Carbon Capture Science & Technology 13 (2024) 100300

Contents lists available at ScienceDirect

Carbon Capture Science & Technology

journal homepage: www.elsevier.com/locate/ccst

Full Length Article

Advancing the deployment and information management of direct air capture: A solution enabled by integrating consortium blockchain system

Zihan Chen[a], Yiyu Liu[a,b], Eryu Wang[a], Huajie You[c], Qi Gao[a], Fan David Yeung[a], Jia Li[d,*]

[a] Thrust of Innovation, Policy and Entrepreneurship, The Hong Kong University of Science and Technology, Guangzhou, China
[b] Innovation, Technology, Entrepreneurship & Marketing Group, Eindhoven University of Technology, Eindhoven, Netherlands
[c] Thrust of Data and Science Analytics, The Hong Kong University of Science and Technology, Guangzhou, China
[d] School of Interdisciplinary Studies, Lingnan University, Lingnan, Hong Kong

ARTICLE INFO

Key words:
Direct air capture (dac)
Blockchain technology
Carbon neutrality
Consensus Mechanism
Digital Signature

ABSTRACT

Direct air capture (DAC) is a critical and emerging Negative Emissions Technology (NET) that directly removes CO2 from the atmosphere, significantly contributing to climate change. However, the deployment and management of large-scale DAC faces challenges such as collections and analysis of energy consumption data, intricate device and system management, emission prediction and operation strategy, precise carbon footprint tracking, etc. This paper proposes the integration of blockchain technology with DAC systems to address these challenges, utilizing blockchain's inherent properties of immutability, security, and transparency. The implementation strategy includes the development of a DAC consortium blockchain system, leveraging a consensus mechanism,[1] ECDSA encryption,[2] IoT[3] integration, and digital signatures. Preliminary modeling of the proposed system suggests potential improvements in operational efficiency and a reduction in data inaccuracies. The proposed system underscores the system's ability to streamline identity verification, improve data collection accuracy, and facilitate secure, confidential information sharing among DAC stakeholders. By enhancing the efficiency and reliability of DAC operations, this approach supports the scalable and effective deployment of NETs in the global effort to combat climate change. Future research will focus on empirical validation through pilot projects and simulations to further substantiate these claims.

1. Introduction

The Intergovernmental Panel on Climate Change (IPCC) (Calvin et al., 2023) has emphasized that human activities have caused global surface temperatures to rise by 1.1°C above pre-industrial levels. To mitigate extreme impacts on resources, ecosystems, biodiversity, food security, and urban areas, it is critical to limit warming to below 1.5°C (Mukherji et al., 2023). Achieving this goal requires a significant reduction in global annual emissions to 25–30 Gt CO_2 by 2030, as suggested by the IPCC in 2018 (Bongaarts, 2019; Levin, 2018). In this context, Negative Emission Technologies (NETs) have become increasingly important for balancing emissions, as outlined in the Climate Change Mitigation Program under the Paris Agreement (International Energy Agency, 2022).

Direct Air Capture (DAC), one of the NETs is an engineering solution that removes CO_2 directly from the air. Although this process is technically challenging due to the low concentration of CO2 in the air (approximately 0.04 %), it offers a scalable and flexible solution for carbon removal, particularly when compared to conventional Carbon Capture and Storage (CCS) technologies (Erans et al., 2022; Wang et al., 2024). The IEA report(2022) highlights that Direct Air Carbon Capture and Storage (DACCS) will play a pivotal role in achieving a zero-emissions pathway by capturing CO_2 directly from the air and permanently sequestering it underground. Moreover, the captured CO2 can be utilized as a climate-

* Corresponding author.
E-mail address: jia.li@ln.edu.hk (J. Li).

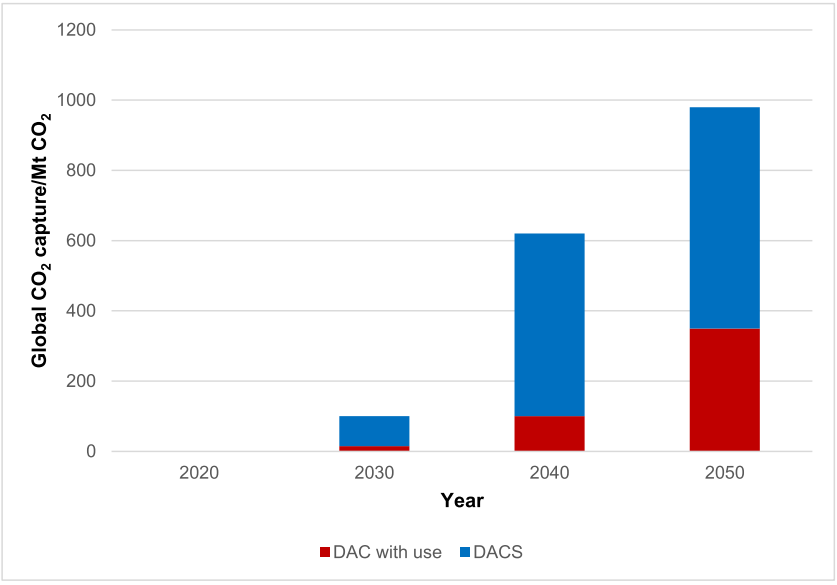
[1] Consensus mechanism: The programming and process used in blockchain systems to achieve distributed agreement about the ledger's state or the state of a data set. (Source: Investopedia)

[2] Elliptic Curve Digital Signature Algorithm (ECDSA): In cryptography, the Elliptic Curve Digital Signature Algorithm (ECDSA) offers a variant of the Digital Signature Algorithm (DSA) which uses elliptic-curve cryptography. As with elliptic-curve cryptography in general, the bit size of the private key believed to be needed for ECDSA is about twice the size of the security level, in bits. (Source: Wikipedia)

[3] Internet of things (IoT): describes devices with sensors, processing ability, software and other technologies that connect and exchange data with other devices and systems over the Internet or other communication networks. (Source: Wikipedia)

https://doi.org/10.1016/j.ccst.2024.100300
Received 30 June 2024; Received in revised form 30 August 2024; Accepted 12 September 2024

Table 1
Global CO_2 capture from DACS and DAC with use in the Net Zero Scenario.
(Source: IEA Report regarding to Direct Air Capture).



neutral carbon source for producing beverages, chemicals, and synthetic fuels, benefiting industries such as aviation.

Unlike conventional CCS technology,[4] DAC technology is mechanically scalable, deployable in diverse locations, and capable of operating on renewable energy sources. It has been applied in various sectors, including transportation (He et al., 2022), building construction and indoor air purification (Miao et al., 2022), and even space stations (Wang et al., 2023). Furthermore, DAC technology has fewer negative environmental impacts compared to other carbon-negative technologies like biomass carbon capture and storage (BECCS) and afforestation, as it does not compete for water and land required for food production. This makes DAC a complementary technology to existing decarbonization solutions (Miao et al., 2021).

The growing recognition of DAC's role in achieving net-zero goals has led to increased political support and investment. Since the beginning of 2020, nearly $4 billion in funding has been allocated for DAC research, development, and deployment (RD&D), and leading companies have raised approximately $125 million in capital (International Energy Agency, 2022). Plans for nine DAC facilities are currently underway, and if these projects proceed as expected, DAC deployment will reach approximately 3 million tons of CO2 by 2030. Wit still accounts for only 3.4 % of the deployment level required for a net-zero scenario (Calvin et al., 2023).

As shown in Table 1, scaling up DAC deployment in the IEA net-zero scenario requires adding more than 30 DAC plants with a capacity of 1 million tons per year, annually, from 2020 to 2050 (International Energy Agency, 2022). This ambitious deployment will hinge on ensuring cost competitiveness, operational efficiency, and the availability of low-carbon energy sources, along with essential consumables such as CO_2 adsorbents.

Despite its potential, DAC technology faces significant challenges related to energy consumption, equipment management, carbon footprint tracking, and the secure trading of captured CO2 rights. Recent research has highlighted the technology gaps between the current state of the art (Technology Readiness Level[5] [TRL] 7–9) and full-scale industrial applications (TRL 11) (Bisotti et al., 2024). Moreover, DAC deployment is not just a technical issue; it involves complex financial, political, and social considerations. Factors such as operational management, energy consumption assessment, and cost-effectiveness are crucial for facilitating DAC deployment (Bisotti et al., 2024).

This paper aims to address these challenges by proposing an innovative approach that integrates blockchain technology with DAC systems. By leveraging blockchain's properties of immutability, security, and transparency, this research offers a novel solution for improving the efficiency, accuracy, and scalability of DAC operations. Specifically, the paper contributes to the field by introducing a DAC consortium blockchain system that enhances identity verification, data collection, and secure information sharing among stakeholders. This approach not only supports the broader deployment of NETs but also represents a significant advancement in the application of blockchain technology in environmental engineering.

2. Five challenges of scaling up the DAC technology

Direct Air Capture (DAC) technology as a pivotal solution is gaining traction in the international society, the slow pace of its implementation restricts the extent to which it can contribute to the efforts aimed at mitigating climate change (Qiu, 2022). According to the 2020 report from the Global CCS Institute, the volume of large-scale carbon capture is projected to reach only 40 million $MtCO_2$ annually, with nearly the entire amount occurring in developed nations and predominantly involving gas processing and applications in enhanced oil recovery. Researchers emphasize the environmental impacts of a large-scale DAC deployment have not yet been accurately quantified, and more precise statistics are needed. The slow adoption of DAC is attributed to a variety of technical, environmental, economic, social and political hurdles.

From the technological perspectives, previous studies have detailed a series of barriers to scale DACCS technology, including material selection, development of key equipment, system integration, facility op-

[4] Carbon capture and storage (CCS) is a process in which a relatively pure stream of carbon dioxide (CO_2) from industrial sources is separated, treated and transported to a long-term storage location (Masson-Delmotte et al., 2021).

[5] Technology readiness levels (TRLs) are a method for estimating the maturity of technologies during the acquisition phase of a program. TRLs enable consistent and uniform discussions of technical maturity across different types of technology.

eration and management, data integration and accounting, and infrastructure development (Küng et al., 2023). For example, academic breakthroughs have been enhancing the functionality of the capturing materials. For example, Wu et al. (2024) demonstrated strong environmental adaptability through the development of structured adsorbents, enhancing CO_2 capture efficiency while maintaining excellent hydrothermal stability. However, the effectiveness of DAC is contingent upon the systems' capacity to operate at high efficiency levels. Little has been explored regarding its long-term operation stability. The trace pollutant in the air, when processed in such large volumes, could exert a detrimental influence on DAC systems. Moreover, these systems must be capable of enduring environmental condition, which can range from water, wind, cold to sandstorms, based on their specific locations (Bui et al., 2018).

The implementation of DAC has environmental trade-off that need to be considered. One of the main environmental trade-offs of DAC is the energy resources for running the capture processes, which can lead to increased energy consumption and associated emissions if not sourced sustainably. For example, a modeling study for the integration of DACCS plants into a greenhouse gas-neutral European energy system showed applying fully electric DAC systems and current technological projections, removing 288 MtCO2/a increases electricity demand in Europe 385–495 TWh_{el} in 2050 . Moreover, the siting of DAC plants is important for minimizing regional environmental impacts and integrating them into energy system planning. In addition, application of DAC can result in considerable spatial variations in surface temperature anomalies and other climatic changes, such as cooler tropopause or disrupted tropical regions (Erans et al., 2022). A life cycle assessment of DAC technologies shows that decarbonizing the electricity sector improves sequestration efficiency but also increases terrestrial ecotoxicity and metal depletion levels per tonne of CO_2 sequestered (Qiu et al., 2022). The siting of DAC plants is important for minimizing regional environmental impacts and integrating them into energy system planning. Different sorbents used in DAC processes have varying environmental performances, with chemisorbents showing lower impacts on the environment compared to physisorbents (Leonzio et.al., 2022). The capture process can ensure negative CO_2 emissions and even the net removal of CO_2 from the atmosphere, but there is a need for further research to improve the physical properties of sorbents and reduce energy consumption. The climate benefits of DAC depend on the energy source, with low-carbon energy and careful plant construction being important factors (Deutz et.al., 2021). Furthermore, the application of DAC can result in considerable spatial variations in surface temperature anomalies and other climatic changes, such as cooler tropopause or disrupted tropical regions (Bodai et.al., 2018).

Cost is a key factor in the large-scale deployment of DAC technologies. Different developers of sorbent- and solvent-based DAC technologies have provided estimates for the cost of removing CO2 from the atmosphere, ranging from approximately $95 to $600 per ton. However, due to differing study assumptions and limited detail in the disclosures, it is challenging to assess and directly compare the reported costs (Valentine et al., 2022). For instance, the case study of Carbon Engineering's system suggested the capital cost at the 2018 45Q required scale has a capital cost of around $244 USD/$tCO_2$. In addition, Lux et al. (2023) predicted through modeling that the cost of DACCS in Europe in 2050 could be in the range of 60–140 EUR/tCO_2, which provides a positive outlook on the economics of DAC technology.

Societal acceptance for DAC is crucial for achieving successful deployment. Cox et al. (2020) found, through national surveys and deliberative workshops in the US and the UK, that the public perceives CDR technologies as being too slow to solve the current climate crisis and not addressing the root causes of climate change. This suggests that dilemmas regarding the short- and long-term impacts of technology and policy development need to be addressed to gain social license. Scott-Buechler, C. et al. (2024) used nationally representative surveys to assess public perceptions and conducted focus groups to evaluate community perceptions in four U.S. communities: Houston, Texas; Monaca, Pennsylvania; Bakersfield, California; and Rock Springs, Wyoming. Their team found that focus group participants were conditionally supportive of DAC deployment, while the majority of national survey respondents expressed general support for DAC deployment. After analyzing CDR deployment in the AR6 database, Motlaghzadeh, K. et al. (2023) delve into 54 DACCS scenarios, discussing the key factors that account for significant changes in the model projections. Motlaghzadeh, K.'s team suggests that future models should include variations of DAC technologies, as well as different carbon use and storage pathways. They also emphasize the need for optimizing overall DAC deployment and operational processes, as these factors can influence system demand, economic efficiency, and public acceptance.

Political challenges posit in the deployment of DAC including government subsidies, private sector investment on demonstration projects and the integration with other viable mitigation strategies. On one side, Kerner (2023) demonstrated through a survey that climate experts in relevant fields show strong support for BECCS and DAC. They argue that policy support and market incentives are critical to driving the development and deployment of DAC technology. Bisotti, F. et al. (2023) explore the importance of national-level context and dynamics in deploying DAC technologies within a specific country. Through a case study of Norway, the authors suggest that national energy strategies, resource availability, and potential natural constraints and barriers must be considered when planning DAC deployment. Bisotti, F. et al. hope that this study highlights the importance of considering the national context, particularly potential energy availability and the impact of DAC installation and operation. On the other side, governments have not provided the necessary support for its widespread implementation, and the preference for unabated fossil fuel use remains a significant barrier to its advancement. Despite the anticipation of smooth political support, there have been indications that the political landscape is more complex than initially assumed. The transition from expert consensus to concrete action has encountered significant political and economic barriers. Although DAC remains relatively obscure to the general public and many stakeholders, there have been instances where it has gained political prominence, particularly in developed economies.

As a technology still in its nascent stages, the global rollout of DAC initiatives necessitates meticulous preparation. Presently, the scaling of DAC plants designed for industrial contexts and modular DAC devices adaptable to urban and industrial settings alike has encountered numerous hurdles. Researchers have implemented a roadmap with prioritized initiatives aimed at accelerating the deployment of secure, scalable, and low-cost DACCS technologies, focusing on the collaboration with multiple key players in the field. Challenges persist, as mentioned above, including the technological barriers, economic viability, environmental impacts, societal perceptions, and political supports. Addressing these challenges requires collaborative efforts across academia, industry, investors, governments, policymakers and the general public to ensure comprehensive and effective deployment strategies. Therefore, the large-scale deployment of DAC is driven by the need to strengthen the information delivery pipeline (Meckling and Biber, 2021).

Blockchain technology is a state-of-the-art strategy to deal with the multifaceted nature of DAC deployment. The emergence of DAC technology, along with strategies such as the Regional Direct Air Capture (DAC) Hubs program, demands an organized and uniform management strategies to address the challenges. The following sections further emphasize the use of Blockchain for DAC within a designed framework.

3. Current DAC deployment in a blockchain-enabled information system

To achieve a larger scale deployment, enhancing systematic efficiency, reducing deployment costs, and increasing societal acceptance are key aspects to be considered. Previous studies emphasize the multidimensional impacts of DAC, its synergies with other NETs, and how it

Table 2
Key concepts that underpin blockchain.

Key Concepts	Description
Decentralization	Decentralization refers to the distribution of data storage and processing across a network of computers, rather than relying on a central authority. This eliminates single points of failure and can enhance the resilience of the system.
Immutability	Immutability is ensured by the blockchain's design, where once data is recorded, it cannot be altered retroactively. This is achieved through cryptographic techniques that link blocks in a sequential chain.
Security	Security is a fundamental feature of blockchain, provided by cryptographic algorithms that protect the integrity and confidentiality of the data. Each block contains a unique code (hash) that is generated based on the content of the block and the hash of the previous block.
Transparency	Transparency is facilitated by the open ledger system, where all participants in the network can view transaction records, although identities can be pseudonymous or anonymous.

can contribute to global climate goals. Scott-Buechler et al. (2024) believes that the principles of environmental justice and its transformation should be central in the planning and implementation of DAC projects. They underscore the importance of a committee in the planning and implementation process of a DAC program, as the expected community benefits (e.g., infrastructure improvements and labor market opportunities for the local area) are important determinants of support for DAC deployment (Scott-Buechler et al., 2024). Bisotti et al. (2024) identified efficiency issues as the primary obstacle limiting the large-scale deployment of DAC. Wang et al. (2020) believe that the key to promoting the large-scale deployment of DAC lies in improving the efficiency of DAC projects and reducing the operating costs of CO_2 capture through continuously technological innovations and organizational efforts. These innovations include, but are not limited to, improvements in the design of an integrated DACCS systems, monitoring of energy consumption and carbon footprints to reduce energy use, and optimization of adsorbent performance.

In Section 2, we delved into the current challenges of DAC deployment, spanning from managing energy consumption and overseeing equipment information to tracking carbon footprint data, collecting operational metrics from plant operations, and facilitating the trading of captured CO_2 rights. Blockchain technology, renowned for its distinctive attributes such as immutability, security, cross-industry applicability, traceability, and transparency, has emerged as a pivotal enabler across various sectors and disciplines (Drescher, 2017; Vigna and Casey, 2016). The integration of the blockchain technology is a potential solution to address operational complexities in a DACCS global value chain, enhance data transparency, and scale up the synergies with other NETs. In this section, we examine the current studies linking blockchain with other NETs, the technological viability of such an informational system, and the commercial use across sectors and scenarios.

3.1. Overview of blockchain

Blockchain technology is a transformative innovation that has gained significant attention due to its potential to disrupt various industries. At its core, a blockchain is a distributed database or shared ledger technology that allows multiple parties to maintain a continuous, tamper-evident record of transactions or data exchanges, where each block serves as a storage unit for data (Nakamoto, 2008). The key concepts that underpin blockchain technology, as shown in Table 2, include decentralization, immutability, security, and transparency (Nakamoto, 2008; Wood, 2014).

In a blockchain system, blocks record all transactional information from each node over a specific period, thereby significantly enhancing the trustworthiness, security, and integrity of the data (Nakamoto, 2008). Blockchain comprises several key component technologies that work together to maintain its functionality and security, including hashing, encryption, consensus mechanism and so on. Blockchain consists of a vast number of interconnected blocks, forming a continuous data chain through which information is transmitted. Each block comprises two essential components: the block header and the block body, each serving distinct roles within the blockchain (Nakamoto, 2008; Wood, 2014). The blockchain model relies heavily on cryptographic techniques to ensure secure data ownership confirmation while safeguarding data privacy (Zhai et al., 2019). Electronic data, being a digital asset or means of production, lacks the straightforward proof of ownership that physical assets enjoy. Consequently, transactions involving substantial data quantities, such as carbon rights, are susceptible to issues like duplication and disputes (Hua et al., 2020). Additionally, the data in a blockchain system is collectively maintained by its nodes, ensuring that the information remains public and transparent (Nakamoto, 2008).

In blockchain technology, the hash function plays a crucial role in transferring information from one block to another, facilitating secure and efficient communication across the blockchain. Also referred to as a cryptographic hash function, it transforms data or messages of varying lengths and formats into fixed-length strings (Cachin, 2016; Nakamoto, 2008). For instance, if D represents a data message with unknown characteristics in terms of length and memory size, and f denotes the resultant hash value of a predetermined length, the hash function can be mathematically expressed as follows:

$$f = F(D)$$

Blockchain systems leverage various types of cryptographic hash functions tailored to specific application scenarios to ensure the integrity of uploaded information and data. The inherent collision resistance of these hash functions makes blockchain systems inherently tamper-proof. For instance, in Bitcoin, one of the pioneering blockchain applications, addresses are derived through dual rounds of hashing followed by specific encoding. Hash functions come in different types based on diverse designs and encodings, each suited to particular requirements and scenarios. Among these, the SHA-256 function stands out, designed to transform data of varying lengths, memory sizes, and formats into a consistent 256-bit random output string known as a digest or hash value. This function boasts several advantages, including rapid computation speed, deterministic output, and inherent randomness in its outputs. Determinism ensures that running the same data through the SHA-256 function repeatedly yields identical results, regardless of the number of computations. For instance, as shown in Fig. 1, when integrated into Python for application development, running the SHA-256 function with the input "HKUST" consistently produces identical outputs, as demonstrated in the figure. This deterministic property underscores the reliability and predictability essential for blockchain applications.

The randomness of the hash function ensures that even minor changes in the input content result in vastly different hash values. This characteristic means the output values are entirely random, leading to significant variations, making it highly improbable for similar inputs to produce similar outputs. Although this property might seem to contradict the previous one, it highlights one of the most crucial advantages of hash functions. For example, when the SHA-256 function is initially run in Python application development software with the input "HKUST," the output is consistent with previous results. However, changing the uppercase "S" to a lowercase "s" to form "HKUsT" and running the function again produces a completely different hash value. Similarly, altering the uppercase "H" to a lowercase "h" to form "hKUST" and running the function a third time also yields a distinct output. Finally, replacing the uppercase "HKUST" with all lowercase "hkust" in the fourth run re-

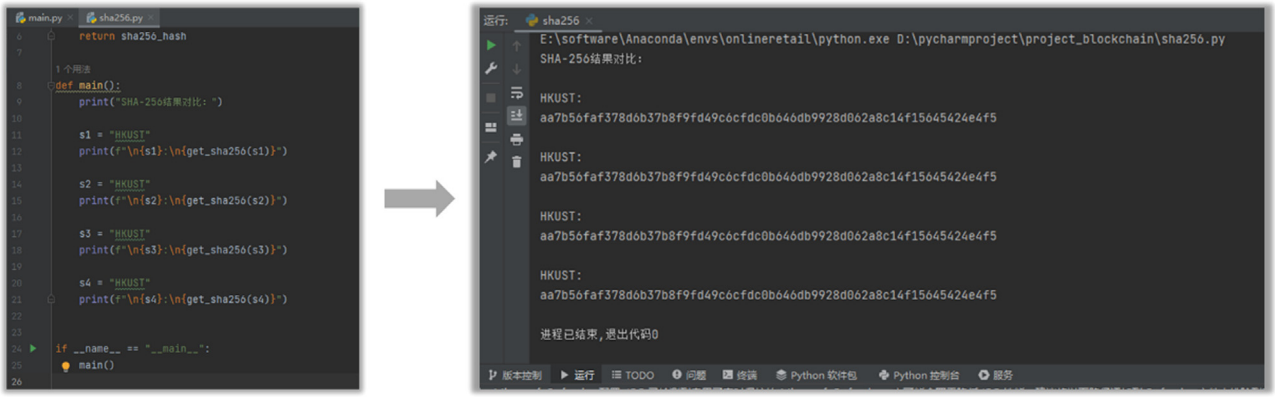


Fig. 1. Verifying the "Output Determinism" of Hash Function (Software: Python).

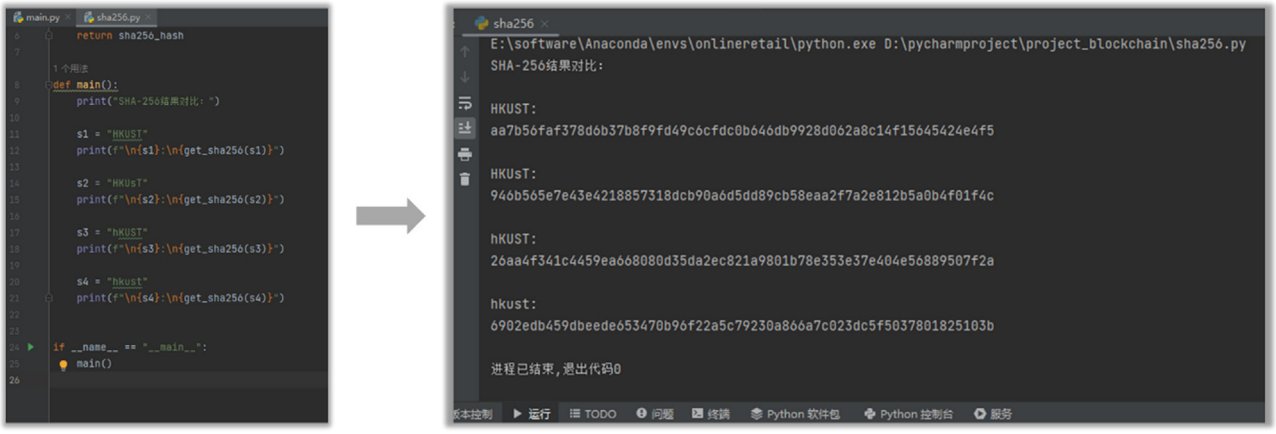


Fig. 2. Verifying the "Output Randomness" of Hash Function (Software: Python).

sults in yet another unique hash value. As shown in the Fig. 2, despite the minor changes in the letters, the four hash function operations produce entirely different outputs. Each input variant—"HKUST," "HKUsT," "hKUST," and "hkust"—generates a unique hash value, demonstrating the hash function's sensitivity to input changes and its robustness in ensuring data integrity.

A well-executed hash function must fulfill the property known as collision resistance. This means that for any given input data, the hash value produced by the function is not easily predicted by a malicious attacker as being the same as the hash value for another piece of input data. In other words, the more collision-resistant a hash function is, the less correlation there is between its output hash value and the original data, making it more difficult for attackers to crack or manipulate (Cachin, 2016). Although the likelihood of a hash collision is low, it is crucial to choose an appropriate hash function to minimize the possibility of such conflicts when building the underlying system of a blockchain. Additionally, some blockchain systems, such as Bitcoin, require a certain level of encoding after the hash operation is performed. The encoding system used by Bitcoin is detailed in the Appendix (Cachin, 2016).

3.2. Current blockchain applications in various fields combined with negative emissions technologies (NETs)

Blockchain technology has been adopted by numerous research institutes and companies across various fields, integrating and enhancing different industries and sectors (Zhai et al., 2019). As a decentralized data storage solution, blockchain's immutability ensures data integrity and security, with all transactions and records being traceable, thus boosting transparency and accountability in research (Tönnissen and Teuteberg, 2020). In Industry 4.0, blockchain is utilized for equipment authentication and transparent documentation of production processes (Huo et al., 2022). Additionally, blockchain facilitates interdisciplinary collaboration and knowledge sharing among researchers from different disciplines (Yeung, 2021). In supply chain management, blockchain technology provides transparent and tamper-proof records, helping companies track the entire process from production to delivery, thereby increasing efficiency, reducing fraud, and enhancing consumer trust (Lu, 2019).

The advantages of blockchain in sustainable supply chain and data management are proven to be multifaceted. Upadhyay, A., et al. (2021) review the contributions of blockchain to sustainability by lowering transaction costs, improving supply chain performance, and enhancing information transfer. He et al. (2023), analyzed the role of digital intelligence technologies such as the Internet of Things (IoT), big data, and artificial intelligence in reducing carbon emissions. They emphasized the significant role blockchain technology can play in improving the effectiveness, efficiency, and accuracy of carbon footprint measurements. Additionally, blockchain can be used to record environmental data such as carbon footprints and energy consumption, supporting sustainable development and environmental governance (Parmentola, A. et al., 2022). It can also support green bonds and other environmental financial instruments, ensuring that funds are utilized for sustainable projects (Kim and Huh, 2020).

When combined with NETs, previous studies mostly focus on blockchain application on the carbon trading mechanism, bridging the communication between Internet of Things (IoT) devices and the integrity of data exchange in carbon credit trading (Sadawi et al., 2021, Pan et al., 2019, Hua et al., 2020). In construction project management system, blockchain enhances efficiency and transparency, optimizing processes, reducing resource waste, decreasing carbon emissions, and minimizing environmental damage (Chen, 2023; Mahmudnia et al., 2022; Yang et al., 2020). Hunhevicz's research team (2022) developed a holistic framework for systematically applying blockchain technology in the construction industry, which includes determining its necessity and designing a decision-making framework for its use. To optimize the energy efficiency, blockchain is employed for energy transactions and smart grid management, further scaling up the distribution of renewable energy use (Van Cutsem et al., 2020). To prove an asset ownership, blockchain streamlines transactions by providing a transparent record of land registration and property ownership (Saari et al., 2022).

While private chain and consortium chain are the main solutions in the previous studies, the adoption of public network such as Ethereum is relatively limited. Xu et al. (2024) have integrated Ethereum into their carbon management platform for building certification, which offers the advantage of public disclosure of carbon data while ensuring platform security through Ethereum's gas fees. The integration also paves the way for potential access to the green investment market, leveraging the transparency and security provided by blockchain technology (Xu et al., 2024).

DAC systems can be integrated with other NETs to achieve negative emissions, offering a more secure and efficient solution for permanent carbon storage. To advance the construction and manufacturing process of DAC system, McQueen and Drennan (2024) propose the warehouse automation method. Baus et al. (2022) design a system to balance energy conservation in building operations integrating heating, ventilation, and air handling systems with DAC. This combination aims to optimize both energy efficiency and indoor air quality (Sodiq et al., 2023). Climeworks and CrabFix have joined forces to create the first permanent DACCS system, utilizing heat derived from a geothermal power plant. Integrating DAC with CO_2 mineralization technology offers the advantage of achieving negative emissions without being limited by geographical constraints, leading to a reduction in the costs associated with CO_2 transportation (Gutknecht et al., 2018). Snytnikov and Potemkin (2022) proposed a solution combining low-temperature steam reforming hydrocarbon technology with blockchain technology to monetize currently flared associated LPG. This approach, combined with CO2 capture and regeneration technologies, can enhance oil recovery and reduce atmospheric CO2 emissions. However, no previous studies have mentioned blockchain integration into the DAC system. Therefore, this state-of-the-art study sets the cornerstone in the field.

Blockchain can provide tamper-proof records through its distributed ledger systems, to enhance efficiency and accountability in various industrial processes, from asset ownership authentication, manufacturing and construction, to supply chain management and the integration with other NETs. Furthermore, when combining with other digital technologies such as IoT and AI, blockchain secures the device communication, optimizes system efficiency, and enhances the data integrity and traceability. This comprehensive integration supports sustainable development, environmental governance, and the effective management of carbon capture initiatives.

3.3. The optimal decision-making strategy of blockchain type for DAC deployment and management

Based on the methods of data transfer, the degree of sharing, and user rights, blockchain can typically be categorized into four types: public blockchain, private blockchain, hybrid blockchain, and consortium blockchain.

Public blockchain is a decentralized peer-to-peer framework (Pilkington, 2016). Anyone can access, write, and participate in the network's broadcasting and information sharing. In a public chain, information is completely open and transparent. Every node, driven by its own computational power, has equal rights and interests in the public protocol process and information transmission within the consensus mechanism. However, due to the large number of participating nodes, particularly when using proof of work (PoW)[6] as the consensus mechanism, the process of transactions may be slow and easy to cause attacks (Pilkington, 2016). The Proof of Work (PoW) consensus, in particular, where Bitcoin is utilized, performs calculations according to a prescribed algorithm during the process of "mining", consuming a large amount of energy. Each miner is rewarded by the amount of workloads they have achieved, which are verified by other nodes (Nakamoto, 2008). The process of mining or PoW further reinforces security by requiring substantial computational effort to solve complex cryptographic puzzles. This not only deters tampering but also ensures that new blocks meet the network's consensus criteria before being appended to the chain. The "trustless" issue does not imply a lack of trust among participants but rather a shift from reliance on traditional intermediaries or third-party entities to trust in the system itself. In a public blockchain, trust is established through cryptographic proof and consensus mechanisms that validate transactions and record them immutably. The "Trustlessness" issue offers several advantages, particularly in environments where traditional trust structures are either absent or deemed unreliable. It eliminates the single point of failure and the potential for centralized control, which can be susceptible to corruption or fraud. Instead, trust is distributed across the network, reducing the risk of any single entity manipulating the system. Recent developments in blockchain technology have introduced more energy-efficient and faster consensus mechanisms. Proof of Stake (PoS)[7] is a consensus mechanism that significantly reduces energy consumption compared to PoW. Instead of relying on energy-intensive computations to validate transactions and create new blocks, PoS allows validators to create new blocks and validate transactions based on the number of coins they hold and are willing to "stake" as collateral (Pilkington, 2016). This approach not only conserves energy but also speeds up the consensus process. In addition to PoS, other consensus mechanisms like Proof of Authority (PoA)[8] provide alternative approaches that prioritize efficiency and control, especially in scenarios where the network participants are known and trusted (Pilkington, 2016). Together, these ongoing advancements in consensus mechanisms demonstrate a concerted effort to balance the need for security and decentralization with the pressing demands for energy efficiency and operational speed.

Private Blockchain, also known as a Permissioned Blockchain, restricts membership and access to the participating network (Helliar et al., 2020). Node participation in a Private Blockchain is highly limited, allowing only specific entities to join. This type of blockchain is primarily utilized for internal information management and data preservation within companies or simple organizational structures. The transaction or information and data transfer sharing

[6] Proof of work (PoW) is a decentralized consensus mechanism that requires network members to expend effort in solving an encryption puzzle. Proof of work is also called mining, in reference to receiving a reward for work done. (Source: Investoprdia)

[7] Proof-of-stake (PoS) protocols are a class of consensus mechanisms for blockchains that work by selecting validators in proportion to their quantity of holdings in the associated cryptocurrency. This is done to avoid the computational cost of proof-of-work (POW) schemes. The first functioning use of PoS for cryptocurrency was Peercoin in 2012, although the scheme, on the surface, still resembled a POW. (Source: Wikipedia)

[8] Proof of authority (PoA) is an algorithm used with blockchains that delivers comparatively fast transactions through a consensus mechanism based on identity as a stake. The most notable platforms using PoA are VeChain, Bitgert, Palm Network and Xodex. (Source: Wikipedia)

Table 3
Critical factors in choosing blockchain type and specific descriptions.

Key Factors	Specific Description
Database for Carbon Footprint Tracking and DAC Energy Consumption	It needs to be clarified whether a database is required for a DAC project to meet the needs for tracking changes in the amount of energy consumed and the carbon footprint of the direct air carbon capture process.
Shared Editorial Access	It is important to identify whether project participants and stakeholders need to have shared editorial access to data (right of writers) and which participants can have right of writers.
Trust Issue	It needs to be clear whether the identity of the writers needs to be provided and whether the writers can be trusted to grant the relevant access, editing and modification rights.
Relevance of Interests	It needs to be made clear whether the interests of the system's WRITERS are aligned with each other.
The Necessity of Trusted 3rd Party	It needs to be clarified whether a 3rd party entity or platform that helps both A and B manage data processing and handle access control operations is needed. This entity or platform acts as an infomediary or centralized conduit of data and information, i.e., it acts as an "infrastructure platform" between A and B to help establish or mediate trust between A and B and potentially validate the trustworthiness (i.e., reputation) of other participants.
Functionality	It needs to be made clear whether writers need to be fully or partially in control of the function.
Openness or Privatization of Transactions	There is a need to clarify whether public or private is required for data and relative trading in direct air capture programs.
Collective Maintenance	It needs to be clarified whether the participants in the project need to have the obligation and responsibility to jointly maintain the blockchain system.
Consensus Mechanism	It needs to be made clear whether the participants involved need to jointly acknowledge the authenticity of the data and the relevant details, and whether the participants are working within the same organization or across organizations.

mechanisms are entirely controlled by a single organization, with the degree of data openness and sharing being adjustable to manage information transfer or transactions. Consequently, information transfer or transactions on a private blockchain are faster, more efficient, and more secure than the public chain. However, this also means that private blockchain is a centralized structure since participants are divided into different access rights by the platform administration.

Hybrid Blockchain differs from both Public and Private Blockchains, incorporating features of both to form a partially decentralized structure (Zhu et al., 2020). Unlike a Public Blockchain, which displays every transaction and information transfer process, a Hybrid Blockchain allows entities to choose which transactions remain private, offering a middle ground by enabling organizations to maintain private, closed networks while still benefiting from the transparency and security of a Public Blockchain when necessary. This means that Hybrid Blockchains provide optional transparency, allowing certain parts to be open to everyone while restricting access to others (Zhu et al., 2020). By integrating features of Private Blockchains, Hybrid Blockchains can process transactions faster than typical Public Blockchains (Helliar et al., 2020).

Consortium Blockchain is a blend of private and public blockchain systems, involving member entities from multiple organizations in the consensus process rather than a single organization (Li et al., 2017). Unlike private blockchains controlled by a single entity or public blockchains open to all, Consortium Blockchains are governed by authorized members within an organization. These members, usually invited or vetted by the consortium, participate in the decision-making consensus process (Dib et al., 2018). Similar to Hybrid Blockchains, Consortium Blockchains allow the choice of which data, transactions, and information transfer processes remain private or public. However, control resides with consortium members who manage the consensus process (Li et al., 2017). Key features of Consortium Blockchains include limited access and multiple control centers, ensuring that only authorized members can join the network and participate in transactions. Unlike private blockchains with a single control point, Consortium Blockchains may be jointly controlled by multiple organizations, each managing a portion of the network (Li et al., 2017). Trusted organizations, selected as nodes with decision-making authority, conduct "mining" or information transmission activities, which are then verified and jointly recognized by other nodes. Some specific consortium nodes provide partial interface access for queries (Dib et al., 2018).

The deployment of DAC plants and modular devices is crucial and must be scientifically and rigorously planned (International Energy Agency, 2022). Future DAC projects, both industrial plants and urban devices, encompass extensive data to perform site management tasks. Key considerations include energy consumption and carbon footprint monitoring, system maintenance, stakeholder engagement, and the collaboration with storage sites or the utilization firms. DAC project participants—including DAC equipment providers, material suppliers, upstream capturers, and downstream storage sites or factories—have different levels of permissions to access information within the ecosystem (Dib et al., 2018; Du et al., 2021; Meng et al., 2021; Zhu et al., 2020). Key factors for DAC project managers to choose a blockchain can be summarized in Table 3. To begin with, whether the project needs to establish a database, and whether participants require shared editorial access to the data needs to be determined. Furthermore, the trust issue concerns whether the identities of the writers need to be disclosed and whether these writers can be trusted with the rights of access, editing, and modification (Dib et al., 2018; Du et al., 2021; Meng et al., 2021; Zhu et al., 2020). The relevance of interests pertains to whether the interests of the system's writers are aligned. A trusted third party entity operating on the client's behalf acts as an information broker or a centralized conduit, mediates trust and verifies the trustworthiness (i.e., reputation) of other participants. Regarding functionality, each node can fully or partially responsible for controlling functions. Next, the financial transactions related to the project should be determined whether to be open or privatized. Finally, obligations of participants to involve in the system maintenance are diverse. The consensus mechanism involves validating data within the blockchain system. Data authenticity, regardless of the holders, shall gain open access among the system. A decision tree approach to determine an optimal type of blockchain is adopted, as shown in Fig. 3.

Throughout the lifecycle of DAC projects, from planning, sourcing, operation, to decommission, numerous data such as materials use, energy consumption, land use, water use, costs, and storage monitoring data must be meticulously recorded, stored, and exchanged within and across projects and regions (Deutz and Bardow, 2021; Madhu et al., 2021). Establishing a comprehensive database accessible to all stakeholders involved in DAC projects is essential. Each participant requires varying levels of access rights for data sharing and editing within the blockchain system. Hence, a decentralized blockchain model with distributed data storage is selected.

The decentralized architecture relies on commissioned external platforms authorized by multiple stakeholders for the validation purposes. Project participants who possess editing rights also require corresponding control functionalities to ensure the system operates smoothly. Transactions within DAC projects are restricted to participants who possess both editing rights and control functionalities, excluding external development. Participants in the project collaborate across firms rather than within a single organization, sharing the responsibility to collectively maintain the blockchain system with the introduction of a consensus mechanism. Integrating these considerations into the decision-

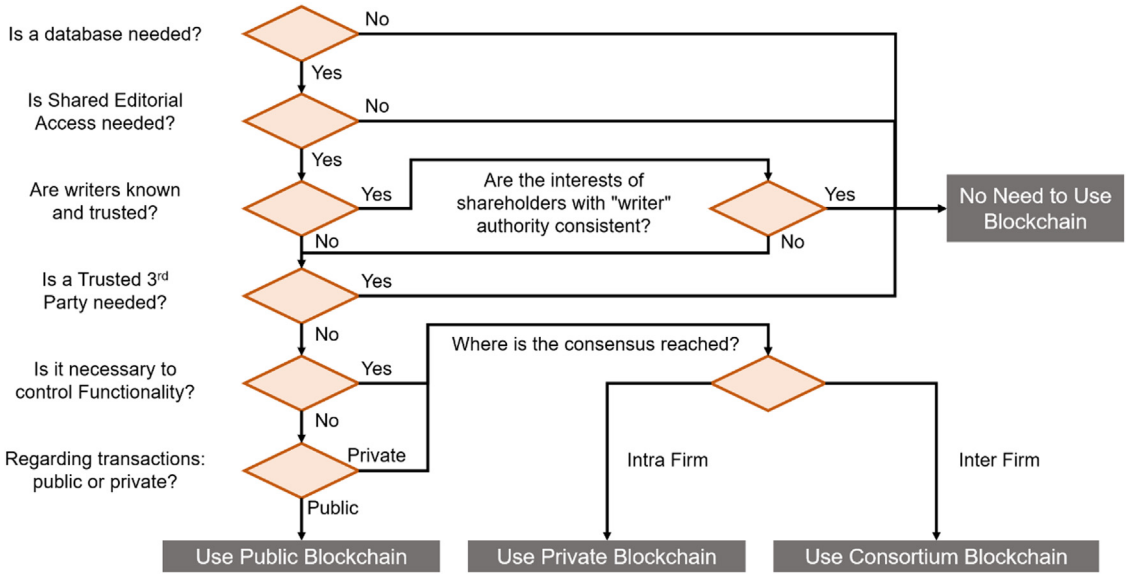


Fig. 3. The Decision-Making Strategy Adopted for blockchain type. The strategy provides a visual representation of the decision-making process for selecting the most suitable type of blockchain for Direct Air Capture (DAC) deployment and management. The decision-making process is guided by several key factors that are critical for DAC project managers when choosing a blockchain type including Database for Carbon Footprint Tracking and DAC Energy Consumption, Shared Editorial Access, Trust Issue, Relevance of Interests, The Necessity of Trusted 3rd Party, Functionality, Openness or Privatization of Transactions, Collective Maintenance, Consensus Mechanism;.

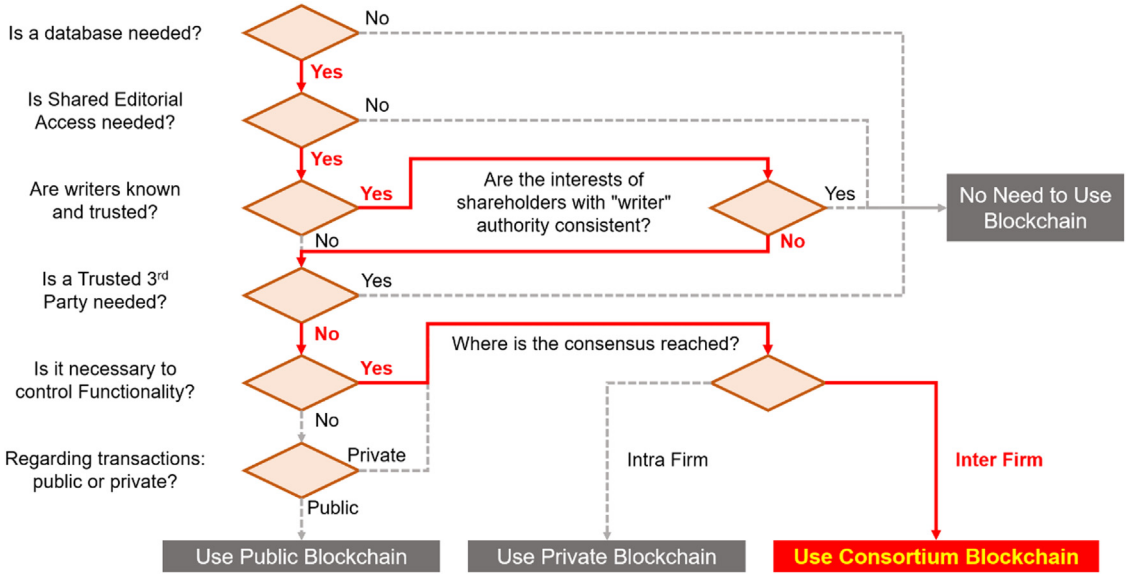


Fig. 4. The Blockchain Type Decision-Making Process for DAC Deployment. The figure presents a visual representation of the decision-making strategy for selecting the most appropriate type of blockchain technology to support the deployment and management of Direct Air Capture (DAC) projects. This decision-making process is crucial because it helps determine how data related to DAC projects, such as energy consumption and carbon footprint tracking, will be stored, shared, and managed among various stakeholders. Considering the need for a balance between data security, accessibility, and the involvement of multiple stakeholders in DAC projects, the consortium blockchain emerges as the optimal solution. Consortium blockchain allows for limited access, controlled by multiple organizations, and provides a consensus mechanism that ensures data authenticity while accommodating the collaborative nature of DAC projects.

making framework of Turk and Žiga's team reveals that a consortium blockchain emerges as the most suitable model for establishing the deployment and management of data information within DAC projects, as depicted in Fig. 4.

In the context of DAC deployment and management, leveraging a consortium blockchain can provide a secure, transparent, and tamper-evident system among blockchain members for tracking and verifying carbon capture data. This approach aligns with the need for reliability and traceability in environmental projects, ensuring that DAC initiatives contribute effectively to climate change mitigation efforts.

3.4. The DAC project information management strategy coupled with digital signature technology

According to the net-zero scenario proposed by the IEA and IPCC, global demand for DAC will grow exponentially in the future, leading to more DAC projects being situated in industrial and urban ar-

eas. During the construction and operation of these projects, it will be essential to document, store, and transfer a variety of data and documents, including construction management records, system efficiency metrics, energy consumption data, carbon footprints of the capture process, CO_2 capture costs, and the pathways for CO_2 storage or utilization. With the large-scale deployment of DAC, there will be stringent requirements for accurately recording and transferring extensive data and information related to carbon footprint tracking and energy consumption. Ensuring the authenticity and traceability of this data will necessitate robust information management and clear identification of project leaders. The foundational technology of blockchain, namely digital signature technology, is poised to effectively address the anticipated "DAC project data explosion" in the future (Bralić et al., 2020; Lai et al., 2010; Nist, 1992; Simmons, 1979; Wang et al., 2022). The digital signature process involves two critical algorithmic functions: the Sign function and the Verify function. The Sign function is utilized to sign data files encompassing various aspects of direct air capture projects, while the Verify function is employed to confirm the authenticity of signatures appended to these data files by engineers or other relevant stakeholders (Fang et al., 2020; Wang et al., 2022; Zhang et al., 2019).

The technique pivotal for encryption and authentication functions between the Sign and Verify operations is asymmetric cryptography (Simmons, 1979; Wang et al., 2022). In traditional symmetric encryption method, a single key is utilized for both encryption and decryption of data. This key must be securely shared between the sender and the recipient before any encrypted communication can take place. Unlike symmetric encryption, which relies on a shared key for simultaneous encryption and decryption, asymmetric encryption assigns each participant their own unique private key. This private key is asymmetrically encrypted into a publicly accessible data form known as a public key, as illustrated in the Fig. 5. The private key is kept secret by the user and is used to sign data, creating a digital signature. The public key can be openly shared and is used by others to verify the digital signature. It is also used to encrypt data that only the owner of the private key can decrypt. Participants use these public keys to securely communicate with one another (Chen, 2023; Fang et al., 2020; Simmons, 1979). In Fig. 5, the digital signature process involves two main functions: the Sign function and the Verify function. The Sign function uses the user's private key to sign data, creating a signature that is unique and verifiable. The Verify function uses the corresponding public key to confirm the authenticity of the signed data.

There are numerous models capable of performing asymmetric cryptography, with the Elliptic Curve Digital Signature Algorithm (ECDSA) standing out as one of the most widely utilized (Johnson et al., 2001; Liu et al., 2021; Simmons, 1979). ECDSA operates within an elliptic curve framework across a two-dimensional, multi-ordered, discrete finite field. Its fundamental algorithmic process involves converting a private key "k", composed of a string of 256-bit binary numbers, into a public key using an asymmetric encryption algorithm. Specifically, ECDSA derives a public key by mapping it onto an image, defined by a selected model of an elliptic curve function over a discrete finite domain, and subject to specific constraints. In ECDSA, this resultant public key manifests as a point on the elliptic curve function. Due to the vast number of possible binary numbers of varying bits and sizes that can be derived from this public key point, deducing the private key from the public key becomes practically infeasible, exemplifying the essence of asymmetric encryption (Johnson et al., 2001; Liu et al., 2021). The elliptic curve used by ESCDA needs to satisfy a basic condition (Specific examples are shown in the appendix):

$$f(i) = i^3 + pi + q \ where - 16\left(4p^3 = 27q^2\right) \neq 0$$

In the prescribed elliptic curve function model, assuming that the private key is k and the public key P, the base point of the elliptic curve is prescribed to be the base point B (i, j), and ki and kj are calculated by

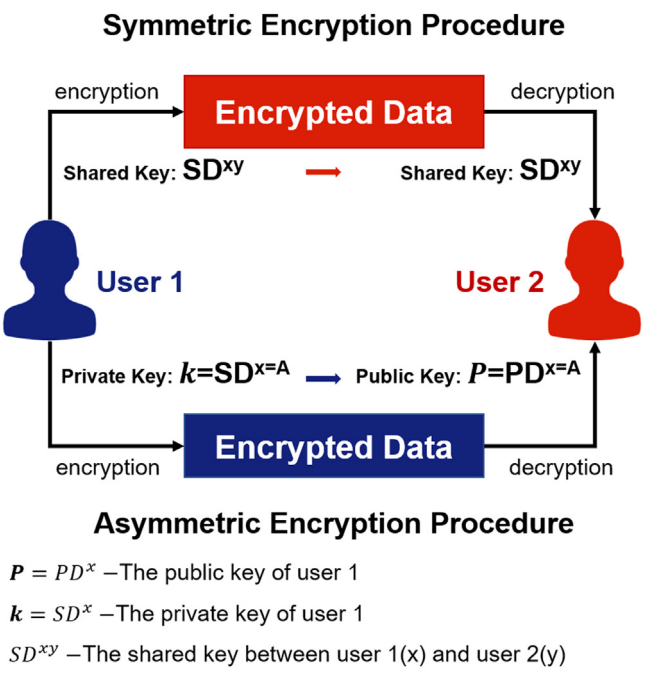


Fig. 5. Diagram of Asymmetric Encryption and Symmetric Encryption Verification. The diagram illustrates the fundamental concepts of asymmetric and symmetric encryption methods, which are categorized as follows: (a) Symmetric encryption uses a single key for both encryption and decryption of data; This key must be securely shared between the sender and the recipient before any encrypted communication can take place. (b) Asymmetric encryption involves a pair of keys: a private key and a public key. The private key is kept secret by the user and is used to sign data, creating a digital signature. The public key can be openly shared and is used by others to verify the digital signature. It is also used to encrypt data that only the owner of the private key can decrypt.

"elliptic multiplication" to obtain the public key:

$$P = (ki + kj) = kB$$

This algorithm here introduces two special new rules of arithmetic, called "elliptic addition"[9] and "elliptic multiplication".[10] By analogy, the final public key P=kA is obtained by 2^{256} "additions" of the private key k. In addition, it is necessary to define a multi-order two-dimensional discrete interval to prevent the intersection line or tangent line obtained by two points or $(A + A)$ from intersecting the elliptic curve without a new intersection, which makes it impossible to enter the public key "B". "B". The addition of kA is not "$A + A$ = 2A, 2A+A = 3A, ……, (k-1)A + A=kA", but actually it is an exponential increase of the number of points of symmetry through the intersection of tangents. In fact, it is through the continuous "intersection of tangent points, find the symmetry point" of exponential increase, that is, "$A + A$ = 2A, 2A + 2A = 4A, 4A + 4A = 8A, ……, 2^{255}A + 2^{255}A = 2^{256}A ". Hereby the program

[9] Elliptic Addition: In a Cartesian coordinate system, consider two points on a plane, point A (with coordinates (i1, j1)) and point B (with coordinates (i2, j2)). The result of "A + B" is defined as follows: the line segment AB, which connects point A (i1, j1) and point B (i2, j2), intersects the chosen elliptic curve at point C (i3, j3). The point C2 (i3, -j3), which is the reflection of C across the x-axis, is the result of the addition. In cryptography, C2 is referred to as an element of an Abelian group. (Source: Wikipedia)

[10] Elliptic Multiplication: Similarly, the operation A + A is determined by the tangent line at point A (where it touches the curve) intersecting the elliptic curve at another point D (i4, j4). The point D2, symmetric to D with respect to the x-axis (i4, -j4), represents the result of "A + A," indicating that A + A = 2A = D2. Continuing this process, adding D2 to A yields the new intersection point, symmetrically mirrored with respect to the x-axis, resulting in 3A, denoted as point E2, which represents the outcome of A + A + A. (Source: Wikipedia)

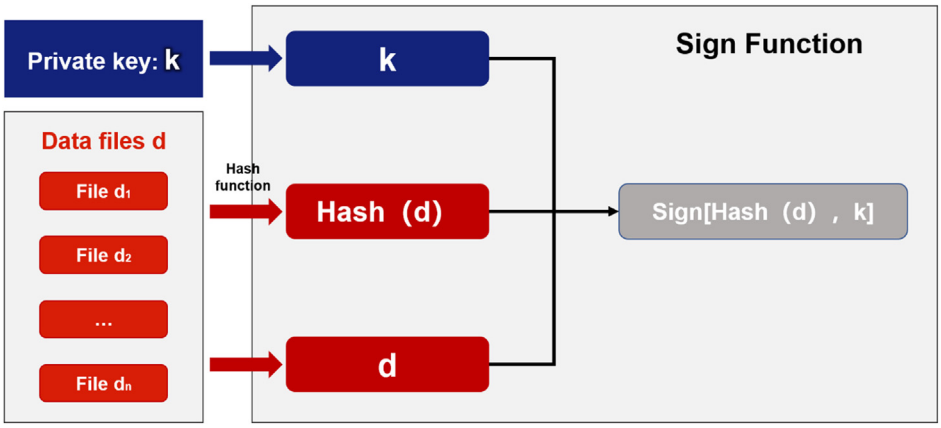


Fig. 6. Flow of the Sign Function. The figure outlines the process flow of how the Sign function operates within the digital signature scheme. The flow generally includes the following steps: (a) Input of Independent Variables: The Sign function requires three independent variables: the hash value of the data file (Hash(d)), the data file itself [d], and the private key (k) of the user signing the data; (b) Hashing: The data file [d] is passed through a cryptographic hash function to produce a fixed-size hash value (Hash(d)). This hash value represents the digital fingerprint of the data; (c) Signing: The private key (k) and the hash value are then used as inputs to the Sign function, which outputs a signature value (sign(Hash(d), k)); (d) Output: The result, which is the digital signature, is a pair of values (m, n) that uniquely represent the signed data file.

only needs 256 new "addition" operations instead of $(2^{256} - 1)$ to get the public key:

$$\boldsymbol{P = k * B}$$

As shown in the Fig. 6, the Sign function requires three independent variables as input. The first independent variable is the function value Hash(d), obtained by hashing the data file [d] related to the direct air capture projects to be signed, and the second is the data file [d] itself. The third independent variable is the private key k. By inputting these three independent variables into the Sign function, the operation will output the function value sign(Hash(d), k).

The operation rules of the Sign function are divided into four parts: first, generate a random proprietary private key k (not the signer's personal key), and obtain the public key P based on the specified datum B; then, define the i-axis coordinates of the public key P to be m; second, assign that

$$n = k^{-1}(Hash(\mathrm{d}) + k * m)$$

where k^{-1} is the inverse element[11] of k inverse element, (i.e., $k^{-1} * k = 1$). Finally, the Sign function obtains the function value (m, n) by operation, i.e., the function value of sign (Hash (d), k) is the coordinate point (m, n). Its operation process is shown in Fig. 7.

When the Sign function completes the "signature" process, it is necessary to use the Verify function for the "verification" process. The Verify function involves the input of three independent variables: the data to be signed (d), the function value Sign(Hash(d), k), and the public key P, which is the dependent variable of the Sign function. As shown in the figure, after entering these three values, the Verify function will be executed and automatically return a Boolean value[12] (true or false). The logic of the Verify function's operation primarily involves programmatically verifying two issues:

A. It proves that the Sign function and the public key P use the same private key k, thereby confirming the identity of the corresponding engineer or other relevant person responsible for the signature.
B. It proves that the Sign function is used for signing the specified DAC project data file "d" rather than another data file "d*".

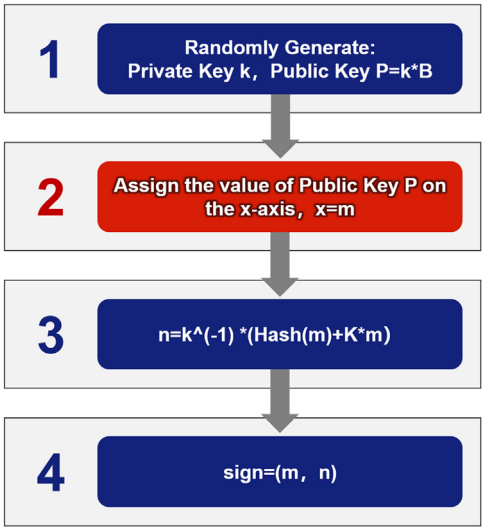


Fig. 7. Operation Rules for the Sign Function. The figure provides a detailed explanation of the operational rules for generating the digital signature using the Sign function. The process includes: (a) Generation of a Random Private Key (it is generated for the signing process. This is not the user's actual private key but a value used for the specific operation); (b) Calculation of Public Key P (generated via utilizing ECDSA); (c) Signature Calculation ($n = k\hat{}(-1) * (\mathrm{Hash(m)} + K * \mathrm{m})$); (d) Output of Signature (The final signature is (m, n), which are the coordinates of a point on the elliptic curve that represents the signed data file.).

Only when these two issues are verified to match will the Verify Function return a Boolean value of "true"; otherwise, it will return a Boolean value of "false".

As shown in the figure, the specific rules of operation of the Verify function are mainly divided into two parts: first, the introduction of α and β, and the provisions of α and β

$$\alpha = n^{-1} * hash(d)$$

$$\beta = n^{-1} * m$$

where d, m, and n all come from the variables in the Sign function that needs to be verified. Then, substitute the value of "n" in Sign function:

$$n = k^{-1}(Hash(d) + k * m)$$

Perform the computation to get

$$\alpha * B + \beta * P = \alpha * B + \beta * k * B = \alpha + k * \beta B = n^{-1} hashd + k * mB = k * B = P$$

[11] The word 'inverse' is derived from Latin: inversus that means 'turned upside down', 'overturned'. This may take its origin from the case of fractions, where the (multiplicative) inverse is obtained by exchanging the numerator and the denominator (the inverse of $\frac{i}{j}$ is $\frac{j}{i}$. (Source: Wikipedia)

[12] Boolean value: In mathematics and mathematical logic, Boolean algebra is a branch of algebra. It differs from elementary algebra in two ways. First, the values of the variables are the truth values true and false, usually denoted 1 and 0, whereas in elementary algebra the values of the variables are numbers (Boole, 1847).

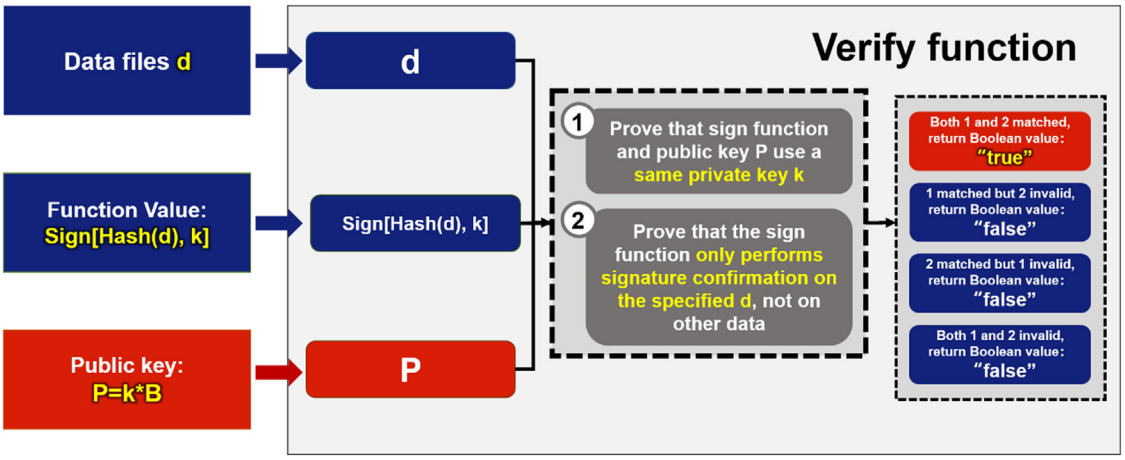


Fig. 8. Flow of the Verify function. The figure represents the procedural flow of the Verify function within the digital signature scheme. The Verify function is used to verify the authenticity of a digital signature. The flow generally includes the following steps: (a) Input of Variables: The Verify function requires three pieces of information: the original data file (d), the digital signature (sign(Hash(d), k)), and the public key (P) associated with the signer; (b) Execution of Verify Function: The function is executed with the provided inputs. It checks whether the signature is valid and whether it was indeed created by the signer using their private key; (c) Return of Boolean Value: Based on the verification process, the Verify function returns a Boolean value. If the signature is valid and matches the data file, it returns "true," indicating successful verification. If the signature is invalid or does not match the data file, it returns "false".

In the entire calculation process, if the final calculation of the public key P matches the public key P generated by the asymmetric encryption of the randomly generated private key k in the previous Sign function, then the verification is accurate, and a Boolean value of "true" is returned. During the normal operation of the two functions in the digital signature program (Sign function and Verify function), if the "data confirmation" and "identity confirmation" parts do not match, it will result in the final public key P not matching the original public key. In this case, a Boolean value of "false" is returned. The procedural mismatch (false) under the mathematical logic indicates the failure of the digital signature confirmation process, which ensures the authenticity of the data tracking during the operation of the project.

Digital signature technology, coupled with the ECDSA, can effectively secure the data recording, modification, transfer, and storage processes involved in the construction and operation of direct air capture (DAC) projects. In DAC projects, accurate data recording is critical for tracking carbon capture metrics and operational parameters. Every time an engineer or responsible party uploads data, the data must be "signed" via using their private key. This digital signature uniquely identifies the data provider and ensures that the data originates from an authenticated source. For example, when an engineer records daily CO_2 capture volumes, they sign this data with their private key before it is uploaded to the blockchain. This signature is then verified by other nodes in the consortium blockchain using the engineer's public key, ensuring the data's authenticity and preventing unauthorized uploads. Since blockchain is a decentralized structure, user operations within the blockchain system are observable and trackable, preventing illegal tampering with data in an open and transparent environment within the consortium chain. Any modifications to the recorded data, such as corrections or updates, require a new digital signature from the person making the changes. For instance, if an update is needed for a previously recorded carbon capture metric, the new data must be signed by the individual responsible for the modification. This process ensures that every change is authenticated and traceable back to its origin. In addition, when modifications occur, the supporting documentation and rationale for the changes must be shared with all project participants on the blockchain. This ensures that everyone in the consortium chain is informed, and the changes are validated by requiring the signature of the responsible authority.Fig. 8, Fig. 9

For the management of data and information involved in DAC project construction and operation, this paper proposes a strategy to convert information into a public key, as shown in Fig. 10, which can be applied to distributed broadcasting and information transfer among users in the consortium chain system. For example, when disseminating operational data or updates across the network, the information is encrypted using asymmetric encryption, and the public key is shared with authorized users in the consortium. Only users with the corresponding private key can decrypt and access the data, ensuring both security and confidentiality. The architecture suggests the use of a PKI system to manage the lifecycle of digital certificates, which are used to verify the authenticity of public keys. By deploying the aforementioned cryptography-based

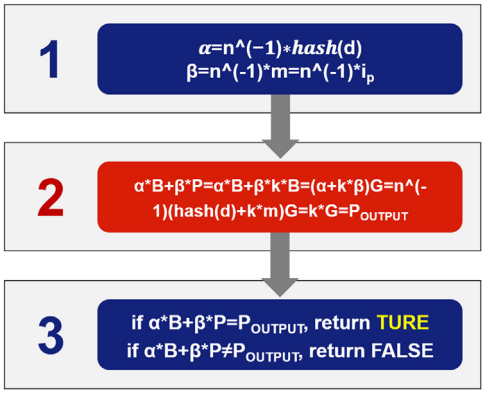


Fig. 9. Operation Rules for the Verify Function. The figure details the operational rules for the Verify function, which typically includes: (a) Calculation of α and β: The values of α and β are calculated using the public key (P), the signature point (n, m), and the hash of the data file (Hash(d)). The formulas provided in the figure are used for this calculation; (b) Point Addition on Elliptic Curve: Using the values of α and β, point addition is performed on the elliptic curve. This involves adding the point αB (where B is the base point of the elliptic curve) to the point βP (where P is the public key point). The result of the point addition is compared with the expected public key (P_OUTPUT), which is derived from the signer's private key (k) using the formula provided; (c) Return of Verification Result: If the result of the point addition matches the expected public key (P_OUTPUT), the Verify function returns "true," confirming that the signature is valid and was created with the corresponding private key. If the result does not match, the function returns "false," indicating that the signature is invalid or has been tampered with.

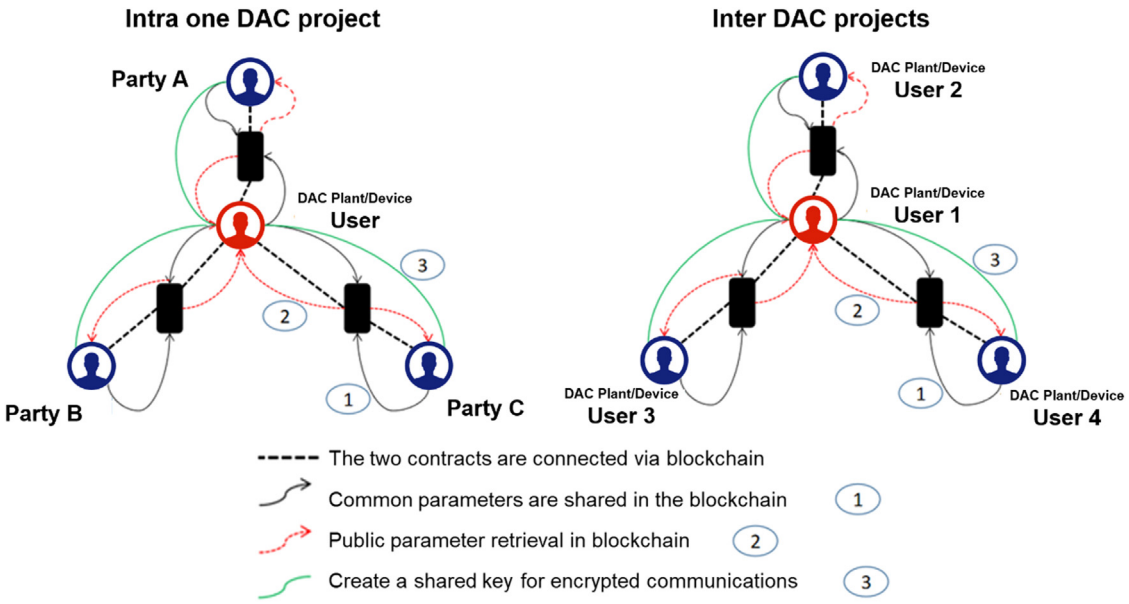


Fig. 10. System Architecture of the Proposed Key Management "Dual Authentication" Strategy. The strategy is designed to address the need for stringent data security and integrity in the context of blockchain-based DAC project management. The proposed system architecture aims to provide a dual layer of security—ensuring both the authenticity of the data through digital signatures and the confidentiality of the data through encryption. This dual-authentication strategy is essential for DAC projects not only intra one DAC project but also inter DAC projects information management, where data integrity and security are paramount for regulatory compliance, investor confidence, and effective project management.

asymmetric encryption technology, the sharing of asymmetrically encrypted private key information among DAC project participants (i.e., system users) can effectively achieve dual authentication of "insider authentication" and "data security and confidentiality". The architecture includes the use of smart contracts that can automate processes and enforce rules within the DAC project management. These contracts are self-executing with the terms of the agreement directly written into code. For instance, when a DAC project participant needs to access sensitive information, they must authenticate their identity using their private key. At the same time, the data they access is protected through encryption, ensuring that only authorized participants can view or modify it. This dual-layer security framework is essential for maintaining the integrity and confidentiality of DAC project data, particularly in sensitive areas such as carbon footprint tracking and regulatory compliance.

3.5. Decentralized DAC deployment and information management conceptual model based on blockchain consensus mechanism

According to the IEA's Net Zero Scenario, the large-scale deployment of future DAC projects will involve managing vast amounts of information and data. This includes construction management data and documents within and between projects in different regions, the cost of CO2 capture, the carbon footprint of the DAC process, system efficiency, energy consumption, and the storage or utilization of captured CO2. These elements all need to be recorded, modified, stored, and transmitted. Currently, DAC projects are primarily deployed and operated in developed and wealthy regions, including the European Union, Canada, the United States, and Switzerland. However, the total CO2 captured by existing DAC projects is still insufficient to effectively combat climate change and the greenhouse effect (Calvin et al., 2023; International Energy Agency, 2022). Conversely, most developing countries, including China, are still in the early stages of DAC technology and industrialization. Significant breakthroughs in key technologies are still required, and the lack of communication bridges at both the technological and policy levels between countries presents significant obstacles to the global large-scale deployment of DAC technology. Additionally, the absence of blockchain encryption technology and decentralized distributed storage in the global DAC project process may compromise the authenticity and traceability of data aggregation. This includes carbon footprint tracking, the calculation of negative carbon levels, net-zero and carbon-neutral strategies, as well as energy consumption and cost accounting.

Blockchain comprises interconnected blocks that form a chain. Additionally, it is a distributed data system. The principle of the blockchain consensus mechanism is that each block acts as a data storage unit, recording all data transaction information for each node over a specified period. These blocks are linked through a hash pointer created by a hash function (Nakamoto, 2008; Wood, 2014). A block consists of a "Block Header" and a "Block Body," each serving different roles within the blockchain. The primary function of the "Block Header" is to identify the "block identity." As shown in the figure, the Block Header comprises six parts: the timestamp, the Merkle Root hash value, the version number, the hash value of the previous block header, the random number Nonce, and the current difficulty.

The role of the block header serves as the identity of a block, ensuring its integrity and authenticity, encompassing six essential components, as depicted in the Fig. 11. The block header serves as a fundamental part of the blockchain, playing a pivotal role in establishing the identity and integrity of each block within the chain. The block header is composed of several key components: (a) Version Number (the version of the block and helps in managing different block structures that may be implemented as the blockchain evolves); (b) Hash Value of the Previous Block Header (a cryptographic hash of the header of the preceding block, creating a link in the chain); (c) Merkle Root (the combined hash of all the transactions in a block, represented in the block header.); (d) Timestamp (the record of the exact time when the block was created); (e) Current Difficulty (it reflects the computational difficulty required to mine the block, a crucial parameter in Proof of Work-based blockchains); (f) Nonce (a random number used in the mining process to produce a hash within a certain range, indicating a successful mining instance). These six components undergo successive nested hash function operations, resulting in an output known as the "hash value," which defines the identity of the current block header. Crucially, the hash value of the previous block header is also incorporated into the hash function calculation of the current block, thereby forming a vital

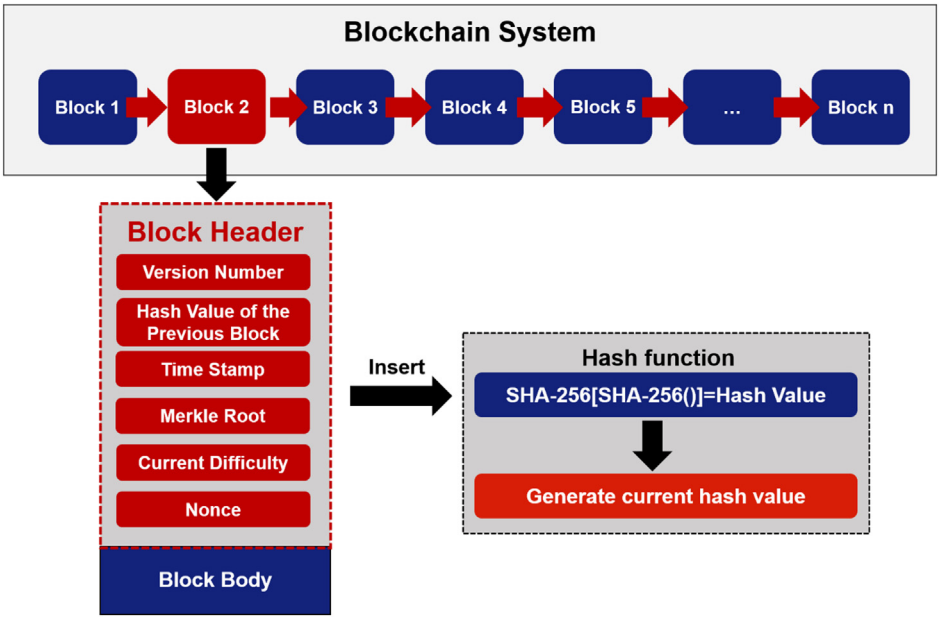


Fig. 11. Components of the 'block header' and the principle of its functioning. The block header serves as a fundamental part of the blockchain, playing a pivotal role in establishing the identity and integrity of each block within the chain. The block header is composed of several key components: (a) Version Number (the version of the block and helps in managing different block structures that may be implemented as the blockchain evolves); (b) Hash Value of the Previous Block Header (a cryptographic hash of the header of the preceding block, creating a link in the chain); (c) Merkle Root (the combined hash of all the transactions in a block, represented in the block header.); (d) Timestamp (the record of the exact time when the block was created); (e) Current Difficulty (it reflects the computational difficulty required to mine the block, a crucial parameter in Proof of Work-based blockchains); (f) Nonce (a random number used in the mining process to produce a hash within a certain range, indicating a successful mining instance).

linkage in the blockchain's interconnected chain for information transfer and integrity (Cachin, 2016). Moreover, the data stored within the "Block Body" is encapsulated within the Merkle Root hash value, further contributing to the overall block hash. Each new block's header inherently includes a timestamp, marking its creation time. This timestamp, along with referencing the hash value of the preceding block, forms the foundational basis for sequencing data within the blockchain. Consequently, all nodes within the blockchain network have visibility into the complete history of open data records, arranged in a chronological sequence. This chronological ordering enables nodes to trace data back to its origin along the blockchain's timeline, ensuring transparency and verifiability. In the event of any attempted tampering with data by a node, the blockchain's design facilitates effective verification of data authenticity across all nodes, safeguarding the integrity of recorded information (Cachin, 2016).

The primary function of the block body is to store data information, organized in the hierarchical structure of a Merkle tree (Alzubi, 2021; Coron et al., 2005). The Merkle tree utilizes hash functions to construct a binary tree-like data structure, where each leaf node represents individual data blocks. The leaf nodes of the Merkle tree represent the individual data blocks or transactions. Each leaf node contains the hash of a specific piece of data, such as a transaction record in a blockchain. Each higher-level node in the tree aggregates the hash values of its child nodes. As these levels progress, they culminate in the generation of the "root value" of the Merkle tree data structure, earning it the name "Merkle Tree" due to its branching resemblance to a tree (Coron et al., 2005). The integrity of the "Merkle Tree" data structure hinges on the collision resistance property of hash functions. Any alteration to data within a block will lead to a modification in its corresponding hash value, cascading changes up the tree to the Merkle Root. Thus, once the Merkle Root is established, it becomes computationally impractical to tamper with any block of data without detection (Alzubi, 2021; Cachin, 2016).

As depicted in the Fig. 12, to interlink all data stored within the block body using the "Merkle Tree," each data file (i_1, i_2, i_3,..., i_n) undergoes two consecutive rounds of nesting with the SHA-256 function. The first application, $SHA256(SHA256(i_1))$, results in $Hash_1$, and this process is repeated to derive $Hash_1$, $Hash_2$, $Hash_3$, $Hash_4$, $Hash_5$.....$Hash_n$ for each respective data file. These hashes form the lowest level of data. Moving up to the second level, $Hash_1$ and $Hash_2$ are merged and nested again with SHA-256 to produce $SHA256(SHA256(Hash_{12}))$, denoted as $Hash_{12}$. Similarly, $Hash_{34}$, $Hash_{56}$,....., $H_{n(n-1)}$ are derived through analogous operations. This pattern continues with successive rounds of SHA-256 nesting, creating the third layer with $Hash_{1234}$, $Hash_{5678}$, ..., $H_{n(n-1)(n-3)(n-2)}$, until reaching the final operation resulting in $H_n!$. Because the hash pointer links the entire structure, any alteration to data within the "Block Body" will propagate changes up to the Merkle Root ($Hash_n!$), thus affecting the entire block. The security of the Merkle tree lies in the properties of the cryptographic hash function used. It is computationally infeasible to generate the same hash output from different inputs due to the hash function's collision resistance and one-way properties. The Merkle tree's structure ensures that any change in the data set will be detectable. This is because the hash values are derived from the data itself, and any alteration will result in a different hash value. This property underpins the tamper-proof nature of blockchain. Therefore, the Merkle Root effectively binds together the block header and block body, ensuring integrity across the entire block structure.

Consequently, alongside integrating digital signature technology into the deployment and management of DAC projects, it is essential to leverage the blockchain's consensus mechanism for managing a consortium blockchain system in decentralized Direct Air Capture initiatives. Blockchain systems offer robust stability and data integrity, ensuring the credibility and traceability of carbon capture and carbon footprint data. The consensus mechanism, such as PoS or Delegated Proof of Stake (DPoS) ,[13] plays a critical role in maintaining this stability by ensuring that all participating nodes in the consortium blockchain reach agreement on the validity of transactions and data entries. In DAC projects, validators comprising key stakeholders such as DAC companies, operators, and investors participating in the consensus process by staking tokens or being elected as delegates. This method ensures that only legitimate and authenticated data is added to the blockchain, thereby safeguarding the accuracy and integrity of crucial project information such as carbon capture volumes and energy usage metrics. With numerous stakeholders involved in DAC projects, not all information needs to be publicly accessible, making it feasible to construct a system that selectively involves project stakeholders. Section 3.3 provides a specific analysis where a consortium blockchain system optimizes the deploy-

[13] Delegated Proof-of-Stake (DPoS) is a modified version of the Proof-of-Stake (PoS) consensus mechanism. In DPoS, participants select delegates to validate blockchain blocks. DPoS offers an inclusive, scalable, and democratic approach to transaction validation in a blockchain network. (Source: Wikipedia)

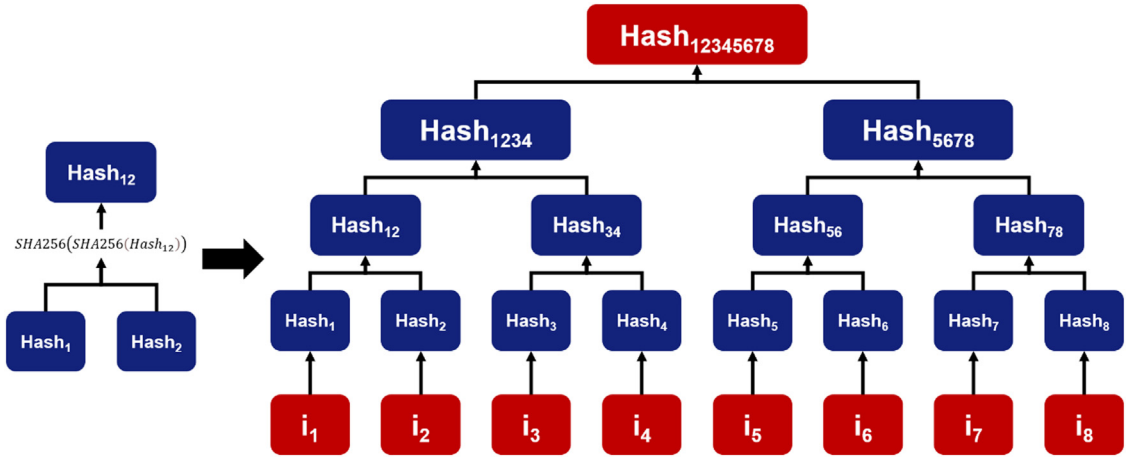


Fig. 12. Data structure of "Merkle Tree". The figure shows a series of nodes with hash values, starting from the leaf nodes at the bottom and culminating in the Merkle Root at the top. The arrows or lines connecting the nodes would indicate the hierarchical relationship and the flow of data aggregation through hashing.

ment and operational management of DAC projects, facilitating a partially decentralized operational model and deployment strategy. In this framework, the consensus mechanism not only ensures the integrity of the data but also allows for flexible participation based on predefined roles and privileges. For instance, DAC technology providers and operators, who act as premium nodes, have higher stakes in the system and thus greater influence in the consensus process. This ensures that those with the most responsibility for project outcomes have a more significant role in verifying the accuracy and authenticity of critical data. At the same time, the consensus mechanism helps balance the system's efficiency by minimizing the computational resources needed for validation, aligning with the sustainability goals of DAC projects. In the context of DAC projects, consortium blockchain nodes encompass various project participants: DAC equipment technology firms, specific DAC project operators, suppliers across the supply chain, relevant governmental departments (if applicable), international energy agencies (if applicable), investors, and construction entities. The consortium blockchain system enhances the deployment and operational management modes of DAC projects, granting different parties varying degrees of participation. The consortium blockchain, where multiple entities collaborate on a shared, yet permissioned ledger, is partially decentralized, meaning that while all participants have access to the ledger, certain nodes or members may have more privileges or roles than others. Through the consensus mechanism, such as PoS or DPoS, this system ensures that all data entries, such as sensor readings from carbon dioxide concentration sensors, energy consumption data, and carbon footprint metrics, are validated by the relevant parties, maintaining a high level of trust and data integrity. As depicted in the Fig. 13, in the architecture of the consortium blockchain, blockchain nodes include various project participants such as DAC equipment technology firms, DAC project operators, suppliers, governmental departments, international energy agencies, investors, and construction entities. These participants are represented as nodes within the blockchain network, each with specific roles and access rights. DAC equipment technology providers and DAC operators may function as premium nodes, enjoying extensive information privileges and access functions. Other stakeholders operate as ordinary nodes, with access to specific functional information rights and access functions. The platform facilitates the sharing of relevant information and data files involved in DAC projects according to the privileges of the respective projects. This selective sharing of information is made possible due to the differentiated operation and access privileges in the consortium blockchain system. Furthermore, during carbon dioxide capture in DAC projects, real-time data from carbon dioxide concentration sensors, energy consumption sensors, carbon footprint sensors, environmental monitors, etc., are crucial. The consortium blockchain platform supports an Internet of Things (IoT)[14] architecture for real-time data collection, transformation, and geographical and temporal mapping of DAC projects. This enables seamless data transmission and information sharing among different DAC projects. The consensus mechanism within this architecture plays a pivotal role in ensuring that all real-time data is consistently and accurately recorded across the distributed network. By validating data through a consensus process that involves multiple stakeholders, the system ensures that the information shared among different DAC projects is both reliable and verifiable, thereby reinforcing the integrity of project operations and outcomes.

In this consortium blockchain system, which differentiates operation and access privileges and clearly delineates the responsibilities and roles of various project stakeholders, all relevant information and data files involved in DAC projects are shared among specific DAC projects according to their respective privileges through the platform. The blockchain's decentralized nature ensures that data is not stored in a single location, which enhances data security and integrity. Any attempt to tamper with the data would require altering the information across the entire network, making it highly secure against unauthorized changes. The consensus mechanism further ensures that these differentiated access rights are enforced correctly, as the system validates not only the data but also the permissions associated with each transaction. However, due to the distributed nature of different data related to DAC projects—such as extensive project construction management data and documents, real-time tracking of project system efficiency and energy consumption, tracking of the carbon footprint of the capture process, the amount of captured carbon dioxide, and the sink path of captured CO2—and the contractual constraints between project stakeholders, there may be disparities in data access levels and information sharing. Additionally, given the contractual relationships among project stakeholders, establishing absolute trust between certain parties in some special cases can be challenging. Therefore, it is essential to entrust the ownership and management of information to a distributed, decentralized platform among the members. The consensus mechanism also addresses this challenge by creating a trustless environment where data validation does not rely on the trustworthiness of individual entities but on the collective agreement of the network participants. At the same time, considering that blockchain ledger information is publicly disclosed, it is not suitable for sharing sensitive project information in the DAC project. To handle sensitive information sharing confidentially, by coupling the key management

[14] The Internet of things (IoT) describes devices with sensors, processing ability, software and other technologies that connect and exchange data with other devices and systems over the Internet or other communications networks (Atzori et al., 2010; Gazis, 2017; Gillis, 2021).

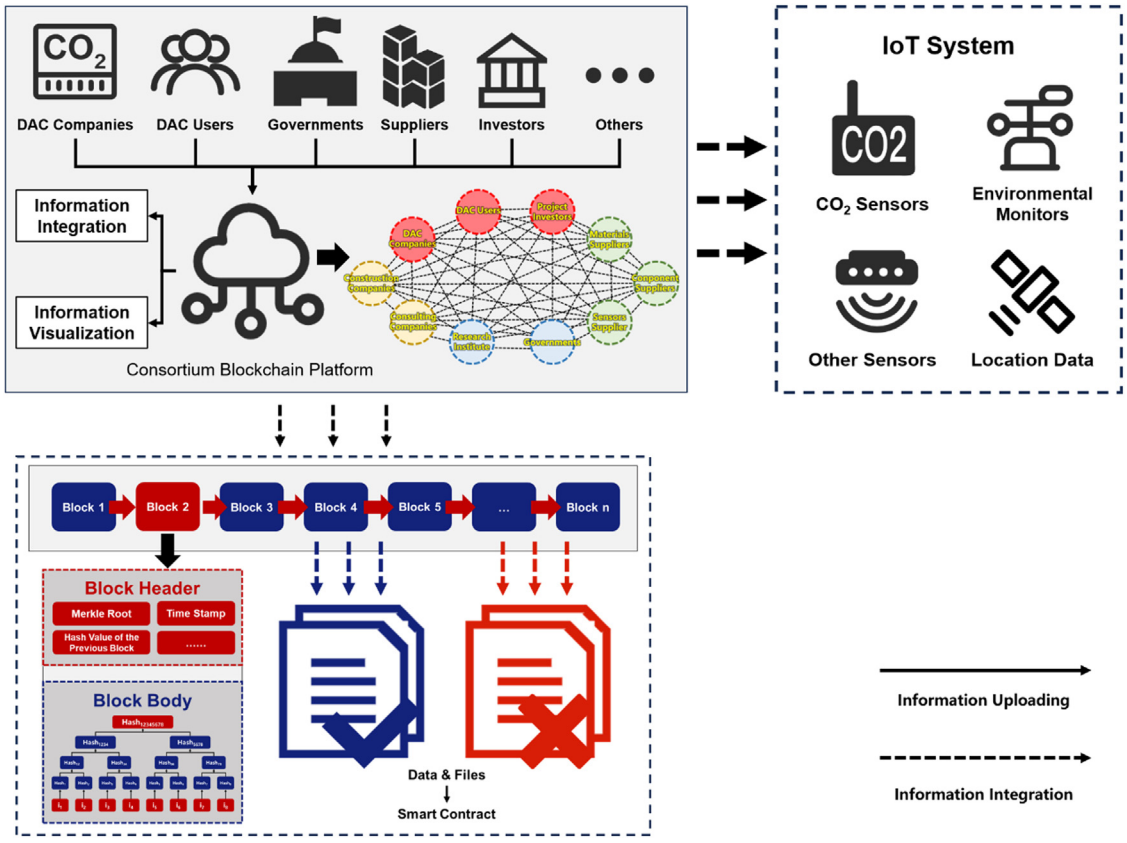


Fig. 13. Decentralized DAC Deployment and Operations Management Consortium Blockchain System. A visual representation of how a consortium blockchain system can be integrated into the deployment and management of Direct Air Capture (DAC) projects with key parts including Nodes (Premium and Ordinary Nodes) and Stakeholders, Data Flow and IoT Integration System, Information Management (Decentralized Storage and Data Integrity), Key Management "Double Authentication", Transparency and Verifiability.

"double authentication" distribution strategy proposed in Section 3.4, project-related parties can verify their identities and share sensitive information confidentially through digital signature technology. This key distribution management strategy, based on the blockchain network architecture, can verify the identity of honest parties involved in "confidential messaging," avoiding the need to delegate verification to a third-party centralized entity, effectively minimizing the energy consumption of generating key management, and reducing communication costs.

The proposed system presents transformative potential for advancing carbon neutrality efforts due to practical implications. Firstly, the use of consortium blockchain ensures that all data related to DAC projects is immutable and secure, reducing the risk of data tampering and fraud, and it enables a transparent and verifiable record of carbon capture data, allowing stakeholders to trace the history of carbon offsets and verify their authenticity. Meanwhile, by leveraging smart contracts and automated processes, the consortium blockchain can streamline DAC operations, reducing manual overhead and increasing efficiency. In addition, the transparency and reliability of the blockchain system can help DAC projects meet regulatory requirements for carbon capture reporting and verification, providing a robust framework for compliance, and attract investment by providing clear evidence of carbon capture performance and project progress. In addition, the integration of digital signature technology enhances identity verification processes, ensuring that only authorized parties can make changes to the DAC project data.

However, there are also potential bottlenecks and challenges associated with its implementation. For instance, integrating existing DAC infrastructure with new blockchain systems may be technically challenging and require significant upfront investment, especially the digital infrastructure like databases, data centers, sensor-based IoT system. As the number of DAC projects grows (Scalability Issues), the regulatory landscape for blockchain and DAC technologies is still evolving, and there may be legal and regulatory uncertainties that could slow adoption. And while DAC projects themselves are energy-intensive, the blockchain operations should also be energy-efficient to avoid adding to the carbon footprint as well as the energy consumption concerns. On the other hand, ensuring that the consortium blockchain can interoperate with other blockchains and systems used by different stakeholders is crucial for widespread adoption. Furthermore, the system must be robust against cybersecurity threats, as breaches could compromise data integrity and security.

To address these concerns, we propose a phased implementation approach, starting with pilot projects that can demonstrate the system's viability and gradually scaling up as confidence and infrastructure develop. Specifically, in terms of technical integration challenges, develop an integration framework with APIs and middleware that facilitate communication between the existing DAC infrastructure and the new blockchain systems. Regarding to upfront investment, it is necessary explore public-private partnerships, grants, or low-interest loans to finance the initial investment. Leverage cost-sharing models among stakeholders and consider the long-term savings from improved efficiency and data management. To solve scalability issues, utilizing blockchain architectures that are inherently scalable, such as those employing sharding or off-chain solutions like state channels or sidechains. Continuously monitor the network's performance and plan for upgrades to accommodate growth. About energy efficiency of blockchain operations, in the real application, it is a better choice to choose blockchain platforms that employ energy-efficient consensus mechanisms like Proof of Stake (PoS) or Delegated Proof of Stake (DPoS). Consider integrating renewable en-

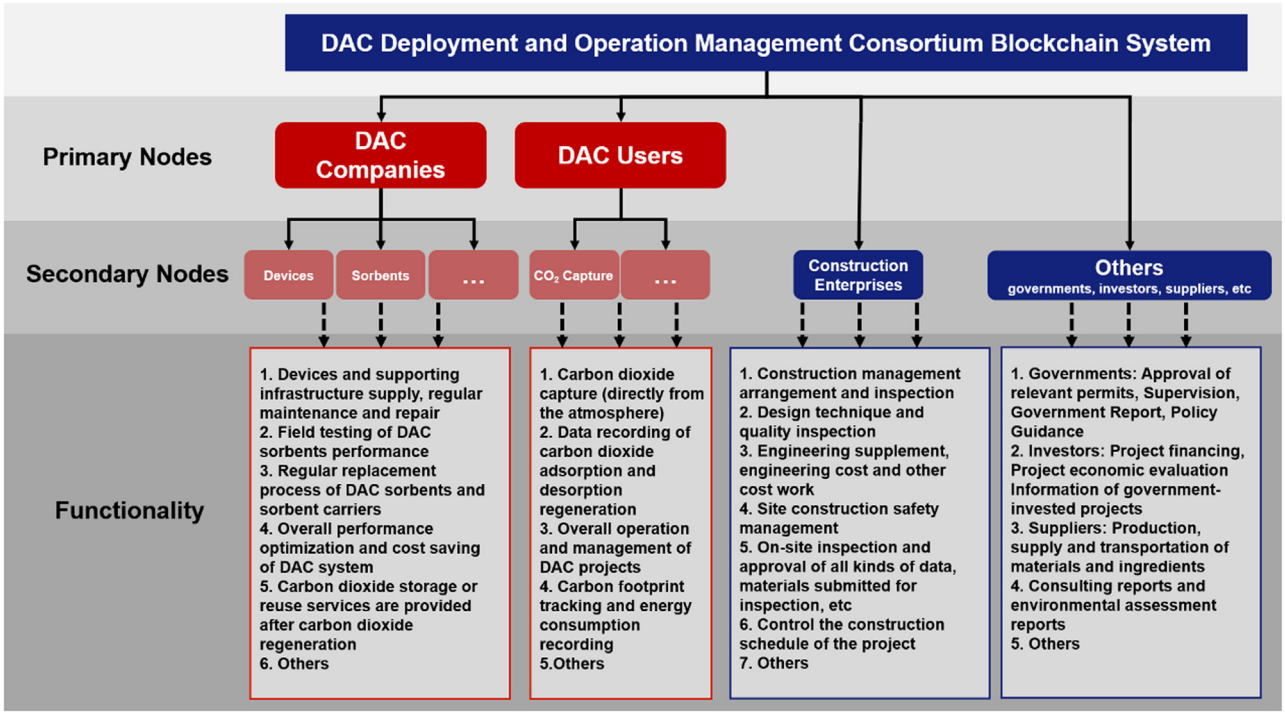


Fig. 14. Functional Diagram of DAC Deployment and Operation Management Consortium Blockchain System. The diagram represents the interconnectivity and interactions among various nodes and components of the system, which are categorized as follows: (a) Primary Nodes represent the main participants including DAC companies and users responsible for more capabilities and responsibilities for DAC projects and controls subsidiary departments (secondary nodes); (b) Secondary Nodes have less authorities and capabilities in comparison with primary; (c) The nodes are associated with specific functionalities, which are essential for the operation of the DAC projects.

ergy sources to power blockchain operations. In addition, adopt open standards and interoperability protocols to ensure seamless data exchange between the consortium blockchain and other systems, achieve interoperability with other systems. Utilize cross-chain technologies to facilitate transactions and communication between different blockchain networks. While facing cybersecurity threats, invest in robust cybersecurity measures, including regular security audits, penetration testing, and the implementation of advanced encryption standards. Develop incident response plans to address potential breaches effectively. Moreover, it is needy to emphasize the need for stakeholder education and training to ensure smooth adoption and to capture the full benefits of our proposed system.

4. DAC deployment and operation management consortium blockchain system construction

4.1. Overall design of the consortium blockchain system

Based on the rights and responsibilities of the parties involved in the DAC project, the alliance chain nodes of the system and their functions, a system functional diagram has been developed (as shown in Fig. 14). After functional abstraction, the modules of this system include creation, project contract management, document review, document upload, and document modification.

The system distinguishes between different types of nodes, such as primary and secondary nodes. Primary nodes may have more responsibilities and capabilities within the network, such as validating transactions and maintaining the ledger, while secondary nodes might have more limited roles. The nodes are associated with specific functionalities, which are essential for the operation of the DAC projects, including DAC infrastructure supply and maintenance, field testing and optimization of DAC sorbents and carriers, carbon dioxide adsorption and desorption processes, recording and management of carbon footprints, overall operation tracking and energy consumption, construction management (cost, quality, safety, etc.) and so on. Each stakeholder is associated with particular roles and responsibilities within the DAC project lifecycle, from government approvals and financing to material supply and construction management, and it is great to echo the conceptual model in Section 3.5. The system is composed of several key modules that facilitate different aspects of DAC project management, including “Creation”, “Contract Management” and so on.

Fig. 15, which is an accompanying diagram to Fig. 14, would typically provide a detailed Unified Modeling Language (UML)[15] use case diagram. The figure also identifies various stakeholders involved in the DAC projects, such as DAC companies, project investors, DAC users, construction enterprises, governments, suppliers and other interested participants. Each stakeholder group has specific roles and interactions with the system. This figure illustrates the interactions between various participants (such as DAC Users, Construction Enterprises, Governments, Investors, Suppliers, etc.) and the system’s functionalities, showing how they utilize different modules within the blockchain system. For actors (participants in the blockchain system), the diagram would typically identify different actors or users who interact with the system, including DAC Users (Individuals or entities utilizing the DAC project services), DAC companies (Providers of DAC technology service), Investors (Entities providing financial support for DAC projects), Suppliers (Providers of materials like sorbents and other necessary for DAC projects) and other interested parties. Use cases are the actions or operations that the system allows users in the system to perform, including project initiation (the process of starting a new DAC project within the blockchain system), documents upload (the functionality allowing users to upload relevant documents to the blockchain), project supervision (activities

[15] The unified modeling language (UML) is a general-purpose visual modeling language that is intended to provide a standard way to visualize the design of a system (Medvidovic et al., 2002).

Table 4
Information structure of the users of consortium blockchain system.

Attribute	Type	Purpose/Statement	Constraints/Units
Id	Integer	Unique identifier for each user in the system.	Auto-incremented by the system.
Address	String	Blockchain address associated with the user's node.	Must be a valid blockchain address format.
Name	String	The name of the system user.	No special characters; limited to 50 characters.
Password	String	Password for user authentication.	Must be at least 8 characters long, include uppercase and lowercase letters, a number, and a special character.
Identity	String	Role or identification of the user within the system.	Must be one of the predefined roles.
Time	DateTime	Date and time of user registration.	Stored in UTC; format: YYYY-MM-DD HH:MM

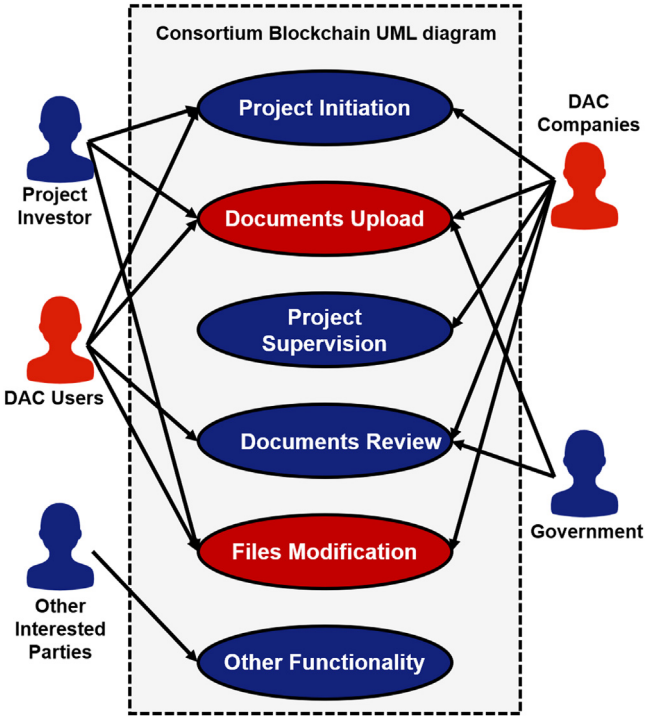


Fig. 15. System UML Use Case Diagram. The diagram a visual representation that illustrates the various actors and their interactions with the system's functionalities within the context of a Consortium Blockchain System designed for Direct Air Capture (DAC) deployment and operation management.

related to overseeing and managing the progress of DAC projects), files modification (the ability to make changes to the documents and data within the system), and other functionality (additional features and processes supported by the system). The diagram also shows the relationships between the actors and the use cases, including which actors are involved in each use case and The flow of actions between actors and the system.

4.2. Consortium blockchain system architecture design

This system uses blockchain to store data, requiring several structures to be defined in the smart contract[16] to store data in a tabular format. The consortium blockchain system is designed to store data across a decentralized network. This data is structured in a tabular format within smart contracts, which are self-executing contracts with the terms of the agreement directly written into lines of code. The system defines several data structures within the smart contracts to organize and store information in a clear and accessible manner. These structures act like tables in a database, allowing for the systematic recording and retrieval of data.

As illustrated in the Table 4, the user information structure is used to store user information. The Address serves as the unique identifier for each user, representing "the address of the node where a user is located in the blockchain." This table stores user information, which is essential for managing access and identities within the blockchain system, including "Id" (a unique identifier for each user, auto-incremented by the system), "Address" (the blockchain address associated with the user's node, ensuring a valid format), "Name" (the name of the user, with restrictions on special characters and length), "Password" (a secure password for user authentication, with complexity requirements), "Identity" (the role or identification of the user within the system, predefined to maintain consistency), "Time" (the date and time of user registration, stored in UTC for universal standardization).

Additionally, to include DAC project participants in the Consortium Blockchain system, the project participant structure is introduced to store information about the work of each project participant (Table 5). Table 5 is designed to include DAC project participants in the consortium blockchain system, storing information about each participant's involvement in the project, including "Id" (a unique identifier for each project participant), "Project" (the name of the DAC project the participant is involved in, with a character limit for uniqueness), "Investor" (the name of the entity investing in the project), "DACUser" (the user or entity utilizing the DAC project services), "DACCompany" (the DAC technology services provider involved in the project), "Suppliers" (information about suppliers of materials and ingredients for the DAC project), "Others" (information about other stakeholders or interested parties), "Time" (the date and time of the participant's registration or involvement in the project).

A DAC project comprises various types of files, necessitating the creation of the structure illustrated in the Table 6 to store these files. Table 6 is created to manage the various types of files associated with a DAC project.The project file is linked to the project through the "project_id", and the "uploader_id" connects it to the uploader. The "file_hash" is the hash value returned after the file is stored in the IPFS file system, which can be used to retrieve the file. It includes: "Id" (a unique identifier for each document related to the project), "File Name" (the name of the file, with a limit on the number of characters), "File Hash" (the IPFS hash value for the file, used for retrieval and ensuring the integrity of the file), "Uploader Id" (the identifier of the user who uploaded the file, linking it to a valid user account), "Project Id" (the identifier of the DAC project associated with the file), "Validity" (the verification status of the file, indicating if it's approved or not), "Delete" (the deletion status of the file, allowing for soft deletions), "Type" (the type of the file, such as a contract, report, or image, with predefined types within the system), "Time" (the date and time the file was uploaded or last modified, stored in UTC).

The Consortium Blockchain System Architecture Design leverages smart contracts to create a structured, secure, and efficient way to store and manage data related to DAC projects. The tables within the system

[16] Smart contracts are digital contracts stored on a blockchain that are automatically executed when predetermined-terms and conditions are met. Smart contracts are typically used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without any intermediary's involvement or time loss. They can also automate a workflow, triggering the next action when pre-determined conditions are met. (Source: Wikipedia)

Table 5
Information structure of DAC project participant of the federation chain system.

Attribute	Type	Purpose/Statement	Constraints/Units
Id	Integer	Unique identifier for each project participant in the system.	Auto-incremented by the system.
Project	String	Name of the DAC project the participant is involved in.	Limited to 100 characters; must be unique within the organization.
Investor	String	Name of the entity investing in the DAC project.	Limited to 100 characters.
DACUser	String	User or entity utilizing the DAC project services.	Limited to 100 characters.
DACCompany	String	DAC technology services provider involved in the project.	Limited to 100 characters.
Suppliers	String	Suppliers of relevant materials and ingredients for the DAC project.	Limited to 200 characters.
Others	String	Other interested parties or stakeholders in the DAC project.	Limited to 200 characters.
Time	DateTime	Date and time of the participant's registration or involvement in the project.	Stored in UTC; format: YYYY-MM-DD HH:MM

Table 6
Project document structure.

Attribute	Type	Purpose/Statement	Constraints/Units
Id	Integer	Unique identifier for each document related to the project.	Auto-incremented by the system.
File Name	String	Name of the file associated with the DAC project.	Limited to 255 characters.
File Hash	String	IPFS index hash value for the file, used for retrieval.	Must be a valid IPFS hash.
Uploader Id	Integer	Identifier of the user who uploaded the file.	Must match a valid user Id.
Project Id	Integer	Identifier of the DAC project to which the file belongs.	Must match a valid project Id.
Validity	Boolean	Verification status of the file (approved or not).	True if approved, False otherwise.
Delete	Boolean	Deletion status of the file (soft deletion indicator).	True if deleted, False otherwise.
Type	String	Type of the file (e.g., contract, report, image).	Limited to predefined types within the system.
Time	DateTime	Date and time the file was uploaded or last modified.	Stored in UTC; format: YYYY-MM-DD HH:MM

serve to organize user information, participant details, and document management, ensuring that all data is accessible, traceable, and secure, which is crucial for the operation and success of DAC projects.

4.3. Consortium blockchain system functional module design

A. Login and Registration Module: To ensure that each node is registered only once, the program first checks if the node's address exists in the user information structure. If it does not exist, the node is not registered. Upon adding new information to the user information structure, registration is successful, and a user ID is returned. When a user logs in, the program verifies if the node has been registered by checking the user information structure for the node address. If the node is registered and the input password is correct, the login is successful.

B. DAC Project Initiation Module: Since only the construction unit can create a project, it is necessary to first verify the identity of the project creator. To manage multiple requests for project creation efficiently and avoid potential conflicts or delays, the system employs a queuing mechanism. When a project creation request is submitted, it is assigned a unique timestamp and placed in a priority queue based on the time of submission and the user's authorization level. The system processes requests sequentially, ensuring that the first-come, first-served principle is upheld. In the event of simultaneous submissions, the system cross-references the timestamps to determine the order of processing. Additionally, the system provides real-time feedback to users regarding the status of their project creation request, allowing them to make informed decisions and reducing the likelihood of duplicate submissions. After verification, a new project information structure is created, and its ID is returned.

C. Project-Related File Upload Module: This module first verifies user permissions. Before files are uploaded to the IPFS file system, the module will now include a preliminary integrity check. This step employs a cryptographic hash function to generate a unique hash value for the file. The generated hash is then compared against a whitelist of pre-approved hash values or a set of rules that define acceptable file characteristics. Any file that fails this integrity check will be flagged and prevented from being uploaded, thereby ensuring that only verified and secure files are stored within the system.. Upon successful upload, IPFS returns a hash value for indexing the file. This additional layer of security safeguards the network against the potential risks associated with storing malicious files. A new project file structure is then created, incorporating the hash value and basic file information, thus completing the file upload process.

D. DAC Project-Related File Modification Module: Similar to the file upload module, this module first verifies if the user's identity is from the design unit. The file is then uploaded to IPFS, and the "file_hash" attribute of the original project file structure is updated with the hash value returned by IPFS. Whenever a file is modified, the system automatically generates a new version, while preserving all previous iterations. Each version is assigned a distinct version number, accompanied by a timestamp and the identifier of the user responsible for the modification. To prevent concurrent edits, the system implements a locking mechanism if multiple users attempt to modify the same file simultaneously. In instances where multiple users attempt to modify the same file, the system implements a robust conflict resolution protocol. Upon initiation of a file edit, the system assigns temporary 'edit locks' to the file, preventing other users from making concurrent changes. Each modification is tracked through a detailed version history, which records the timestamp, user identifier, and a summary of changes made. If concurrent modification attempts occur, the system prioritizes edits based on the initiation time or user permissions. Subsequent modifications are queued and merged sequentially, with version control ensuring that all changes are logged and can be audited. This ensures that only one user can make changes at a given time, while others are notified that the file is currently in use. Additionally, the system maintains a detailed history of all versions, enabling users to review past modifications and, if necessary, revert to earlier versions. This functionality ensures that all changes are fully traceable, and previous document states can be restored as needed. This process not only maintains the integrity of the document but also provides a transparent trail for auditing and reverting to previous versions if necessary.

E. DAC-Related File Audit Module: Only supervisory units and government departments have the authority to audit files. This module is meticulously designed to uphold the accuracy, integrity, and compliance of DAC project documentation by adhering to stringent audit criteria. It ensures that all files conform to industry standards, regulatory requirements, and organizational policies, while simultaneously safeguarding data accuracy and preventing unauthorized modifications through cross-referencing with version histories and audit logs. The module also verifies that any document alterations

are appropriately authorized. In instances where disputes or errors occur, the system triggers a resolution process that involves relevant stakeholders and a designated review panel. This panel evaluates the issue, documents the findings, and, if necessary, implements corrective actions, followed by a re-audit to confirm resolution. Any identified errors are flagged for correction, with all related actions meticulously recorded in the audit trail to maintain transparency. Should any issues remain unresolved, they are escalated to higher authorities (higher-level nodes) in the consortium blockchain system for further intervention. If the audit passes, the validity attribute of the project file structure is set to 1; otherwise, it is set to 0.

F. DAC Project Contract Management Module: The construction and supervision units jointly manage project contracts, enabling functions such as “delete files” and “classified display files”. For the “delete files” function, the system first checks permissions and then sets the delete attribute of the project file structure to 1, effectively performing a soft deletion. For the “classify and display files” function, the system verifies permissions, filters out files that have been approved but not deleted, and finally classifies and displays them based on the type attribute of the project file structure.

5. Conclusion

In conclusion, integrating consortium blockchain systems offers a transformative solution for advancing the deployment and information management of Direct Air Capture (DAC) technology. This paper has highlighted the potential of leveraging blockchain’s inherent properties—immutability, security, and transparency—to address the multifaceted challenges associated with DAC projects. The proposed consortium blockchain model provides a structured approach to data management, ensuring efficient recording, tracking, and sharing of carbon footprint data, energy consumption metrics, and operational performance indicators. The innovative application of digital signature technology, coupled with the consortium blockchain system, introduces a robust layer of security and authentication, enhancing the trustworthiness and reliability of DAC project documentation and data transactions. This dual-authentication strategy not only safeguards against unauthorized data manipulation but also facilitates a transparent and accountable project management process.

Furthermore, the paper underscores the importance of a tailored decision-making strategy for selecting the appropriate blockchain type, emphasizing the need to balance accessibility, control, and privacy in the context of DAC deployment. The consortium blockchain’s hybrid nature, combining elements of private and public blockchains, emerges as an optimal solution, catering to the unique requirements of DAC stakeholders while maintaining the integrity and confidentiality of shared information. The conceptual model presented in this paper leverages the consensus mechanism of a decentralized blockchain system, providing a scalable and adaptable framework for DAC projects. It supports the global ambitions of achieving carbon neutrality, as outlined by the IPCC and IEA, and contributes to the operational efficiency and effectiveness of DAC initiatives.

In summary, the integration of consortium blockchain systems in DAC deployment is not only a technological advancement but also a strategic imperative for the future of carbon dioxide removal technologies. Further research should focus on the deeper integration of blockchain technology to enhance data management, security, and transparency within DAC systems. Promoting cross-disciplinary research that synthesizes expertise from engineering, economics, environmental science, and social science is crucial to ensuring that blockchain solutions are not only technically robust but also compliant with regulatory and environmental standards. The development of a standardized framework for the integration of blockchain in environmental technologies is pivotal for facilitating broader adoption and enhancing interoperability across various systems and sectors. To move towards real-world implementation, the next steps should involve the initiation of pilot projects in collaboration with leading DAC companies and environmental agencies. These pilots will provide a controlled environment to evaluate and refine the blockchain system, yielding valuable insights into its scalability and overall effectiveness. Simultaneously, early engagement with regulatory bodies will be essential to ensure that these innovations adhere to all compliance requirements and can be seamlessly incorporated into existing legal frameworks. This holistic approach will be crucial for driving innovation, ensuring cost-effectiveness, and fostering widespread acceptance and implementation of DAC technologies in the pursuit of climate change mitigation strategies. It paves the way for a more coordinated, secure, and sustainable approach to combating climate change and progressing towards a net-zero emissions future.

In future research direction, to enhance data management, security, and transparency, we recognize the need for additional research in complementary areas. Specifically, we propose exploring the integration of artificial intelligence (AI) and machine learning (ML) with blockchain technology. AI and ML could offer significant advancements in predictive analytics and anomaly detection within DAC projects. By leveraging AI algorithms, the system could predict patterns in energy consumption, carbon capture efficiency, and potential system failures, allowing for proactive measures rather than reactive solutions. Machine learning models can be trained to identify outliers and anomalies in real-time data streams, enhancing the monitoring process and ensuring the early detection of issues that could affect the performance or security of DAC systems. Furthermore, AI-driven data analysis could complement blockchain’s immutability and transparency by providing deeper insights into the data collected. This could lead to more informed decision-making and optimized operational strategies for DAC projects. The combination of AI with blockchain could also improve the personalization and responsiveness of DAC systems, tailoring operations to specific environmental conditions and requirements. We also encourage research into other emerging technologies, such as the Internet of Things (IoT) for enhanced data collection and real-time monitoring, and quantum computing for potentially revolutionizing data processing capabilities within the blockchain framework. Promoting cross-disciplinary research that synthesizes expertise from engineering, economics, environmental science, AI, ML, and other relevant fields is crucial to ensuring that blockchain solutions are not only technically robust but also compliant with regulatory and environmental standards. The development of a standardized framework that incorporates these technologies for the integration of blockchain in environmental technologies is pivotal for facilitating broader adoption and enhancing interoperability across various systems and sectors.

Appendix

For certain blockchain systems, the resulting string needs to undergo a final encoding process after completing the hash operation. One encoding system closely related to the Bitcoin blockchain system is the Base-64 encoding system, as illustrated in Table 7. This system comprises 64 symbols and adheres to a 64-base encoding rule. The 64 symbols include 26 uppercase letters, 26 lowercase letters, the 10 Arabic numerals “0–9”, and the symbols “+” and “/”. For example, a random binary string “010011010110000101101110” can be encoded as “TWFu” by referring to the Base-64 encoding table (Nakamoto, 2008).

The Bitcoin blockchain system uses a different encoding system from BASE-64 encoding system called BASE-58 encoding system, which is closely related to it. BASE-58 encoding, as shown in Table 8, is based on BASE-64 encoding but with some symbols removed, including “+”, “/”, “0”, “O”, “I”, and “l”. Bitcoin’s blockchain system uses a BASE-58 encoding system that removes these six symbols from BASE-64 encoding, which may have two possible reasons: a) the deleted letters have similarities that make human recognition difficult; b) Satoshi Nakamoto’s personal preference. Therefore, BASE-58 converts the initial address obtained from the two hash operations to a 58-base binary number, adds

Table 7
BASE-64 Encoding System Table.

Numerical Value	Symbol	Numerical Value	Symbol	Numerical Value	Symbol	Numerical Value	Symbol
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/

Table 8
BASE-58 encoding system table.

Numerical Value	Symbol	Numerical Value	Symbol	Numerical Value	Symbol	Numerical Value	Symbol
0	A	16	S	32	i	48	z
1	B	17	T	33	j	49	1
2	C	18	U	34	k	50	2
3	D	19	V	35	m	51	3
4	E	20	W	36	n	52	4
5	F	21	X	37	o	53	5
6	G	22	Y	38	p	54	6
7	H	23	Z	39	q	55	7
8	J	24	a	40	r	56	8
9	K	25	b	41	s	57	9
10	L	26	c	42	t		
11	M	27	d	43	u		
12	N	28	e	44	v		
13	P	29	f	45	w		
14	Q	30	g	46	x		
15	R	31	h	47	y		

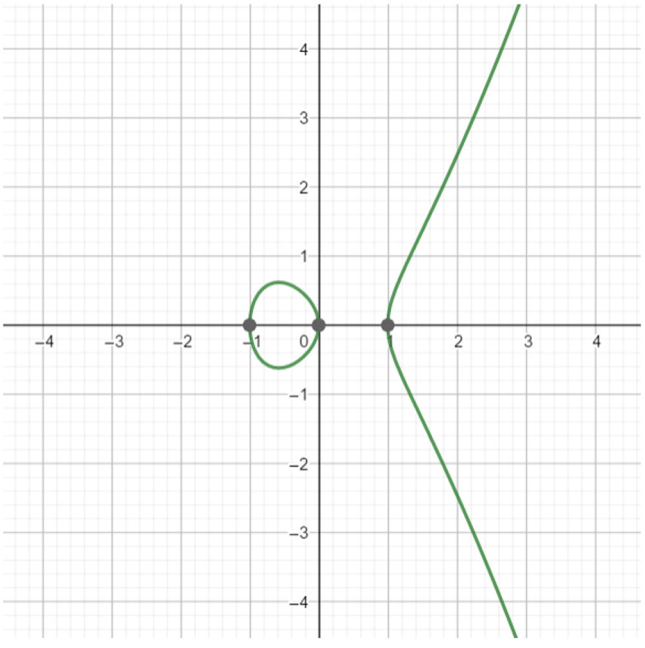


Fig. 16. The curve of $y = x^3 - x$ (Software: Origin).

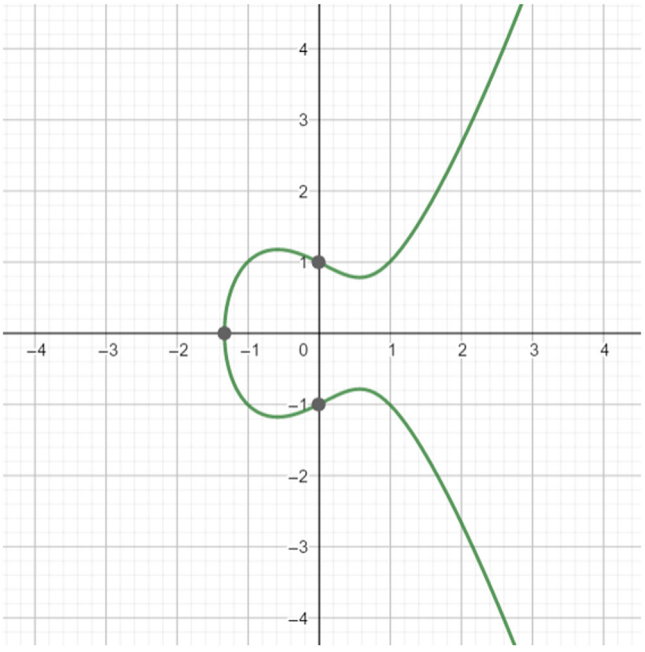


Fig. 17. The curve of $y = x^3 - x + 1$ (Software: Origin).

a “1” identifier to the front of the string, and then adds the verification characters obtained from the double hash function to the end to form the final address of a Bitcoin block.

The Bitcoin blockchain system employs a distinct encoding system known as BASE-58 encoding, closely related to BASE-64 encoding but with certain symbols omitted, as depicted in Table 8. Symbols such as “+”, “/”, “0”, “O”, “I”, and “l” are excluded from BASE-58 encoding. Bitcoin adopts BASE-58 encoding for its addresses, which removes these symbols from BASE-64 encoding, possibly for two reasons: a) these characters are visually similar, making them prone to human error; b) it reflects Satoshi Nakamoto’s personal preference. Therefore, BASE-58 converts the original address derived from two hash operations into a 58-base binary number. It prefixes the string with a “1” identifier and appends verification characters obtained from a double hash function to form the final Bitcoin address.

Take an elliptic curve function as an example, shown in Fig. 16, when a=−1 and $b = 0$.

$$-16(4\alpha^3 3 + 27\beta^3 2) = -368 \neq 0$$

$$y = x^3 - x^3 + 1$$

when a=−1 and $b = 0$, $-16(4a^3+27b^2) = 64 \neq 0$ and $y = x^3 - x + 1$, the elliptic curve is shown in Fig. 17.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests:

Jia Li reports financial support was provided by University Grants Committee Research Grants Council. Jia Li reports financial support was provided by the Science and Technology Commission of Shanghai Municipality (STCSM). Jia Li reports financial support was provided by Guangzhou Municipal Science and Technology Bureau. Jia Li reports financial support was provided by European Union’s Horizon 2020 Research and Innovation program. If there are other authors, they declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

CRediT authorship contribution statement

Zihan Chen: Conceptualization, Methodology, Project administration, Software, Supervision, Visualization, Writing – original draft, Writing – review & editing. **Yiyu Liu:** Writing – review & editing. **Eryu Wang:** Project administration, Writing – review & editing. **Huajie You:** Writing – review & editing. **Qi Gao:** Writing – review & editing. **Fan David Yeung:** Writing – review & editing. **Jia Li:** Conceptualization, Funding acquisition, Supervision.

Acknowledgments

The authors are deeply grateful to funding received from Theme-based Research Scheme (TRS) funded via Research Grants Council (University Grants Committee, HK SAR), and the grant agreement number is T32–615_24/R.

The authors are deeply grateful to funding received from 2024 Annual Special Topic Project on Basic and Applied Basic Research “Carbon Capture Research Program: Innovative Pathways to Achieving Carbon Neutrality”, Guangzhou Science and Technology Bureau (no. SL2023A04J01789).

The authors are deeply grateful to the Science and Technology Commission of Shanghai Municipality (STCSM) for the financial support (no. 21DZ1206200).

The authors further thank the support from the Consensus project, which received funding from the European Union’s Horizon 2020 Research and Innovation program under grant agreement no. 101022484.

References

Alzubi, J.A., 2021. Blockchain-based Lamport Merkle Digital Signature: authentication tool in IoT healthcare. Comput. Commun. 170, 200–208. doi:10.1016/j.comcom.2021.02.002.

Atzori, L., Iera, A., Morabito, G., 2010. The Internet of Things: a survey. Comput. Netw. 54, 2787–2805. doi:10.1016/j.comnet.2010.05.010.

Bisotti, F., Hoff, K.A., Mathisen, A., Hovland, J., 2024. Direct Air capture (DAC) deployment: a review of the industrial deployment. Chem. Eng. Sci. 283, 119416. doi:10.1016/j.ces.2023.119416.

Bongaarts, J., 2019. Intergovernmental panel on climate changespecial report on global warming of 1.5°CSwitzerland: IPCC, 2018. Popul. Dev. Rev. 45.

Boole, G., 1847. The Mathematical Analysis of Logic. CreateSpace Independent Publishing Platform.

Bralić, V., Stančić, H., Stengård, M., 2020. A blockchain approach to digital archiving: digital signature certification chain preservation. Rec. Manage. J. 30, 345–362. doi:10.1108/RMJ-08-2019-0043.

Bui, M., Adjiman, C.S., Bardow, A., Anthony, E.J., Boston, A., Brown, S., Fennell, P.S., Fuss, S., Galindo, A., Hackett, L.A., Hallett, J.P., Herzog, H.J., Jackson, G., Kemper, J., Krevor, S., Maitland, G.C., Matuszewski, M., Metcalfe, I.S., Petit, C., Puxty, G., Reimer, J., Reiner, D.M., Rubin, E.S., Scott, S.A., Shah, N., Smit, B., Trusler, J.P.M., Webley, P., Wilcox, J., Mac Dowell, N., 2018. Carbon capture and storage (CCS): the way forward. Energy Environ. Sci. 11, 1062–1176. doi:10.1039/C7EE02342A.

Cachin, C., 2016. Architecture of the hyperledger blockchain fabric. Presented At the Workshop on Distributed Cryptocurrencies and Consensus Ledgers, Chicago, IL, pp. 1–4.

Calvin, K., Dasgupta, D., Krinner, G., Mukherji, A., Thorne, P.W., Trisos, C., Romero, J., Aldunce, P., Barrett, K., Blanco, G., Cheung, W.W.L., Connors, S., Denton, F., Diongue-Niang, A., Dodman, D., Garschagen, M., Geden, O., Hayward, B., Jones, C., Jotzo, F., Krug, T., Lasco, R., Lee, Y.-Y., Masson-Delmotte, V., Meinshausen, M., Mintenbeck, K., Mokssit, A., Otto, F.E.L., Pathak, M., Pirani, A., Poloczanska, E., Pörtner, H.-O., Revi, A., Roberts, D.C., Roy, J., Ruane, A.C., Skea, J., Shukla, P.R., Slade, R., Slangen, A., Sokona, Y., Sörensson, A.A., Tignor, M., Van Vuuren, D., Wei, Y.-M., Winkler, H., Zhai, P., Zommers, Z., Hourcade, J.-C., Johnson, F.X., Pachauri, S., Simpson, N.P., Singh, C., Thomas, A., Totin, E., Arias, P., Bustamante, M., Elgizouli, I., Flato, G., Howden, M., Méndez-Vallejo, C., Pereira, J.J., Pichs-Madruga, R., Rose, S.K., Saheb, Y., Sánchez Rodríguez, R., Ürge-Vorsatz, D., Xiao, C., Yassaa, N., Alegría, A., Armour, K., Bednar-Friedl, B., Blok, K., Cissé, G., Dentener, F., Eriksen, S., Fischer, E., Garner, G., Guivarch, C., Haasnoot, M., Hansen, G., Hauser, M., Hawkins, E., Hermans, T., Kopp, R., Leprince-Ringuet, N., Lewis, J., Ley, D., Ludden, C., Niamir, L., Nicholls, Z., Some, S., Szopa, S., Trewin, B., Van Der Wijst, K.-I., Winter, G., Witting, M., Birt, A., Ha, M., Romero, J., Kim, J., Haites, E.F., Jung, Y., Stavins, R., Birt, A., Ha, M., Orendain, D.J.A., Ignon, L., Park, S., Park, Y., Reisinger, A., Cammaramo, D., Fischlin, A., Fuglestvedt, J.S., Hansen, G., Ludden, C., Masson-Delmotte, V., Matthews, J.B.R., Mintenbeck, K., Pirani, A., Poloczanska, E., Leprince-Ringuet, N., Péan, C., 2023. IPCC, 2023: Climate Change 2023: Synthesis Report. Contribution of Working Groups I, II and III to the Sixth Assessment Report of the Intergovernmental Panel On Climate Change [Core Writing Team, H. Lee and J. Romero (eds.)]. IPCC, Geneva, Switzerland. Intergovernmental Panel on Climate Change (IPCC). https://doi.org/10.59327/IPCC/AR6-9789291691647

Chen, Z., 2023. Enhancing the engineering supervision process in China: a solution enabled by integrating hybrid blockchain system. Innov. Green Dev. 2, 100091. https://doi.org/10.1016/j.igd.2023.100091

Coron, J.-S., Dodis, Y., Malinaud, C., Puniya, P., 2005. Merkle-Damgård Revisited: how to Construct a Hash Function, in: Shoup, V. (Ed.), Advances in Cryptology – CRYPTO 2005, Lecture Notes in Computer Science. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 430–448. https://doi.org/10.1007/11535218_26

Cox, E., Spence, E., Pidgeon, N., 2020. Public perceptions of carbon dioxide removal in the United States and the United Kingdom. Nat. Clim. Change 10, 744–749. doi:10.1038/s41558-020-0823-z.

Deutz, S., Bardow, A., 2021. Life-cycle assessment of an industrial direct air capture process based on temperature–vacuum swing adsorption. Nat. Energy 6, 203–213. doi:10.1038/s41560-020-00771-9.

Dib, O., Brousmiche, K.-L., Durand, A., Thea, E., Hamida, E.B., 2018. Consortium blockchains: overview, applications and challenges. Int. J. Adv. Telecommun. 11, 51–64.

Drescher, D., 2017. Blockchain basics: a Non-Technical Introduction in 25 Steps. Apress, Berkeley, California?

Du, M., Chen, Q., Chen, J., Ma, X., 2021. An optimized consortium blockchain for medical information sharing. IEEE Trans. Eng. Manage. 68, 1677–1689. doi:10.1109/TEM.2020.2966832.

Erans, M., Sanz-Pérez, S., P. Hanak, E., Clulow, D., M. Reiner, Z., A. Mutch, D., G, 2022. Direct air capture: process technology, techno-economic and socio-political challenges. Energy Environ. Sci. 15, 1360–1405. doi:10.1039/D1EE03523A.

Fang, W., Chen, W., Zhang, W., Pei, J., Gao, W., Wang, G., 2020. Digital signature scheme for information non-repudiation in blockchain: a state of the art review. EURASIP J. Wirel. Commun. Netw. 56, 2020. doi:10.1186/s13638-020-01665-w.

Gazis, V., 2017. A survey of standards for machine-to-machine and the Internet of Things. IEEE Commun. Surv. Tutor. 19, 482–511. doi:10.1109/COMST.2016.2592948.

Gillis, A.S., 2021. What is internet of things (IoT). IoT Agenda 17, 2024.

He, B., Yuan, X., Qian, S., Li, B., 2023. Carbon neutrality: a review. J. Comput. Inf. Sci. Eng. 23. doi:10.1115/1.4062545.

He, Z., Wang, Y., Miao, Y., Wang, H., Zhu, X., Li, J., 2022. Mixed polyamines promotes CO2 adsorption from air. J. Environ. Chem. Eng. 10, 107239. doi:10.1016/j.jece.2022.107239.

Helliar, C.V., Crawford, L., Rocca, L., Teodori, C., Veneziani, M., 2020. Permissionless and permissioned blockchain diffusion. Int. J. Inf. Manage. 54, 102136. doi:10.1016/j.ijinfomgt.2020.102136.

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

Huo, R., Zeng, S., Wang, Z., Shang, J., Chen, W., Huang, T., Wang, S., Yu, F.R., Liu, Y., 2022. A comprehensive survey on blockchain in industrial internet of things: motivations, research progresses, and future challenges. IEEE Commun. Surv. Tutor. 24, 88–122. doi:10.1109/COMST.2022.3141490.

International Energy Agency, 2022. Direct Air Capture: A Key Technology for Net Zero. OECD Publishing.

Johnson, D., Menezes, A., Vanstone, S., 2001. The Elliptic Curve Digital Signature Algorithm (ECDSA). Int. J. Inf. Secur. 1, 36–63. doi:10.1007/s102070100002.

Kim, S.-K., Huh, J.-H., 2020. Blockchain of carbon trading for UN sustainable development goals. Sustainability 12, 4021. doi:10.3390/su12104021.

Küng, L., Aeschlimann, S., Charalambous, C., McIlwaine, F., Young, J., Shannon, N., Strassel, K., Maesano, C.N., Kahsar, R., Pike, D., Van Der Spek, M., Garcia, S., 2023. A roadmap for achieving scalable, safe, and low-cost direct air carbon capture and storage. Energy Environ. Sci. 16, 4280–4304. doi:10.1039/D3EE01008B.

Lai, X., Lu, M., Qin, L., Han, J., Fang, X., 2010. Asymmetric encryption and signature method with DNA technology. Sci. China Inf. Sci. 53, 506–514. doi:10.1007/s11432-010-0063-3.

Levin, K., 2018. 8 Things You Need to Know About the IPCC 1.5°C Report | World Resources Institute [WWW Document]. WORLD Resour. Inst. https://web.archive.org/web/20231106134736/https://www.wri.org/insights/8-things-you-need-know-about-ipcc-15c-report (accessed 6.30.24).

Li, Z., Kang, J., Yu, R., Ye, D., Deng, Q., Zhang, Y., 2017. Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things. IEEE Trans. Ind. Inform. 1–1. https://doi.org/10.1109/TII.2017.2786307

Liu, S.-G., Chen, W.-Q., Liu, J.-L., 2021. An efficient double parameter elliptic curve digital signature algorithm for blockchain. IEEE Access 9, 77058–77066. doi:10.1109/ACCESS.2021.3082704.

Lu, Y., 2019. The blockchain: state-of-the-art and research challenges. J. Ind. Inf. Integr. 15, 80–90. doi:10.1016/j.jii.2019.04.002.

Lux, B., Schneck, N., Pfluger, B., Männer, W., Sensfuß, F., 2023. Potentials of direct air capture and storage in a greenhouse gas-neutral European energy system. Energy Strategy Rev 45, 101012. doi:10.1016/j.esr.2022.101012.

Madhu, K., Pauliuk, S., Dhathri, S., Creutzig, F., 2021. Understanding environmental trade-offs and resource demand of direct air capture technologies through comparative life-cycle assessment. Nat. Energy 6, 1035–1044. doi:10.1038/s41560-021-00922-6.

Mahmudnia, D., Arashpour, M., Yang, R., 2022. Blockchain in construction management: applications, advantages and limitations. Autom. Constr. 140, 104379. doi:10.1016/j.autcon.2022.104379.

Masson-Delmotte, V.P., Zhai, P., Pirani, S.L., Connors, C., Péan, S., Berger, N., Caud, Y., Chen, L., Goldfarb, M.I., Scheel Monteiro, P.M., 2021. IPCC, 2021: summary for policymakers. In: Climate Change 2021: The Physical Science Basis. Contribution of Working Group I to the Sixth Assessment Report of the Intergovernmental Panel On Climate Change (Report). Cambridge University Press, Cambridge, United Kingdom and New York, NY, USA.

Meckling, J., Biber, E., 2021. A policy roadmap for negative emissions using direct air capture. Nat. Commun. 12, 2051. doi:10.1038/s41467-021-22347-1.

Medvidovic, N., Rosenblum, D.S., Redmiles, D.F., Robbins, J.E., 2002. Modeling software architectures in the unified modeling language. ACM Trans. Softw. Eng. Methodol. 11, 2–57. doi:10.1145/504087.504088.

Meng, T., Zhao, Y., Wolter, K., Xu, C.-Z., 2021. On consortium blockchain consistency: a queueing network model approach. IEEE Trans. Parallel Distrib. Syst. 32, 1369–1382. doi:10.1109/TPDS.2021.3049915.

Miao, Y., He, Z., Zhu, X., Izikowitz, D., Li, J., 2021. Operating temperatures affect direct air capture of CO2 in polyamine-loaded mesoporous silica. Chem. Eng. J. 426, 131875. doi:10.1016/j.cej.2021.131875.

Miao, Y., Wang, Y., Zhu, X., Chen, W., He, Z., Yu, L., Li, J., 2022. Minimizing the effect of oxygen on supported polyamine for direct air capture. Sep. Purif. Technol. 298, 121583. doi:10.1016/j.seppur.2022.121583.

Mukherji, A., Thorne, P., Cheung, W., Connors, S., Garschagen, M., Geden, O., Hayward, B., Simpson, N., Totin, E., Blok, K., 2023. AR6 synthesis report: Climate change 2023.

Nakamoto, S., 2008. Bitcoin: a peer-to-peer electronic cash system.

Nist, C., 1992. The digital signature standard. Commun. ACM 35, 36–40.

Pilkington, M., 2016. Chapter 11: Blockchain technology: Principles and Applications.

Qiu, Y., Lamers, P., Daioglou, V., McQueen, N., de Boer, H.-S., Harmsen, M., Wilcox, J., Bardow, A., Suh, S., 2022. Environmental trade-offs of direct air capture technologies in climate change mitigation toward 2100. Nat. Commun. 13, 3635. doi:10.1038/s41467-022-31146-1.

Saari, A., Vimpari, J., Junnila, S., 2022. Blockchain in real estate: recent developments and empirical applications. Land Use Policy 121, 106334. doi:10.1016/j.landusepol.2022.106334.

Sadawi, A.A., Madani, B., Saboor, S., Ndiaye, M., Abu-Lebdeh, G., 2021. A comprehensive hierarchical blockchain system for carbon emission trading utilizing blockchain of things and smart contract. Technol. Forecast. Soc. Change 173, 121124. doi:10.1016/j.techfore.2021.121124.

Scott-Buechler, C., Cain, B., Osman, K., Ardoin, N.M., Fraser, C., Adcox, G., Polk, E., Jackson, R.B., 2024. Communities conditionally support deployment of direct air capture for carbon dioxide removal in the United States. Commun. Earth Environ. 5, 1–13. doi:10.1038/s43247-024-01334-6.

Simmons, G.J., 1979. Symmetric and asymmetric encryption. ACM Comput. Surv. 11, 305–330. doi:10.1145/356789.356793.

Snytnikov, P., Potemkin, D., 2022. Flare gas monetization and greener hydrogen production via combination with cryptocurrency mining and carbon dioxide capture. iScience 25. https://doi.org/10.1016/j.isci.2022.103769

Tönnissen, S., Teuteberg, F., 2020. Analysing the impact of blockchain-technology for operations and supply chain management: an explanatory model drawn from multiple case studies. Int. J. Inf. Manage. 52, 101953. doi:10.1016/j.ijinfomgt.2019.05.009.

Valentine, J., Zoelle, A., Homsy, S., Mantripragada, H., Kilstofte, A., Sturdivan, M., Steutermann, M., Fout, T., 2022. Direct air capture case studies: solvent system (No. DOE/NETL-2021/2864, 1893369). https://doi.org/10.2172/1893369

Van Cutsem, O., Ho Dac, D., Boudou, P., Kayal, M., 2020. Cooperative energy management of a community of smart-buildings: a Blockchain approach. Int. J. Electr. Power Energy Syst. 117, 105643. doi:10.1016/j.ijepes.2019.105643.

Vigna, P., Casey, M.J., 2016. The Age of cryptocurrency: How Bitcoin and the Blockchain Are Challenging the Global Economic Order. Macmillan.

Wang, E., Navik, R., Miao, Y., Gao, Q., Izikowitz, D., Chen, L., Li, J., 2024. Reviewing direct air capture startups and emerging technologies. Cell Rep. Phys. Sci. 5, 101791. doi:10.1016/j.xcrp.2024.101791.

Wang, T., Wang, X., Hou, C., Liu, J., 2020. Quaternary functionalized mesoporous adsorbents for ultra-high kinetics of CO2 capture from air. Sci. Rep. 10, 21429. doi:10.1038/s41598-020-77477-1.

Wang, W., Xu, H., Alazab, M., Gadekallu, T.R., Han, Z., Su, C., 2022. Blockchain-Based reliable and efficient certificateless signature for IIoT devices. IEEE Trans. Ind. Inform. 18, 7059–7067. doi:10.1109/TII.2021.3084753.

Wang, Y., Miao, Y., Ge, B., He, Z., Zhu, X., Liu, S., Li, J., Yu, L., 2023. Additives enhancing supported amines performance in CO_2 capture from air. SusMat 3, 416–430. doi:10.1002/sus2.141.

Wood, G., 2014. Ethereum: a secure decentralised generalised transaction ledger. Ethereum Proj. Yellow Pap. 151, 1–32.

Wu, J., Chen, Y., Xu, Y., Chen, S., Lv, H., Gan, Z., Zhu, X., Wang, R., Wang, C.-H., Ge, T., 2024. Facile synthesis of structured adsorbent with enhanced hydrophobicity and low energy consumption for CO2 capture from the air. Matter 7, 123–139. doi:10.1016/j.matt.2023.10.019.

Xu, Y., Tao, X., Das, M., Kwok, H.H.L., Liu, H., Kuan, K.K.L., Lau, A.K.H., Cheng, J.C.P., 2024. A blockchain-based framework for carbon management towards construction material and product certification. Adv. Eng. Inform. 61, 102242. doi:10.1016/j.aei.2023.102242.

Yang, R., Wakefield, R., Lyu, S., Jayasuriya, S., Han, F., Yi, X., Yang, X., Amarasinghe, G., Chen, S., 2020. Public and private blockchain in construction business process and information integration. Autom. Constr. 118, 103276. doi:10.1016/j.autcon.2020.103276.

Yeung, K., 2021. The health care sector's experience of blockchain: a cross-disciplinary investigation of its real transformative potential. J. Med. Internet Res. 23, e24109. doi:10.2196/24109.

Zhai, S., Yang, Y., Li, J., Qiu, C., Zhao, J., 2019. Research on the application of cryptography on the blockchain. J. Phys. Conf. Ser. 1168, 032077. doi:10.1088/1742-6596/1168/3/032077.

Zhang, H., Wang, J., Ding, Y., 2019. Blockchain-based decentralized and secure keyless signature scheme for smart grid. Energy 180, 955–967. doi:10.1016/j.energy.2019.05.127.

Zhu, S., Cai, Z., Hu, H., Li, Y., Li, W., 2020. zkCrowd: a hybrid blockchain-based crowdsourcing platform. IEEE Trans. Ind. Inform. 16, 4196–4205. doi:10.1109/TII.2019.2941735.