Advanced Database Systems

Orfeas Gkonis MSc in Data Science
International Hellenic University
Thessaloniki,Greece
Email:ogkonis@ihu.edu.gr

Vasilis Kalfopoulos MSc in Data Science
International Hellenic University
Thessaloniki,Greece
Email:vkalfopoulos@ihu.edu.gr

Evaggelos Ziliaxovinos MSc in Data Science
International Hellenic University
Thessaloniki,Greece
Email:eziliachovinos@ihu.edu.gr

Antonis Koutsoupias MSc in Data Science
International Hellenic University
Thessaloniki,Greece
Email:akoutsoupias@ihu.edu.gr

January 2025

1 Abstract

Blockchain technology has revolutionized many industries such as data management ,storage and security by providing a decentralized way,leveraging a distributed ledger technology, of managing data ,ensuring transparency and efficiently handling data transactions.This has created a fertile soil for the next-generation of decentralized applications to emerge, the smart contracts.The smart contracts,are computer protocols designed to facilitate,verify,and enforce automatically the negotiation and agreement among multiple untrustworthy parties.Despite the positive aspects of smart contracts, several concerns continuously undermine their adoption such as security threats,vulnerabilities,and legal issues.In this report we will explore potential solutions and developments to make blockchain more efficient and widely usable in decentralized databases and furthermore,we will identify the applied

markets of smart contracts,explaining their bright side and their negatives.

2 Introduction to blockchain

Blockchain was first proposed in 2008 and implemented in 2009 by Satoshi Nakamoto[21], it is seen by many as a distributive technology[23] that has ultimately changed various industries such as the financial, healthcare and logistical industries and has enabled a new way of thinking across many industries. Although blockchain offers many advantages such as decentralization, immutability, transparency, and security, there are also some serious issues with its usage such as:

- **High Energy Consumption**. First and foremost, the compute resources to run a blockchain like Bitcoin expends large amounts of electricity. All the energy is used by the miners in order to solve cryptographic puzzles to validate blocks. The amount of energy consumed increases with the level of difficulty increase that is related to more hashing power from compute resources. The more nodes you have mining, the greater the computational effort required to validate a block of transactions. This requires plenty of energy consumed [13]

- **Scalability**.One of the major issues of blockchain is scalability,many thousands of transactions have occurred every day in recent years. In Ethereum, the limited block size cannot accommodate all the transactions submitted by the miners. It is therefore challenging for the miners to verify every transaction. The consequence is that the miners tend to select transactions with more rewards for the sake of securing more rewards. The transactions with fewer rewards are left in the queue, leading to longer transaction latency[30]. It is estimated that more than 10 k transactions are waiting to be verified.[15]

- **Security**.In a Statistical report of the International Data Corporation,it has been identified that the challenge of security to be the most critical[28].The fundamental concepts behind blockchain technology are quite powerful, offering compelling features to secure applications, networks, and devices. However, the current cryptographic functions, due to limited resources, are hard to implement. Elliptic curve cryptography and RSA based public key encryption have a large footprint and are deemed as not suitable for Blockchain[2].Hence,it is required to use solutions and approaches that go beyond the traditional techniques that are used.[28]

- **Blockchain's image problem**.Blockchain is heavily linked with cryptocurrencies such as Bitcoin, in the mind of many.Especially crypto has a negative image that is surrounded by fraudsters, hackers that are using

he technology for criminal activities.This has a result of people thinking twice before adopting a blockchain technology system.Before making blockchain widely usable, people should understand the difference between bitcoin,other cryptocurrencies and blockchain.Cryptocurrencies occupy only a small proportion of the blockchain technology.[7]

3 Exploring Solutions

3.1 High Energy Consumption

To overcome this issue,more efficient algorithms are in development by some blockchain supporters, that are less energy taxing. So-called proof-of-stake (PoS) protocols were introduced, that involve a combination of a participant's stake in the network and an algorithm to randomly assign the task of validation to a node. Given that the participants are not required to solve complex puzzles, these mechanisms significantly reduce energy consumption.Furthermore, from a business perspective, private blockchains are more suitable to serve company interests, as they provide restricted access, an additional layer of privacy to protect trade secrets, and are more energy-efficient.[7]

3.2 Scalability

Currently the solution to micropayments and scalability is to offload the transactions to a custodian, whereby one is trusting third party custodians to hold ones coins and to update balances with other parties. Trusting third parties to hold all of ones funds creates counterparty risk and transaction costs.Instead, using a network of these micropayment channels, Bitcoin can scale to billions of transactions per day with the computational power available on a modern desktop computer today. Sending many payments inside a given micropayment channel enables one to send large amounts of funds to another party in a decentralized manner. These channels are not a separate trusted network on top of bitcoin. They are real bitcoin transactions. Micropayment channels create a relationship between two parties to perpetually update balances, deferring what is broadcast to the blockchain in a single transaction netting out the total balance between those two parties. This permits the nancial relationships between two parties to be trustlessly deferred to a later date, without risk of counterparty default.Micropayment channels use real bitcoin transactions, only electing to defer the broadcast to the blockchain in such a way that both parties can guarantee their current balance on the blockchain; this is not a trusted overlay network payments in micropayment channels are real bitcoin communicated and exchanged o-chain.[24]

3.3 Security

One possible solution to the security problem are the Smart Contracts.Smart contracts are digital contracts stored on a blockchain that are automatically

executed when predetermined terms and conditions are met. The concept is not new; it dates back to the 1990s, when Nick Szabo[5], a computer scientist, introduced it. Szabo envisioned a world where contracts would function like vending machines — reliable, tamper-proof, and automatic. This innovation eliminates the need for third-party intermediaries, making transactions secure, transparent, and efficient[11][22][12].Smart contracts provide a reliable alternative to traditional paper contracts, which Szabo described as "law code." In contrast, smart contracts are "dry code", meaning they are automated, precise, and secure. Their implementation ensures verifiability, observability, privacy, and enforceability — key features for an efficient and tamper-resistant system. Szabo outlined early examples of smart contract concepts, such as POS systems, electronic data interchange (EDI) for corporations, and SWIFT for banking transactions[29]. By embedding contractual terms directly into code, smart contracts make breaches costly, minimize fraud, and streamline transactions across industries. In conclusion, Nick Szabo's vision of smart contracts has transformed modern digital agreements, laying the groundwork for today's blockchain-based systems.

4 The Smart Contracts

4.1 Thechnical Architecture of the Smart Contracts

Smart contracts are self-executing contracts with the terms of the agreement directly written into code. They run on blockchain technology, which ensures transparency, security, and immutability. Unlike traditional contracts that require intermediaries, smart contracts automate the execution of agreements, reducing the need for trust between parties.[14]

1. **Automation:**Smart contracts automatically execute actions when predefined conditions are met, eliminating manual intervention.

2. **Transparency:**All parties can see the terms and outcomes, which fosters trust.

3. **Security:**The decentralized nature of blockchain makes smart contracts resistant to tampering and fraud.

4. **Cost-Efficiency:**By removing intermediaries, smart contracts can reduce the costs associated with traditional contract enforcement.

4.2 Phases of a Smart Contract Life Cycle

1. **Create:**Contract reiteration and negotiation constitute a significant part of the first phase. First, the parties must agree on the contract's overall content and goals. This can be done online or offline. This is similar to traditional contract negotiations. On the blockchain being used to draw up the smart contract, all participants must have a wallet. Once the contents

of the smart contract have been finalized, they must be converted into code. The following tasks are performed in this phase:

- Negotiation of multiple parties.
- Smart contract's design, implementation, and validation.

2. **Freeze:**Validation of the transactions on a blockchain is done by a set of computers across the network called nodes. These nodes are the blockchain miners. A small fee must be paid to the miners in exchange for this service to prevent the ecosystem from being flooded with smart contracts. The smart contract and its participants become open to the public on the public ledger during the 'freeze' phase. Digital assets of both involved parties in the smart contracts are locked via freezing the corresponding digital wallets, and nodes operate as a governance board that verifies whether the preconditions for smart contract execution have been satisfied. The tasks that are executed in this phase are the following:

   - Smart Contracts are stored on the blockchain.
   - Freezing of digital assets of involved parties.

3. **Execute:**Participating nodes read contracts that are stored on the distributed ledger. The integrity of a smart contract is verified by the authenticating nodes, and the code is executed by the smart contract's interference engine (or by the compiler). When the inputs for the execution from one party are received in the form of coins (commitment to goods through coins), the interference engine creates a transaction triggered by the met criteria.

   Now the new transaction data is added to the blockchain and to ensure fulfillment according to the agreed-upon terms in the Smart contract the governing nodes now verify it again. 'Consensus mechanism' governs this verification process. The tasks that are done in this phase are:

   - Evaluation of smart contact condition.
   - Auto execute smart contact statement is triggered.

4. **Finalize:**After a smart contract has been executed, the new states of all involved parties are updated. Now the updated state information and resulting transactions are put in the distributed ledger of the blockchain and the consensus mechanism verifies that the assets transferred by the first party have been received and unfreezes the assets for the receiving party. The tasks that are completed in this phase are the following:

   - State updating and digital assets allocated.
   - Unfreezing of digital assets received from the first party.

   The smart contract has completed the whole life cycle. During freezing, execution, and finalization, the sequence of transactions has been executed and stored in the blockchain.[18][10]

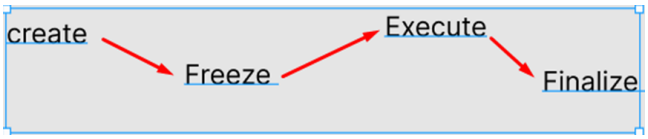

Figure 1: The Life Cycle of a Smart Contract

4.3 Advantages and Disadvantages of Smart Contracts

Nothing's perfect, not even smart contracts. But their pros far outweigh the cons. For starters, they streamline complex transactions, saving both time and money. Transparency is built in, reducing disputes, and because they're based on code, human error is minimized. They have nearly perfect security, thanks to cryptographic protections. On the flip side, smart contracts can be rigid — they don't adapt easily to unexpected situations. In addition, setting up them requires specialized coding knowledge, which can be a hurdle for some. Despite these quirks, smart contracts are invaluable tools that are transforming industries.[6][9]

4.4 Vulnerabilities in Smart Contracts

Smart contracts, once deployed on a blockchain, are immutable, meaning they cannot be altered or modified. While immutability ensures trust and transparency, it also implies that any vulnerabilities or flaws in the code can have long-lasting consequences. Even the smallest bug or oversight can lead to significant financial losses, making thorough code auditing and testing paramount. The absence of a central authority to oversee and rectify these issues calls for a proactive approach to security.[19] Additionally, due to the large quantities of money that pass through them, these programs are frequently targeted by malicious actors seeking to exploit vulnerabilities in smart contracts. Lately, smart contract security concerns have erupted. In February 2022, the Wormhole Cross Chain Bridge Attack deprived Solana and Ethereum of approximately $320 million[31]. DODO DEX was hacked in March 2022, resulting in the loss of approximately $3.8 million worth of cryptocurrency[3]. Not only do smart contract assaults result in significant fund losses, but they also have a negative impact on the credibility of the protocol. The DAO Hack, one of the most notorious events in the history of blockchain and cryptocurrencies, was a 2016 security breach that targeted The DAO, an Ethereum-based investment fund and a pioneering Decentralized Autonomous Organization.[26]

4.5 Companies Leveraging Smart Contracts

Many companies and organizations, primarily in the fields of finance, logistics, energy, and insurance, use Smart Contracts to automate processes and ensure transparency and security. Below are some of the most well-known companies and sectors where Smart Contracts have been applied:

Microsoft-Azure Blockchain. Microsoft Azure Blockchain was a blockchain-as-a-service (BaaS) platform offered by Microsoft through its Azure cloud. It allowed enterprises to develop, manage, and deploy blockchain applications and networks with minimal infrastructure overhead. Although Microsoft retired its standalone Azure Blockchain Service in September 2021, Azure continues to support blockchain solutions through integrations and related services.[20]

Siemens a global leader in industrial manufacturing and automation, is leveraging blockchain technology and smart contracts to enhance transparency, efficiency, and automation in various sectors, including energy, supply chain, mobility, and infrastructure. Smart contracts play a crucial role in Siemens' initiatives, enabling automated and secure operations in decentralized systems.[25]

Energy Sector

- **Decentralized Energy Systems:** Siemens uses smart contracts to facilitate peer-to-peer energy trading in microgrids. Consumers and producers can trade surplus energy directly, with smart contracts automating transactions based on predefined conditions.
- **Dynamic Pricing:** Automated billing systems adjust energy prices in real-time based on demand and supply conditions, ensuring fairness and efficiency.

Siemens' Blockchain Collaborations Siemens collaborates with technology providers and startups to develop blockchain-based solutions, including:

- **Energy Web Foundation (EWF):** Focused on decentralized energy applications
- **IBM and Hyperledger:** For industrial blockchain use cases.
- **Ethereum-based Platforms:** To test and deploy smart contracts for various applications.

Siemens continues to innovate with blockchain and smart contracts, demonstrating their commitment to integrating cutting-edge technology into industrial and urban environments. This approach aligns with their vision of driving digital transformation and sustainability.[25]

IBM-IBM Blockchain. BM Food Trust is a blockchain-based food safety and traceability solution that enhances transparency and accountability across the global food supply chain. It connects participants—including growers, processors, wholesalers, distributors, manufacturers, and retailers—through a permissioned, immutable, and shared record of food provenance, transactions, and processing details.

Key Features

- **Trace Module:** Enables organizations to trace their products along the supply chain and share data with authorized partners.
- **Documents Module:** Allows uploading, viewing, and sharing of documents such as facility certificates and audit reports, with controlled access.
- **Consumer Module:** A customizable application that enables brands to share product stories with customers using permissioned blockchain data.

Benefits

- **Improved Food Safety:** Facilitates quick identification and tracing of contamination sources, aiding in efficient product recalls.
- **Regulatory Compliance:** Assists in meeting safety and regulatory requirements, including the upcoming FSMA 204(d) compliance deadline in January 2026.
- **Supply Chain Efficiency:** Helps eliminate bottlenecks by providing end-to-end visibility, leading to a more efficient food network
- **Consumer Trust:** Builds brand trust by offering transparency into product origins and supply chain practices.[4]

By leveraging IBM Food Trust, companies can enhance food safety, ensure compliance, improve supply chain efficiency, and build consumer trust through increased transparency.

Ethereum-MakerDAO and DAI. The MakerDAO is a cryptocurrency protocol – a set of rules and actions that determines how a specific type of cryptocurrency works[8]. The MakerDAO (which stands for "Decentralized Autonomous Organization") started in 2014 and runs off the Ethereum blockchain. It issues a governance token, called MKR[27], which allows the holder of the token to participate in the governance and policy making of the DAO, as well as the DAI stablecoin. DAI is the specific type of cryptocurrency that is governed by the rules of the MakerDAO. DAI is a type of cryptocurrency token known as a stablecoin, which means that the value of 1 DAI is "soft-pegged" to 1 USD at all times[17]. It is a more stable form of cryptocurrency given that its rate does not fluctuate constantly – hence the term "stablecoin". This peg is maintained as anyone looking to generate or borrow DAI must open a Maker collateral vault and deposit Ethereum-based assets as collateral. The value of the collateral deposited at the vault must always exceed the value of the DAI issued. If the value of the collateral falls below the value of the DAI generated, the collateral will be liquidated automatically by smart contracts to ensure that the value of the DAI doesn't fall below the soft-peg of 1$USD. This makes DAI an algorithmic stablecoin that also has some characteristics of a crypto-backed stablecoin. How

does MakerDAO work? At launch, 1 million MKR tokens were created to govern the Maker protocol. Anyone who owns these MKR tokens can cast a vote on key decisions using a process known as Executive Voting. If an Executive Vote is passed, then the code in the Maker Protocol is changed to reflect the winning proposal. However, before an Executive Vote can be carried out, another form of voting must first take place. This is called Proposal Polling, and it's a way for MKR holders to gauge sentiment on a proposal before committing any changes to the protocol. A third type of vote can be cast by non-MKR holders using threads in the MakerDAO forum. But while anyone may make proposals to MakerDAO, only MKR holders can vote on them. A vote is then measured by the amount of MKR tokens committed to a proposal. For example, if 10 holders with 1,000 MKR vote for Proposal A, while 5 holders with 5,000 MKR vote for Proposal B, Proposal B wins because more MKR tokens support it. Only the number of tokens, not the number of token holders, influences the vote's outcome. DAI Savings Rate Importantly, MKR holders can decide how much DAI holders earn if they save DAI on the platform. The amount DAI holders earn for doing this is known as the DAI Savings Rate. The DAI Savings Rate has been as high as 8.75% per annum, and as low as 0%. In fact, the current savings rate is set at zero due to a market crash in March that caused DAI to trade significantly above $1. In the aftermath of the crash, MKR holders voted to set the DAI Savings Rate to 0% to encourage the sale of DAI, which would bring the price of DAI closer to $1. In this case, MKR holders voted in-line with expectations. When the price of DAI rises above $1, MKR holders are expected to vote to decrease the savings rate to reduce demand, causing the price to fall. If the price of DAI is under a dollar, then MKR holders should vote to raise the savings rate to increase demand to hold DAI, thus causing the price to rise.[1][16]

5 Conclusion

This paper introduced the idea of the blockchain technology and the smart contracts.Specifically, we presented the benefits of disadvantages of blockchain while proposing solutions to make blockchain more usable in decentralized databases.On the other side,we introduced smart contracts as a possible solution to the security problem of blockchain and analyzed it's technical architecture,it's life cycle,advantages and disadvantages and vulnerabilities.Last but not least, we presented some companies that are currently using smart contracts to make their transactions safer,more cost efficient,transparent and improve customer experience overall.

References

[1] Wired: A 50 million hack just showed that the dao was all too human. *online accessed at https://www.wired.com/2016/06/50-million-hack-just-*

showed-dao-human/, 2016.

[2] Mohsen Bafandehkar, Sharifah Md Yasin, Ramlan Mahmod, and Zurina Mohd Hanapi. Comparison of ecc and rsa algorithm in resource constrained devices. In *2013 international conference on IT convergence and security (ICITCS)*, pages 1–3. IEEE, 2013.

[3] Rob Behnke. Explained:the dodo dex hack. *online accessed at https://www.halborn.com/blog/post/explained-the-dodo-dex-hack-march-2021*, 2021.

[4] R Bhuvana and PS Aithal. Blockchain based service: A case study on ibm blockchain services & hyperledger fabric. *International Journal of Case Studies in Business, IT, and Education (IJCSBE)*, 4(1):94–102, 2020.

[5] BRICKKEN. Nick szabo, the man behind the smart contracts. *online accessed at https://www.brickken.com/en/post/blog-nick-szabo*, 2024.

[6] CFI. Smart contracts. *online accessed at https://corporatefinanceinstitute.com/resources/valuation/smart-contracts/*, 2024.

[7] Carlo RW De Meijer. Remaining challenges of blockchain adoption and possible solutions. *online, accessed*, 5(11):2021, 2020.

[8] Eleunthia Wong Ellinger, Tobias Mini, Robert Wayne Gregory, and Alexander Dietz. Decentralized autonomous organization (dao): The case of makerdao. *Journal of Information Technology Teaching Cases*, 14(2):265–272, 2024.

[9] FinaryLabs. Advantages and disadvantages of smart contracts. *online accessed at https://medium.com/coinmonks/advantages-and-disadvantages-of-smart-contracts-91d8bcf4ad27: :text=In*

[10] GeeksforGeeks. Life cycle of smart contract. online accesses at https://www.geeksforgeeks.org/life-cycle-of-smart-contract/*, 2024.*

[11] Iberdola. Smart contracts. online accessed at https://www.iberdrola.com/innovation/smart-contracts.

[12] IBM. What are smart contracts on blockchain? online accessed at https://www.ibm.com/topics/smart-contracts.

[13] Jovan Kalajdjieski, Mayank Raikwar, Nino Arsov, Goran Velinov, and Danilo Gligoroski. Databases fit for blockchain technology: A complete overview. Blockchain: Research and Applications*, 4(1):100116, 2023.*

[14] Victor Youdom Kemmoe, William Stone, Jeehyeong Kim, Daeyoung Kim, and Junggab Son. Recent advances in smart contracts: A technical overview and state of the art. IEEE Access*, 8:117782–117801, 2020.*

[15] *Dodo Khan, Low Tang Jung, and Manzoor Ahmed Hashmani. Systematic literature review of challenges in blockchain scalability.* Applied Sciences*, 11(20):9372, 2021.*

[16] *Shafaq Naheed Khan, Faiza Loukil, Chirine Ghedira-Guegan, Elhadj Benkhelifa, and Anoud Bani-Hani. Blockchain smart contracts: Applications, challenges, and future trends.* Peer-to-peer Networking and Applications*, 14:2901–2925, 2021.*

[17] *Martin Kjäer.* Quantitative analysis of makerDAO's liquidation system*. PhD thesis, Wien, 2021.*

[18] *LCX. Life cycle of a smart contract explained.* online accessed at https://www.lcx.com/life-cycle-of-smart-contract-explained/*, 2023.*

[19] *LCX. Smart contracts security challenges explained.* online accessed at https://www.lcx.com/smart-contracts-security-challenges-explained/*, 2024.*

[20] *MicrosoftAzure.Retrieved December 30th.From https://azure.microsoft.com/en-us/solutions/web3.*

[21] *Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system.* Satoshi Nakamoto*, 2008.*

[22] *NFT.EU. What is a smart contract?* online accessed at https://nft.eu/article/what-is-a-smart-contract*, 2024.*

[23] *Michael Nofer, Peter Gomber, Oliver Hinz, and Dirk Schiereck. Blockchain.* Business & information systems engineering*, 59:183–187, 2017.*

[24] *Joseph Poon and Thaddeus Dryja. The bitcoin lightning network: Scalable off-chain instant payments, 2016.*

[25] *Siemens.Retrieved December 30th.From https://www.siemens.com/global/en/company/innovation/collabo partnerships.html.*

[26] *Cryptomedia staff.* online accessed at https://www.gemini.com/cryptopedia/the-dao-hack-makerdao*, 2023.*

[27] *Xiaotong Sun, Charalampos Stasinakis, and Georgios Sermpinis. Decentralization illusion in decentralized finance: Evidence from tokenized voting in makerdao polls.* Journal of Financial Stability*, page 101286, 2024.*

[28] *Toqeer Ali Syed, Ali Alzahrani, Salman Jan, Muhammad Shoaib Siddiqui, Adnan Nadeem, and Turki Alghamdi. A comparative analysis of blockchain architecture and its applications: Problems and recommendations.* IEEE access*, 7:176838–176869, 2019.*

[29] *Nick Szabo. Winning strategies for smart contracts.* foreword by Don Tapscott, Blockchain Research Institute*, 4, 2017.*

[30] *Ingo Weber, Vincent Gramoli, Alex Ponomarev, Mark Staples, Ralph Holz, An Binh Tran, and Paul Rimba. On availability for blockchain-based systems. In* 2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS)*, pages 64–73. IEEE, 2017.*

[31] *Mengya Zhang, Xiaokuan Zhang, Yinqian Zhang, and Zhiqiang Lin. Cross-chain bridges: Attack taxonomy, defenses, and open problems. 2024.*