

Exploring the Potential of Smart Contracts and Blockchain: Revolutionizing Trust and Transparency

YOUSSEF BENCHAI¹, LUCREZIA MAGGI¹, AND DAVIDE PRANDO¹

¹Università degli studi di Milano-Bicocca, CdLM Data Science

Abstract

This work explores the concept of smart contracts and their application in blockchain technology. It provides an introduction to smart contracts and their potential to revolutionize various industries while highlighting the current applications of smart contracts in several areas, and explains the working principle of smart contracts in a blockchain, emphasizing their self-executing nature and transparency. The role of oracles in expanding the capabilities of smart contracts is also discussed in detail with examples of the most used decentralized oracle networks.

Keywords: Smart Contracts, Blockchain, Ethereum, Digital Economy, Decentralized

1. INTRODUCTION

In the realm of technological advancements, few innovations have captured the imagination and potential for disruption quite like smart contracts (SC) and blockchain technology. With the rise of cryptocurrencies like Bitcoin, Ethereum, and others, the world has witnessed the emergence of a decentralized, transparent, and secure system that has the power to revolutionize various industries. This work delves into the intricacies of smart contracts and blockchain, exploring their underlying principles, their impact on trust and transparency, and their potential to reshape traditional systems. The concept of smart contracts can be traced back to the early 1990s when legal scholar and computer scientist Nick Szabo first introduced the idea. Smart contracts are essentially **self-executing agreements** that run on a blockchain. These agreements, written in code, automatically enforce and execute the terms and conditions defined within them. By eliminating the need for intermediaries, smart contracts provide a more efficient, secure, and cost-effective way of conducting transactions.

Blockchain technology, on the other hand, forms the foundation upon which smart contracts operate. A blockchain is a decentralized and immutable digital ledger

that records transactions across a network of computers. Each transaction, or block, is linked to the previous one, creating a chain of blocks that forms a **complete and transparent history** of all interactions. This distributed nature of blockchain ensures that no single entity has control or authority over the entire network, enhancing security and reducing the risk of fraudulent tampering.

One of the key benefits of smart contracts and blockchain lies in their potential to **revolutionize trust**. Traditional systems often rely on intermediaries, such as banks, lawyers, or government institutions, to establish trust between parties involved in a transaction. However, these intermediaries can introduce delays, costs, and inefficiencies. Smart contracts, powered by blockchain technology, eliminate the need for intermediaries, providing a trustless environment where the execution of agreements is automated, transparent, and tamper-proof. Furthermore, the transparent nature of blockchain technology ensures that all participants have access to the same information, creating a heightened level of transparency. Every transaction and modification to the blockchain is recorded and visible to all participants, enabling anyone to audit and verify the accuracy and integrity of the data. This transparency creates a sense of accountability and can significantly reduce fraud, corruption, and other unethical

practices.

2. WORKING PRINCIPLE

As mentioned, smart contract operates as a self-executing, digital agreement deployed on a blockchain. Conceptually, a blockchain can be visualized as a sequential chain of blocks, each containing transactional information. A smart contract, encoded in a programmatic language, is stored within a block on the blockchain, encompassing the stipulated terms and conditions like a traditional contract. The distinctive aspect emerges when the smart contract interacts with the blockchain. By design, the smart contract autonomously enforces the contractual obligations when predefined conditions are met. This is accomplished through the execution of the code embedded within the smart contract.

For instance, consider the case of a real estate transaction governed by a smart contract. The smart contract's code incorporates essential details such as buyer and seller identities, agreed-upon price, and transactional prerequisites. Upon deployment on the blockchain, the smart contract awaits the fulfillment of specified conditions. In this scenario, once the buyer transfers the designated funds and the seller validates the transfer of property ownership, the smart contract automatically triggers the execution of the transaction. Consequently, intermediaries such as legal professionals or financial institutions are circumvented as the smart contract ensures compliance with the agreed-upon terms, expediting and facilitating the transaction process.

The inherent advantages of employing smart contracts on a blockchain lie in the transparency and security they afford. The decentralized and distributed nature of the blockchain network enables all participants to access identical information, enabling verification of transactions and smart contract execution. Furthermore, the **immutability** of the blockchain ensures that once a transaction is recorded, it becomes impervious to modification or tampering, engendering enhanced security and mitigating the potential for fraudulent activities.

A. Oracles

Up to now, all the description provided can be applied if and only if the software embedded in a smart contract can verify by itself the fulfillment of the encoded condition. This may restrict the application to value transaction that operates only on a blockchain. To expand the possible usage scenario, oracles have been introduced as they act as bridges between the blockchain, which operates in a decentralized manner, and external data sources or systems that exist outside the blockchain. The primary function of an oracle is to provide smart contracts with access to off-chain information, such as real-time data, events, or the outcome of specific conditions that cannot be directly determined within the blockchain. This is essential because blockchains, by design, are isolated and

have limited interaction with external systems. Oracles enable smart contracts to interact with the real world and make informed decisions based on external data.

A.1. Oracles types

Oracles can be categorized into two main types: software-based oracles and hardware-based oracles. The firsts retrieve data from various sources, such as web APIs, databases, or other external systems. They collect, validate, and transmit this data to the smart contract, ensuring its accuracy and reliability. The seconds, on the other hand, involve physical devices that capture real-world data, such as temperature sensors, GPS trackers, or IoT devices. These devices securely transmit the data to the blockchain, where smart contracts can utilize it.

A.2. Vulnerability

To ensure the integrity of the data provided by oracles, several mechanisms and techniques are employed. One common approach is the use of multiple oracles to retrieve the same information **independently**. By aggregating and comparing data from multiple sources, smart contracts can verify the accuracy and consistency of the received data. Additionally, **reputation systems** and **staking mechanisms** can be implemented to incentivize oracles to provide reliable and trustworthy data. These mechanisms encourage oracles to behave honestly and penalize malicious or inaccurate data reporting.

The role of oracles extends beyond data retrieval. They can also facilitate the execution of complex operations that require off-chain computations or interactions with external systems. For instance, oracles can trigger actions in response to specific events or conditions, such as executing a payment when a certain condition is met or interacting with external APIs to access additional functionalities.

However, it is important to note that oracles introduce a **potential vulnerability** to the smart contract ecosystem. Since oracles are external entities, they can be susceptible to manipulation or compromise. Malicious or inaccurate data reported by an oracle can have detrimental effects on the smart contract's functionality and integrity. Therefore, careful consideration and implementation of security measures, such as data verification, reputation systems, and auditing, are crucial to mitigate these risks and ensure the overall reliability of the oracle system.

A.3. Decentralized oracles network

To partially overcome the described vulnerabilities, decentralized oracles networks (DON) have been developed. DON are networks of independent oracles aimed to minimize the risk of information tampering and are usually specialized in a particular field. Some popular DON are:

- **Chainlink**: a DON that provides data to smart contract, specialized in DeFi (decentralized finance) application, it also offer price, weather and sport data. [1]

- **Band Protocol:** known for its high quality data, Band protocol data sources include many government agencies, financial institutions and weather services. It also offer weather and sport data. [2]
- **Provable:** it's a DON specialized in providing data for gaming applications, including dices and fair poker games, for this reason it is also called Randomness Oracle. [3]
- **Tellor:** it uses consensus mechanism to ensure that data is as accurate and reliable as possible. It's mechanism is based on miners principle, who compete to provide the most accurate data. [4]

3. SMART CONTRACTS CURRENT APPLICATIONS

Ethereum offers greater flexibility than Bitcoin because of its ability to support decentralized applications, enabling a wider and more diverse use of blockchain technology. While Bitcoin focuses primarily on the digital currency function, Ethereum stands out for its versatility due to its ability to execute smart contracts, making it a more suitable choice for a wide range of blockchain applications. This allowed Ethereum to outperform bitcoin usage in mid-2017.

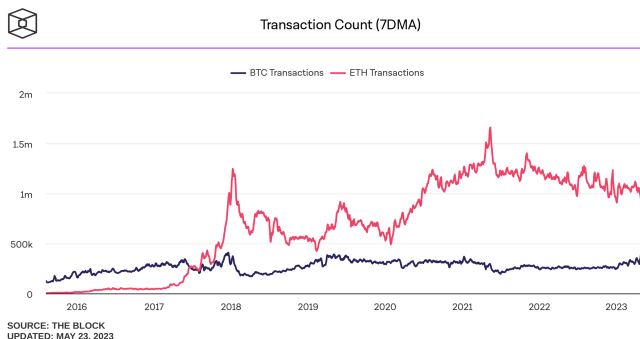


Fig. 1. Bitcoin vs Ethereum transaction count since 2016[5]

A. Finance

SCs have demonstrated their versatility and potential in a wide range of industries, revolutionizing various processes and transactions. One of the prominent applications of SCs is in the financial sector. Traditional financial agreements, such as loans, insurance policies, and derivatives, are often complex, time-consuming, and involve multiple intermediaries. SCs streamline these processes by automating the execution of agreements, reducing paperwork, and eliminating the need for intermediaries. This allows for faster settlement times, lower costs, and increased transparency. Additionally, they enable the creation of decentralized finance (DeFi) platforms, where users can engage in peer-to-peer lending, decentralized

exchanges, and other financial services without relying on centralized authorities.

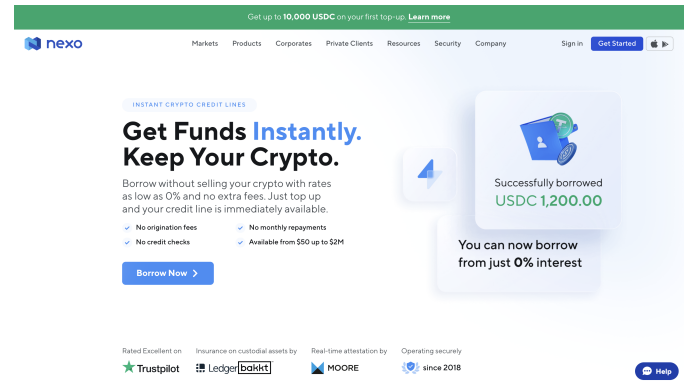


Fig. 2. Nexo, lending institution in the digital finance industry[6]

B. Supply chain

Supply chain management is another area where smart contracts have found significant application. The complex nature of global supply chains often leads to inefficiencies, lack of **transparency**, and difficulties in tracing products. Smart contracts embedded in a blockchain enable end-to-end visibility and transparency, allowing stakeholders to track and verify each step of the supply chain journey. This ensures authenticity, reduces fraud, and enhances product traceability. With SCs, supply chain participants can automate tasks such as payments, quality assurance, and compliance, leading to streamlined operations and improved trust among stakeholders.

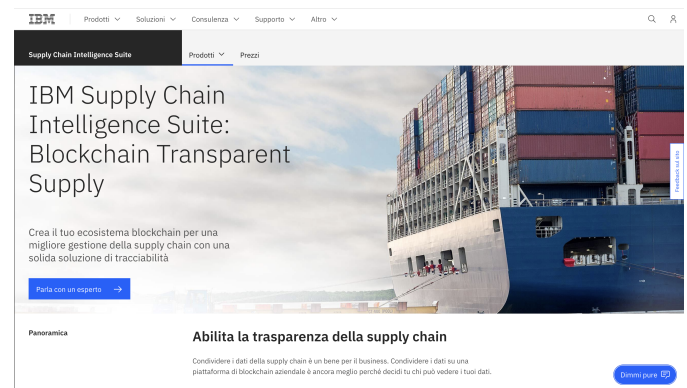


Fig. 3. IBM Food Trust, food supply chain management. Enables food producers, distributors, and retailers to track the movement of food products across the supply chain, ensuring transparency and traceability[7]

C. Healthcare

Smart contracts also have the potential to transform the healthcare industry. Medical records, insurance claims, and clinical trials are often plagued by issues of **data integrity**, privacy, and **interoperability**. By leveraging blockchain technology and smart contracts, healthcare

providers can securely store and share patient data, ensuring privacy and control while enabling seamless data exchange between different entities. Smart contracts can automate insurance claim processing, reducing administrative overhead and enabling faster reimbursement. Furthermore, they can facilitate the execution of clinical trial agreements, ensuring compliance, transparency, and immutable record-keeping.

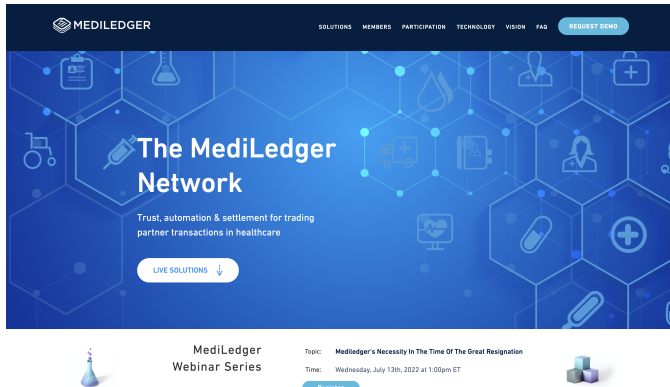


Fig. 4. MediLedger, enables companies across the prescription drug supply chain to verify the authenticity of medicines, as well as expiry dates and other important information[8]

D. Copyright

In the realm of intellectual property rights, SCs offer a novel approach to managing copyrights, patents, and licensing agreements. By storing these rights on a blockchain, SCs enable automated royalty payments, ensuring that creators are fairly compensated for their work. They also provide a verifiable and tamper-proof record of ownership and usage rights, reducing disputes and simplifying licensing processes. They can also facilitate decentralized marketplaces for digital content, where creators can directly sell their work to consumers without intermediaries.

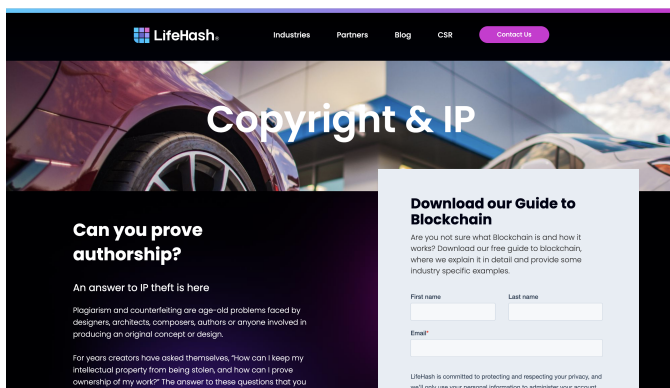


Fig. 5. LifeHash, simplifies the complexities of the copyright process by proving your digital ownership[9]

E. Real estate

As previously mentioned, real estate is yet another sector that stands to benefit from SCs. Property transactions often involve complex legal processes, multiple intermediaries, and high costs. SCs can automate tasks such as property transfers, escrow services, and rental agreements, reducing the need for intermediaries and minimizing the risk of fraud. They can also enable fractional ownership and real estate crowdfunding, allowing investors to participate in real estate ventures with reduced barriers to entry.

These are just a few examples highlighting the current applications of smart contracts. As the technology continues to advance and evolve, the potential for innovation and disruption across various industries is vast. From finance to supply chain management, healthcare to intellectual property, and beyond, smart contracts are reshaping traditional processes, increasing efficiency, transparency, and trust in our digital world.

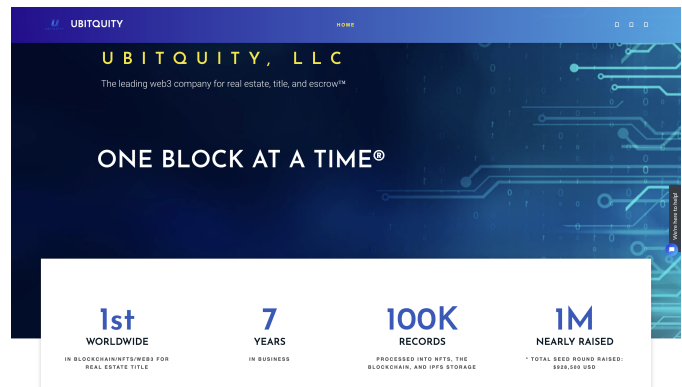


Fig. 6. Ubitquity, a company offering a simple user experience for securely recording and tracking property deeds[10]

4. MOST USED PLATFORMS

Here, the most used platforms and technologies for smart contract stipulation are reported with a focus on differences between platforms:

- **Ethereum:** Ethereum is the **leading platform** for smart contracts and decentralized applications (DApps). It introduced the concept of smart contracts and remains the most utilized blockchain platform for developing and deploying them. Ethereum's **native programming language, Solidity**, is widely adopted by developers, and its extensive ecosystem supports a wide range of applications.



Fig. 7. Logo of Ethereum

- **Binance Smart Chain (BSC):** BSC is a blockchain platform developed by the cryptocurrency exchange Binance. It offers compatibility with the Ethereum Virtual Machine (EVM), making it easy for Ethereum developers to migrate or deploy their smart contracts on BSC. BSC has gained popularity due to its **lower transaction fees** and faster block confirmation times compared to Ethereum.



Fig. 8. Logo of Binance Smart Chain

- **Solana:** Solana is a high-performance blockchain platform designed for decentralized applications and smart contracts. It leverages a unique consensus mechanism known as **Proof of History (PoH)** to achieve fast transaction processing and high throughput. Solana's scalability and low transaction fees have attracted developers looking to build complex applications that require high performance.



Fig. 9. Logo of Solana

- **Avalanche:** it aims to provide a highly scalable and interoperable ecosystem for smart contracts and DApps (decentralized applications). It utilizes a consensus protocol called **Avalanche consensus**, which enables high transaction throughput and fast finality. Avalanche supports the deployment of smart contracts using the Ethereum Virtual Machine (EVM), making it **compatible** with existing Ethereum tools and applications.
- **Cardano:** Cardano is a blockchain platform that aims to provide a secure and scalable infrastructure for smart contracts and DApps. It utilizes a unique **proof-of-stake consensus** algorithm called **Ouroboros** and employs a layered architecture, making it highly flexible and modular. Cardano has gained attention for its focus on peer-reviewed research and formal verification of smart contracts.

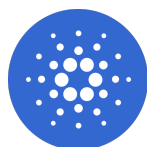


Fig. 10. Logo of Cardano

5. CONCLUSIONS

In conclusion, smart contracts have emerged as a transformative technology, revolutionizing various industries by automating agreements, enhancing transparency, and reducing reliance on intermediaries. Platforms such as Ethereum, Binance Smart Chain, Solana, Avalanche and Cardano have provided fertile grounds for the development and deployment of smart contracts, each offering unique features and capabilities. However, the future of smart contracts holds even greater potential. As blockchain technology continues to evolve, we can expect **advancements in scalability, interoperability, and security**, addressing current limitations and expanding the scope of smart contract applications. Furthermore, emerging platforms and protocols are continuously pushing the boundaries, introducing innovative solutions and refining existing frameworks. We can anticipate increased adoption of smart contracts in sectors such as finance, supply chain management, healthcare, and more. As **regulatory frameworks** become clearer and mainstream acceptance grows, smart contracts are poised to play a pivotal role in shaping the future of digital transactions, governance, and decentralized systems. With ongoing research, development, and collaborative efforts, the future development of smart contracts holds immense promise for a more efficient, transparent, and trustworthy digital economy.

REFERENCES

1. <https://chain.link>
2. <https://www.bandprotocol.com>
3. <https://defiprime.com/provable>
4. <https://tellor.io>
5. <https://www.theblock.co>
6. <https://nexo.com/borrow>
7. <https://www.ibm.com/it-it/products/supply-chain-intelligence-suite/food-trust>
8. <https://www.medilegger.com>
9. <https://www.lifehash.com/>
10. <https://ubitquity.io>