/s21041323.

[44] B. Fu, Z. Shu, and X. Liu. Blockchain Enhanced Emission Trading Framework in Fashion Apparel Manufacturing Industry. *Sustainability*, 10(4):1105, 2018. doi:10.3390/su10041105.

[45] U. Gallersdörfer, L. Klaaßen, and C. Stoll. Energy Consumption of Cryptocurrencies Beyond Bitcoin. *Joule*, 4(9):1843–1846, 2020. doi:10.1016/j.joule.2020.07.013.

[46] G. Greenspan. Multichain private blockchain-white paper. *URl: http://www. multichain. com/download/MultiChain-White-Paper. pdf*, pages 57–60, 2015.

[47] T. Gruber. Ontology. In *Encyclopedia of Database Systems*, pages 1963–1965. Springer US, Boston, MA, 2009. doi:10.1007/978-0-387-39940-9_1318.

[48] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni. Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. *Computers and Security*, 78:126–142, 2018. doi:10.1016/j.cose.2018.06.004.

[49] Q. Hao, F. Zhang, Z. Liu, and L. Qin. Design of Chemical Industrial Park Integrated Information Management Platform Based on Cloud Computing and IOT (The Internet of Things) Technologies. *International Journal of Smart Home*, 9(4): 35–46, 2015. doi:10.14257/ijsh.2015.9.4.04.

[50] S. Hartmann and S. Thomas. Applying Blockchain to the Australian Carbon Market. *Economic Papers: A journal of applied economics and policy*, 39(2):133–151, 2020. doi:10.1111/1759-3441.12266.

[51] H. He, Z. Luo, Q. Wang, M. Chen, H. He, L. Gao, and H. Zhang. Joint Operation Mechanism of Distributed Photovoltaic Power Generation Market and Carbon Market Based on Cross-Chain Trading Technology. *IEEE Access*, 8:66116–66130, 2020. doi:10.1109/ACCESS.2020.2985577.

[52] J. Horta, D. Kofman, D. Menga, and A. Silva. Novel market approach for locally balancing renewable energy production and flexible demand. *2017 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pages 533–539, 2017. doi:10.1109/SmartGridComm.2017.8340728.

[53] J. Hou, H. Wang, and P. Liu. Applying the blockchain technology to promote the development of distributed photovoltaic in China. *International Journal of Energy Research*, 42(6):2050–2069, 2018. doi:10.1002/er.3984.

[54] W. Hua, J. Jiang, H. Sun, and J. Wu. A blockchain based peer-to-peer trading framework integrating energy and carbon markets. *Applied Energy*, 279:115539, 2020. doi:10.1016/j.apenergy.2020.115539.

[55] J.-H. Huh and S.-K. Kim. The Blockchain Consensus Algorithm for Viable Management of New and Renewable Energies. *Sustainability*, 11(11):3184, 2019. doi:10.3390/su11113184.

[56] A. Jackson, A. Lloyd, J. Macinante, and M. HHwener. Networked Carbon Markets: Permissionless Innovation with Distributed Ledgers? *SSRN Electronic Journal*, 2017. doi:10.2139/ssrn.2997099.

[57] M. Jansen, F. Hdhili, R. Gouiaa, and Z. Qasem. Do smart contract languages need to be turing complete? In J. Prieto, A. K. Das, S. Ferretti, A. Pinto, and J. M. Corchado, editors, *Blockchain and Applications*, pages 19–26. Springer International Publishing, 2020.

[58] M. Kamran, H. U. Khan, W. Nisar, M. Farooq, and S.-U. Rehman. Blockchain and Internet of Things: A bibliometric study. *Computers and Electrical Engineering*, 81:106525, 2020. doi:10.1016/j.compeleceng.2019.106525.

[59] U. Khalid, M. Asim, T. Baker, P. C. K. Hung, M. A. Tariq, and L. Rafferty. A decentralized lightweight blockchain-based authentication mechanism for IoT systems. *Cluster Computing*, 23(3):2067–2087, 2020. doi:10.1007/s10586-020-03058-6.

[60] M. A. Khan and K. Salah. IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, 82:395–411, 2018. doi:10.1016/j.future.2017.11.022.

[61] K. N. Khaqqi, J. J. Sikorski, K. Hadinoto, and M. Kraft. Incorporating seller/buyer reputation-based system in blockchain-enabled emission trading application. *Applied Energy*, 209:8–19, 2018. doi:10.1016/j.apenergy.2017.10.070.

[62] S.-K. Kim and J.-H. Huh. A Study on the Improvement of Smart Grid Security Performance and Blockchain Smart Grid Perspective. *Energies*, 11(8):1973, 2018. doi:10.3390/en11081973.

[63] S. K. Kim and J. H. Huh. Blockchain of carbon trading for UN sustainable development goals. *Sustainability (Switzerland)*, 12(10), 2020. doi:10.3390/SU12104021.

[64] A. Kirimtat, O. Krejcar, A. Kertesz, and M. F. Tasgetiren. Future Trends and Current State of Smart City Concepts: A Survey. *IEEE Access*, 8:86448–86467, 2020. doi:10.1109/ACCESS.2020.2992441.

[65] T. Ko, J. Lee, and D. Ryu. Blockchain Technology and Manufacturing Industry: Real-Time Transparency and Cost Savings. *Sustainability*, 10(11):4274, 2018. doi:10.3390/su10114274.

[66] N. Krdzavac, S. Mosbach, D. Nurkowski, P. Buerger, J. Akroyd, J. Martin, A. Menon, and M. Kraft. An Ontology and Semantic Web Service for Quantum Chemistry Calculations. *Journal of Chemical Information and Modeling*, 59(7): 3154–3165, 2019. doi:10.1021/acs.jcim.9b00227.

[67] N. Kshetri. 1 Blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management*, 39:80–89, 2018. doi:10.1016/j.ijinfomgt.2017.12.005.

[68] K. Kuhi, K. Kaare, and O. Koppel. Ensuring performance measurement integrity in logistics using blockchain. In *2018 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI)*, pages 256–261. IEEE, 2018. doi:10.1109/SOLI.2018.8476737.

[69] S. Kurpjuweit, C. G. Schmidt, M. Klöckner, and S. M. Wagner. Blockchain in Additive Manufacturing and its Impact on Supply Chains. *Journal of Business Logistics*, 42(1):46–70, 2021. doi:10.1111/jbl.12231.

[70] A. Laszka, A. Dubey, M. Walker, and D. Schmidt. Providing privacy, safety, and security in iot-based transactive energy systems using distributed ledgers. In *Proceedings of the Seventh International Conference on the Internet of Things*, pages 1–8. ACM, 2017. doi:10.1145/3131542.3131562.

[71] J. Laufs, H. Borrion, and B. Bradford. Security and the smart city: A systematic review. *Sustainable Cities and Society*, 55:102023, 2020. doi:10.1016/j.scs.2020.102023.

[72] R. D. Leonhard. Developing the Crypto Carbon Credit on Ethereum's Blockchain. *SSRN Electronic Journal*, 2017. doi:10.2139/ssrn.3000472.

[73] R. D. Leonhard. Forget Paris: Building a Carbon Market in the U.S. Using Blockchain-Based Smart Contracts. *SSRN Electronic Journal*, 2017. doi:10.2139/ssrn.3082450.

[74] M. Li, D. Hu, C. Lal, M. Conti, and Z. Zhang. Blockchain-enabled secure energy trading with verifiable fairness in industrial internet of things. *IEEE Transactions on Industrial Informatics*, 16:6564–6574, 2020. doi:10.1109/TII.2020.2974537.

[75] Y. Li, W. Yang, P. He, C. Chen, and X. Wang. Design and management of a distributed hybrid energy system through smart contract and blockchain. *Applied Energy*, 248:390–405, 2019. doi:10.1016/j.apenergy.2019.04.132.

[76] Z. Li, M. Shahidehpour, F. Aminifar, A. Alabdulwahab, and Y. Al-Turki. Networked Microgrids for Enhancing the Power System Resilience. *Proceedings of the IEEE*, 105(7):1289–1310, 2017. doi:10.1109/JPROC.2017.2685558.

[77] D.-Y. Liao and X. Wang. Design of a Blockchain-Based Lottery System for Smart Cities Applications. In *2017 IEEE 3rd International Conference on Collaboration and Internet Computing (CIC)*, pages 275–282, San Jose, CA, 2017. IEEE. doi:10.1109/CIC.2017.00044.

[78] X. Lin, J. Wu, S. Mumtaz, S. Garg, J. Li, and M. Guizani. Blockchain-based On-Demand Computing Resource Trading in IoV-Assisted Smart City. *IEEE Transactions on Emerging Topics in Computing*, page 1, 2020. doi:10.1109/TETC.2020.2971831.

[79] C. Machado, F. Medeiros, and A. Antonio. IoT Data Integrity Verification for Cyber-Physical Systems Using Blockchain. In *2018 IEEE 21st International Symposium on Real-Time Distributed Computing (ISORC)*, pages 83–90. IEEE, 2018. doi:10.1109/ISORC.2018.00019.

[80] J. Macinante. Networking Carbon Markets : Key Elements of the Process, 2016. URL `https://openknowledge.worldbank.org/handle/10986/25750`. Last accessed 01 October 2021.

[81] I. Makhdoom, I. Zhou, M. Abolhasan, J. Lipman, and W. Ni. PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. *Computers & Security*, 88:101653, 2020. doi:10.1016/j.cose.2019.101653.

[82] K. Mannaro, A. Pinna, and M. Marchesi. Crypto-trading: Blockchain-oriented energy market. In *2017 AEIT International Annual Conference*, pages 1–5, Cagliari, 2017. IEEE. doi:10.23919/AEIT.2017.8240547.

[83] I. Mayusda and I. I. Wiratmadja. The Development of Industry 4.0 Readiness Model. Case Study in Indonesia's Priority Industrial Sector of Chemical. In *iMEC-APCOMS 2019*, pages 140–146. Springer, 2020. doi:10.1007/978-981-15-0950-6_22.

[84] D. Menasce. QoS issues in Web services. *IEEE Internet Computing*, 6(6):72–75, 2002. doi:10.1109/MIC.2002.1067740.

[85] A. Menon, N. B. Krdzavac, and M. Kraft. From database to knowledge graph — using data in chemistry. *Current Opinion in Chemical Engineering*, 26:33–37, 2019. doi:10.1016/j.coche.2019.08.004.

[86] S. Mohan and R. Katakojwala. The circular chemistry conceptual framework: A way forward to sustainability in industry 4.0. *Current Opinion in Green and Sustainable Chemistry*, 28:100434, 2021. doi:10.1016/j.cogsc.2020.100434.

[87] A. E. C. Mondragon, C. E. C. Mondragon, and E. S. Coronado. Exploring the applicability of blockchain technology to enhance manufacturing supply chains in the composite materials industry. In *2018 IEEE International Conference on Applied System Invention (ICASI)*, pages 1300–1303. IEEE, 2018. doi:10.1109/ICASI.2018.8394531.

[88] S. Mosbach, A. Menon, F. Farazi, N. Krdzavac, X. Zhou, J. Akroyd, and M. Kraft. Multiscale Cross-Domain Thermochemical Knowledge-Graph. *Journal of Chemical Information and Modeling*, 60(12):6155–6166, 2020. doi:10.1021/acs.jcim.0c01145.

[89] A. Muthanna, A. A. Ateya, A. Khakimov, I. Gudkova, A. Abuarqoub, K. Samouylov, and A. Koucheryavy. Secure and Reliable IoT Networks Using Fog Computing with Software-Defined Networking and Blockchain. *Journal of Sensor and Actuator Networks*, 8(1):15, 2019. doi:10.3390/jsan8010015.

[90] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, page 21260, 2008.

[91] S. Nakamoto. Re: Bitcoin p2p e-cash paper, 2008. URL `https://users.encs.concordia.ca/~clark/biblio/bitcoin/Nakamoto%202008.pdf`. Last accessed 01 October 2021.

[92] Y. Nakamura, Y. Zhang, M. Sasabe, and S. Kasahara. Exploiting Smart Contracts for Capability-Based Access Control in the Internet of Things. *Sensors*, 20(6): 1793, 2020. doi:10.3390/s20061793.

[93] S. Noor, W. Yang, M. Guo, K. H. van Dam, and X. Wang. Energy Demand Side Management within micro-grid networks enhanced by blockchain. *Applied Energy*, 228:1385–1398, 2018. doi:10.1016/j.apenergy.2018.07.012.

[94] A. Parmentola, A. Petrillo, I. Tutore, and F. De Felice. Is blockchain able to enhance environmental sustainability? A systematic review and research agenda from the perspective of Sustainable Development Goals (SDGs). *Business Strategy and the Environment*, 2021. doi:10.1002/bse.2882.

[95] D. Patel, B. Britto, S. Sharma, K. Gaikwad, Y. Dusing, and M. Gupta. Carbon Credits on Blockchain. In *2020 International Conference on Innovative Trends in Information Technology, ICITIIT 2020*, 2020. doi:10.1109/ICITIIT49094.2020.9071536.

[96] M. E. Peck and D. Wagman. Energy trading for fun and profit buy your neighbor's rooftop solar power or sell your own-it'll all be on a blockchain. *IEEE Spectrum*, 54(10):56–61, 2017. doi:10.1109/MSPEC.2017.8048842.

[97] R. Radhakrishnan and B. Krishnamachari. Streaming Data Payment Protocol (SDPP) for the Internet of Things. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pages 1679–1684. IEEE, 2018. doi:10.1109/Cybermatics_2018.2018.00280.

[98] S. Ramachandran Gowri, R. Radhakrishnan, and B. Krishnamachari. Towards a Decentralized Data Marketplace for Smart Cities. In *2018 IEEE International Smart Cities Conference (ISC2)*, pages 1–8, Kansas City, MO, USA, 2018. IEEE. doi:10.1109/ISC2.2018.8656952.

[99] A. Richardson and J. Xu. Carbon Trading with Blockchain. In P. Pardalos, I. Kotsireas, Y. Guo, and W. Knottenbelt, editors, *Mathematical Research for Blockchain Economy*, Springer Proceedings in Business and Economics, pages 105–124. Springer, 2020. doi:10.1007/978-3-030-53356-4.

[100] R. Rivera, J. G. Robledo, V. M. Larios, and J. M. Avalos. How digital identity on blockchain can contribute in a smart city environment. In *2017 International Smart Cities Conference (ISC2)*, pages 1–4. IEEE, 2017. doi:10.1109/ISC2.2017.8090839.

[101] P. Rogaway and T. Shrimpton. Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance. In B. Roy and W. Meier, editors, *Fast Software Encryption*, pages 371–388, Berlin, Heidelberg, 2004. Springer Berlin Heidelberg.

[102] S. Roy, M. Ashaduzzaman, M. Hassan, and A. R. Chowdhury. BlockChain for IoT Security and Management: Current Prospects, Challenges and Future Directions. In *2018 5th International Conference on Networking, Systems and Security (NSysS)*, pages 1–9, Dhaka, Bangladesh, 2018. IEEE. doi:10.1109/NSysS.2018.8631365.

[103] N. Rožman, J. Diaci, and M. Corn. Scalable framework for blockchain-based shared manufacturing. *Robotics and Computer-Integrated Manufacturing*, 71: 102139, 2021. doi:10.1016/j.rcim.2021.102139.

[104] M. Sabounchi and J. Wei. Towards resilient networked microgrids: Blockchain-enabled peer-to-peer electricity trading mechanism. In *2017 IEEE Conference on Energy Internet and Energy System Integration (EI2)*, pages 1–5, Beijing, 2017. IEEE. doi:10.1109/EI2.2017.8245449.

[105] S. Saraji and M. Borowczak. A blockchain-based carbon credit ecosystem, 2021.

[106] R. Schollmeier. A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications. In *Proceedings First International Conference on Peer-to-Peer Computing*, pages 101–102. IEEE Comput. Soc, 2001. doi:10.1109/P2P.2001.990434.

[107] P. K. Sharma, M.-Y. Chen, and J. H. Park. A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT. *IEEE Access*, 6:115–124, 2018. doi:10.1109/ACCESS.2017.2757955.

[108] A. Sheikh, V. Kamuni, A. Urooj, S. Wagh, N. Singh, and D. Patel. Secured energy trading using byzantine-based blockchain consensus. *IEEE Access*, 8:8554–8571, 2020. doi:10.1109/ACCESS.2019.2963325.

[109] M. Shen, X. Tang, L. Zhu, X. Du, and M. Guizani. Privacy-Preserving Support Vector Machine Training Over Blockchain-Based Encrypted IoT Data in Smart Cities. *IEEE Internet of Things Journal*, 6(5):7702–7712, 2019. doi:10.1109/JIOT.2019.2901840.

[110] J. J. Sikorski, J. Haughton, and M. Kraft. Blockchain technology in the chemical industry: Machine-to-machine electricity market. *Applied Energy*, 195:234–246, 2017. doi:10.1016/j.apenergy.2017.03.039.

[111] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund. Industrial Internet of Things: Challenges, Opportunities, and Directions. *IEEE Transactions on Industrial Informatics*, 14(11):4724–4734, 2018. doi:10.1109/TII.2018.2852491.

[112] M. Sun and J. Zhang. Research on the application of block chain big data platform in the construction of new smart city for low carbon emission and green environment. *Computer Communications*, 149:332–342, 2020. doi:10.1016/j.comcom.2019.10.031.

[113] N. Szabo. Formalizing and securing relationships on public networks. *First Monday*, 2(9), 1997.

[114] N. Tapas, G. Merlino, and F. Longo. Blockchain-Based IoT-Cloud Authorization and Delegation. In *2018 IEEE International Conference on Smart Computing (SMARTCOMP)*, pages 411–416, Taormina, 2018. IEEE. doi:10.1109/SMARTCOMP.2018.00038.

[115] F. Teng, Q. Zhang, G. Wang, J. Liu, and H. Li. A comprehensive review of energy blockchain: Application scenarios and development trends. *International Journal of Energy Research*, 45(12):17515–17531, 2021. doi:10.1002/ER.7109.

[116] N. Teslya and I. Ryabchikov. Blockchain-based platform architecture for industrial IoT. In *2017 21st Conference of Open Innovations Association (FRUCT)*, pages 321–329, Helsinki, 2017. IEEE. doi:10.23919/FRUCT.2017.8250199.

[117] D. Tse, B. Zhang, Y. Yang, C. Cheng, and H. Mu. Blockchain application in food supply information security. In *2017 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, pages 1357–1361. IEEE, 2017. doi:10.1109/IEEM.2017.8290114.

[118] A. Vatankhah Barenji, Z. Li, and W. M. Wang. Blockchain cloud manufacturing: Shop floor and machine level. In *Smart SysTech 2018; European Conference on Smart Objects, Systems and Technologies*, pages 1–6, 2018.

[119] M. Vivekanandan, S. V. N., and S. R. U. BIDAPSCA5G: Blockchain based Internet of Things (IoT) device to device authentication protocol for smart city applications using 5G technology. *Peer-to-Peer Networking and Applications*, 14(1):403–419, 2021. doi:10.1007/s12083-020-00963-w.

[120] Vyper. Vyper documentation, 2021. URL `https://vyper.readthedocs.io/en/stable/`. Last accessed 01 October 2021.

[121] M. Wang, M. Duan, and J. Zhu. Research on the Security Criteria of Hash Functions in the Blockchain. In *Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts - BCC '18*, pages 47–55. ACM Press, 2018. doi:10.1145/3205230.3205238.

[122] S. Wang, A. F. Taha, and J. Wang. Blockchain-Assisted Crowdsourced Energy Systems. In *2018 IEEE Power and Energy Society General Meeting (PESGM)*, pages 1–5, Portland, OR, 2018. IEEE. doi:10.1109/PESGM.2018.8585864.

[123] S. Wang, D. Li, Y. Zhang, and J. Chen. Smart Contract-Based Product Traceability System in the Supply Chain Scenario. *IEEE Access*, 7:115122–115133, 2019. doi:10.1109/ACCESS.2019.2935873.

[124] X. Wang, W. Yang, S. Noor, C. Chen, M. Guo, and K. H. van Dam. Blockchain-based smart contract for energy demand management. *Energy Procedia*, 158:2719–2724, 2019. doi:10.1016/j.egypro.2019.02.028.

[125] World Bank Group. Blockchain and Emerging Digital Technologies for Enhancing Post-2020 Climate Markets. Technical report, World Bank Group, 2018.

[126] L. D. Xu, E. L. Xu, and L. Li. Industry 4.0: state of the art and future trends. *International Journal of Production Research*, 56(8):2941–2962, 2018. doi:10.1080/00207543.2018.1444806.

[127] R. Xu, Y. L. Chen, E. Blasch, and G. Chen. Blendcac: A blockchain-enabled decentralized capability-based access control for iots. *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pages 1027–1034, 2018.

[128] M. Yan and M. S. Grid. Blockchain for Transacting Energy and Carbon Allowance in Networked Microgrids. *ieeexplore.ieee.org*, 2021.

[129] T. Yang, Q. Guo, X. Tai, H. Sun, B. Zhang, W. Zhao, and C. Lin. Applying blockchain technology to decentralized operation in future energy internet. In *2017 IEEE Conference on Energy Internet and Energy System Integration (EI2)*, pages 1–5, Beijing, 2017. IEEE. doi:10.1109/EI2.2017.8244418.

[130] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, Q. Zhang, and K.-K. R. Choo. An Energy-Efficient SDN Controller Architecture for IoT Networks With Blockchain-Based Security. *IEEE Transactions on Services Computing*, 13(4):625–638, 2020. doi:10.1109/TSC.2020.2966970.

[131] ycharts ether. Ethereum statistics, 2021. URL `https://bitnodes.io/`. Last accessed 01 October 2021.

[132] S. Yi, C. Li, and Q. Li. A Survey of Fog Computing. In *Proceedings of the 2015 Workshop on Mobile Big Data*, pages 37–42, New York, NY, USA, 2015. ACM. doi:10.1145/2757384.2757397.

[133] H. Yu, Z. Yang, and R. O. Sinnott. Decentralized Big Data Auditing for Smart City Environments Leveraging Blockchain Technology. *IEEE Access*, 7:6288–6296, 2019. doi:10.1109/ACCESS.2018.2888940.

[134] N. Zahed Benisi, M. Aminian, and B. Javadi. Blockchain-based decentralized storage networks: A survey. *Journal of Network and Computer Applications*, 162: 102656, 2020. doi:10.1016/j.jnca.2020.102656.

[135] J. J. Zhang, F.-Y. Wang, X. Wang, G. Xiong, F. Zhu, Y. Lv, J. Hou, S. Han, Y. Yuan, Q. Lu, and Y. Lee. Cyber-Physical-Social Systems: The State of the Art and Perspectives. *IEEE Transactions on Computational Social Systems*, 5(3):829–840, 2018. doi:10.1109/TCSS.2018.2861224.

[136] Y. Zhang and J. Wen. The IoT electric business model: Using blockchain technology for the internet of things. *Peer-to-Peer Networking and Applications*, 10(4): 983–994, 2017. doi:10.1007/s12083-016-0456-1.

[137] X. Zhou, A. Eibeck, M. Q. Lim, N. B. Krdzavac, and M. Kraft. An agent composition framework for the J-Park Simulator - A knowledge graph for the process industry. *Computers & Chemical Engineering*, 130:106577, 2019. doi:10.1016/j.compchemeng.2019.106577.

[138] X. Zhou, M. Q. Lim, and M. Kraft. A Smart Contract-based agent marketplace for the J-Park Simulator - a knowledge graph for the process industry. *Computers & Chemical Engineering*, 139:106896, 2020. doi:10.1016/J.COMPCHEMENG.2020.106896.