Journal of Petroleum Research and Studies

Open Access
No. 39, June 2023, pp. 100-118

P- ISSN: 2220-5381
E- ISSN: 2710-1096

DOI: http://doi.org/10.52716/jprs.v13i2.580

Utilizing Blockchain Technology for Oil and Gas Industry

Raad Mohammed
State Company for Gas Filling and Services, Ministry of Oil, Iraq.
Corresponding Author E-mail: raadmohammed797@gmail.com

Received 3/2/2022, Accepted in revised form 29/3/2022, Published 15/6/2023

Abstract

During the last two decades, all fields, including the oil sector, depended mainly on technological progress to keep pace with the developments in this field. This technological progress was accompanied by an increase in hacking attempts. Cyber-attacks are defined as the hacking of a computer by a person or group of people over the Internet, causing a lot of damage, especially to devices and equipment that depend on the Internet; This leads to substantial financial losses. Therefore, it is very important to understand these attacks and try to overcome them. In the oil sector, cyber-attacks can be scanned in three areas (upstream, midstream, and downstream). This paper discusses how to secure cyber security for the oil sector by making plans for Internal and external cybersecurity by creating and securing separate loops by using blockchain technology and creating a smart contract for each loop to protect it information. As well as using the simulation and control system to increase the effectiveness of cyber security, and after this survey process. This paper aims to classify the cyber-attacks that affect the oil and gas sectors. Create a strong system against any type of cyber-attack, and thus provide higher protection for oil and gas companies and equipment through the work of special programs to protect systems and equipment from hacking.

Keywords: cyber-attack, oil, cyber security, infrastructure, Blockchain technology, upstream, downstream, mid-stream.

استخدام تقنية Blockchain في صناعة النفط والغاز

الخلاصة:

خلال العقدين الماضيين، اعتمدت جميع الحقول، بما في ذلك قطاع النفط، بشكل أساسي على التقدم التكنولوجي لمواكبة التطورات في هذا المجال. رافق هذا التقدم التكنولوجي زيادة في محاولات القرصنة. تُعرَّف الهجمات الإلكترونية على أنها اختراق لجهاز كمبيوتر من قبل شخص أو مجموعة من الأشخاص عبر الإنترنت، مما يتسبب في الكثير من الضرر، لا سيما للأجهزة والمعدات التي تعتمد على الإنترنت ؛ هذا يؤدي إلى خسائر مالية كبيرة. لذلك، من المهم جدًا فهم هذه الهجمات ومحاولة التغلب عليها. في قطاع النفط، يمكن فحص الهجمات الإلكترونية في ثلاث مجالات (المنبع والوسط والمصب). تناقش هذه الورقة كيفية تأمين الأمن السيبراني لقطاع النفط من خلال وضع خطط للأمن السيبراني الداخلي والخارجي من خلال إنشاء وتأمين حلقات منفصلة باستخدام

تقنية Blockchain ، وإنشاء عقد ذكي لكل حلقة لحماية معلوماتها. وكذلك استخدام نظام المحاكاة والتحكم لزيادة فاعلية الأمن السيبراني، وبعد عملية المسح هذه. تهدف هذه الورقة إلى تصنيف الهجمات الإلكترونية التي تؤثر على قطاعي النفط والغاز. إنشاء نظام قوي ضد أي نوع من أنواع الهجمات الإلكترونية، وبالتالي توفير حماية أعلى لشركات ومعدات النفط والغاز من خلال عمل برامج خاصة لحماية الأنظمة والمعدات من القرصنة.

1. Introduction:

Due to increased automation based on modern technologies, companies are becoming increasingly vulnerable to cybersecurity dangers as computer networks become more connected, the use of Internet of Things devices grows, and the use of cloud computing services grows. Incident Command System (ICS) was operating in isolation, without infrastructure passing over it. Engineers can manage Supervisory Control and remote Data Acquisition (SCADA) systems and monitor operations in real time thanks to the industry's capacity to integrate a wide range of industrial technologies into information and communication technology (ICT)[1]. Noting these risks and the damage they cause. Oil and Gas companies need to be more aware of current cyber threats. Planning to establish comprehensive security systems to protect its assets on all fronts and enable it to defend itself against these threats [2].

The oil sector can divide into three stages [3]:

1.1 Upstream.

These operations include the production of oil and gas and their facilities, as well as exploration work for potential fields of oil and gas, whether underground or underwater, drilling experimental wells and then operating those wells and extracting crude oil and pumping it to the surface. The success rates of oil and gas exploration and allied businesses are partly due to technological advancements, particularly in the imaging of oil and gas reservoirs.

1.2 midstream

It is one of the major stages of the oil industry, Transportation, storage, and marketing of petroleum products and natural gas liquids are all included. Transportation is carried to the final stage of the oil industry(downstream) through a network of pipelines for petroleum products.

1.3 downstream

Typically, the term "downstream" refers to the refining of crude oil and natural gas, as well as the marketing and distribution of the finished goods created from these raw materials. In the downstream sector, Petrochemicals and petroleum products such as gasoline and kerosene, as well as jet fuel, diesel oil, heating oil, fuel oils, lubricating waxes, asphalt, natural gas, and LPG, all have a direct impact on customers.

These are the stages that must be secured against electronic piracy operations. This insurance is called cyber security, which can be defined as the process of protecting the system from electronic piracy operations that cause heavy losses. For companies and systems, it can also be defined as, Cyber security refers to the process of protecting an organization's information systems from unlawful or unauthorized use of electronic data, as well as the steps used to attain this level of protection, cyber security is a subdivision of information security that focuses on defending organizations computer systems, cyber security aims to protect the companies and systems[4]. Previously, operational technology networks within the oil industry were confined off the internet as opposed to today's desire for efficiency and real-time decision making which remove that freedom, A cyber-attack on an operational technology environment can result in serious consequences, such as protracted service disruptions caused by a Denial-of-Service (DoS) attack, damages to the hole system, cyber-attack can be either be active attacks or passive attacks based on the intentions and motive of the attackers. cyber threats aimed at compromising the cyber security that a company has put in place to against launch a cyber-attack [5], shows in Figure (1).

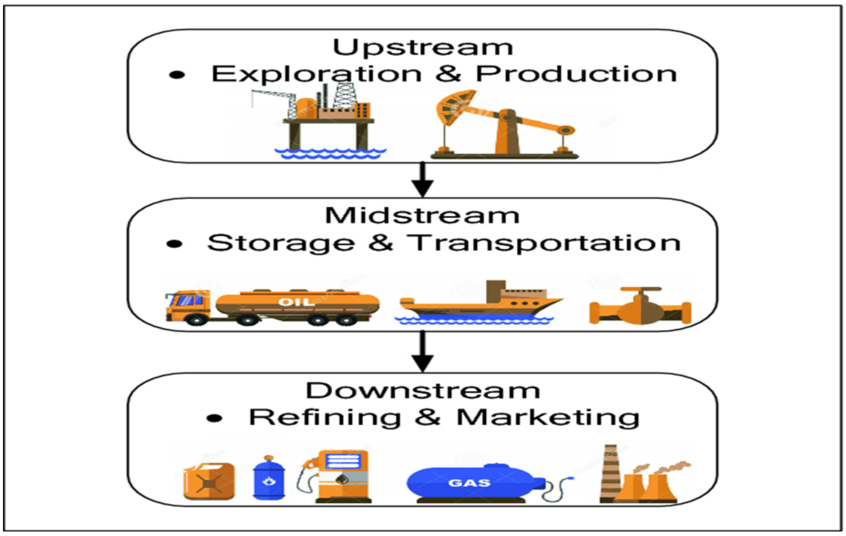

Fig. (1): Upstream, Midstream, Downstream Stages[6].

Blockchain technology is the most important technology used at present to provide a high level of protection and security for various types of digital data. The decentralized environment provided by Blockchain technology can also be integrated to manage data for applications outside of financial systems. Therefore, most of the global programming companies such as Microsoft, IBM, Accenture, and others have moved to establish organizations whose mission is to develop Blockchain-based technologies that can be adopted by their industrial partners [7]. The Blockchain enables authentication, confidentiality, accountability, and data sharing while handing out privacy-related information, providing energy resources and facilities to customers, and making it a smart[8].

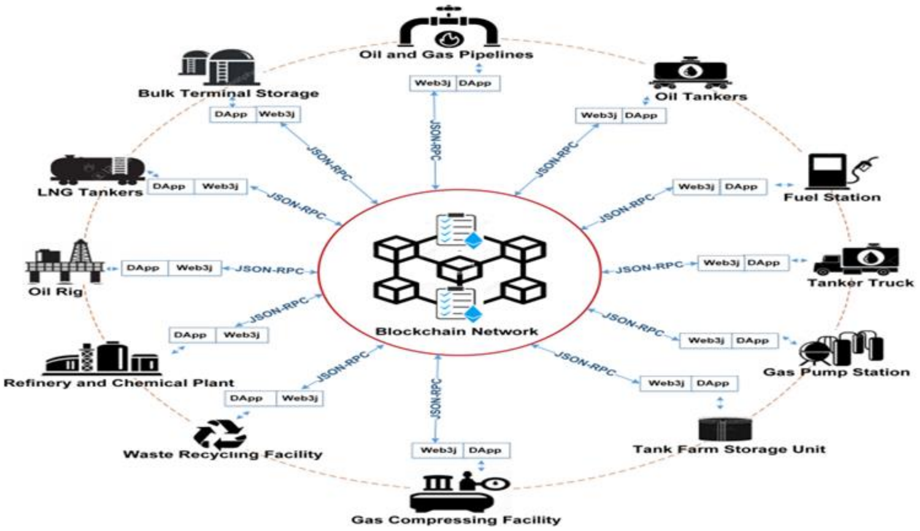

Fig. (2): Storing and retrieving oil and gas-related data using the blockchain[9]

2. Literature Review

In the beginning, must know who the cyber attacker is and where these attacks come from? and the most famous types of attacks, and then define the necessary defensive plans to protect from these attacks, apply cyber security, and answer all these questions through the attack maps provided by Internet service providers, and perhaps the most famous of these maps it [5] [10]:

1- Kaspersky cyber-attack map.

2- Norse attack map.

3- Digital attack map.

4- Trend micro.

5- Fortinet threat map.

6-Fire eye.

7- DoS &cyber-attack map.

8-Checkpoint cyber-attack map.

9- Akamai.

10- Ransomware attack.

This is the first tool that must be obtained to start understanding the problem, and then start defining defensive plans against any attack. The second tool that must be obtained is the processing maps against any attack, the third tool is to identify the gaps in the system (the oil sector), which previously Divide it into three stages, and trying to link these gaps with the electronic attack maps as well as the processing maps. Figure (3) shows Examples for cyber-attack maps.

Fig. (3): One of the cyber-attack maps.

3. Classification of cyber-attack:

The first stage includes exploration and drilling operations, while the second stage includes transportation and storage operations, and the third stage includes refining and distribution operations. each one of these stages is vulnerable to threats of cyberattacks. The Figure (4) shows the impact of cyber threats for each stage.

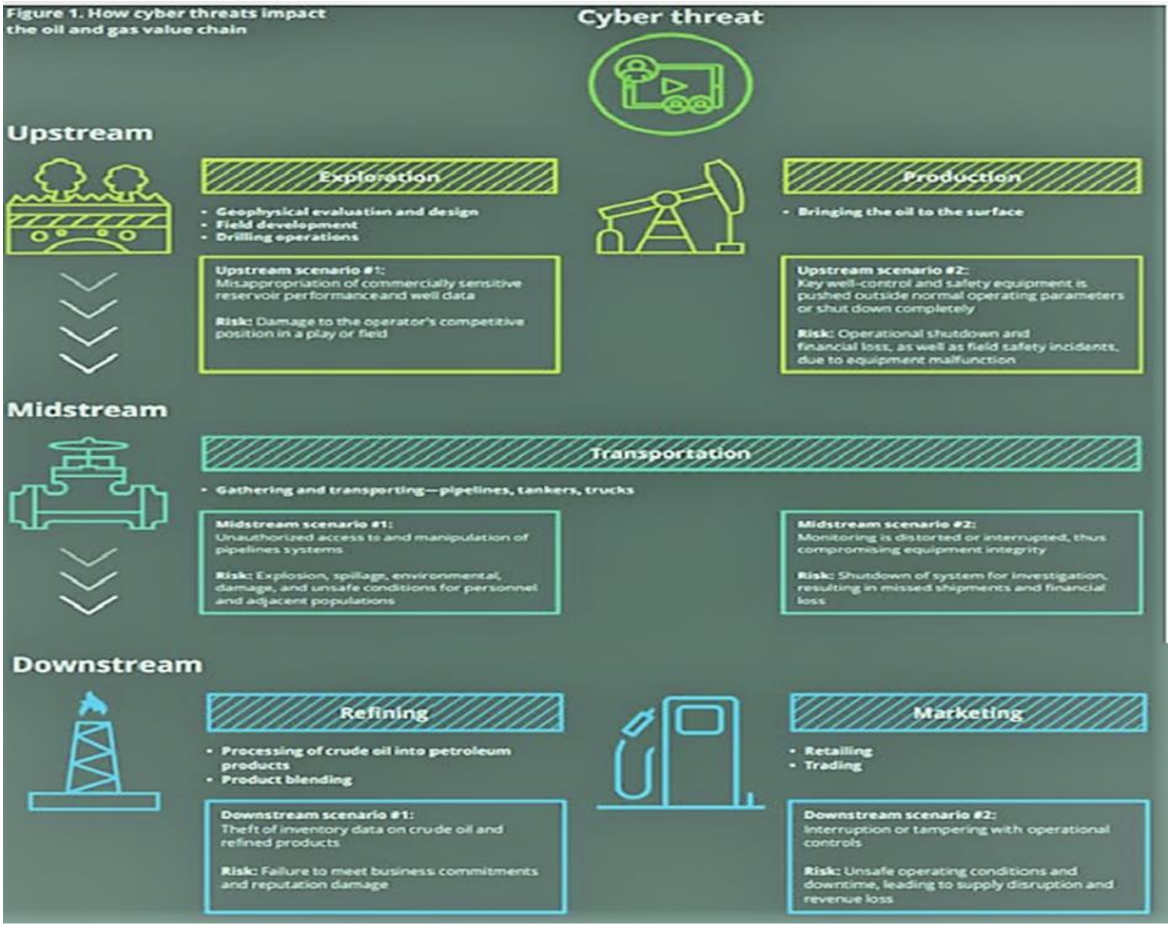

Figure 1. How cyber threats impact the oil and gas value chain

Cyber threat

Upstream

Exploration

- Geophysical evaluation and design
- Field development
- Drilling operations

Upstream scenario #1:
Misappropriation of commercially sensitive reservoir performanceand well data

Risk: Damage to the operator's competitive position in a play or field

Production

- Bringing the oil to the surface

Upstream scenario #2:
Key well-control and safety equipment is pushed outside normal operating parameters or shut down completely

Risk: Operational shutdown and financial loss, as well as field safety incidents, due to equipment malfunction

Midstream

Transportation

- Gathering and transporting—pipelines, tankers, trucks

Midstream scenario #1:
Unauthorized access to and manipulation of pipelines systems

Risk: Explosion, spillage, environmental, damage, and unsafe conditions for personnel and adjacent populations

Midstream scenario #2:
Monitoring is distorted or interrupted, thus compromising equipment integrity

Risk: Shutdown of system for investigation, resulting in missed shipments and financial loss

Downstream

Refining

- Processing of crude oil into petroleum products
- Product blending

Downstream scenario #1:
Theft of inventory data on crude oil and refined products

Risk: Failure to meet business commitments and reputation damage

Marketing

- Retailing
- Trading

Downstream scenario #2:
Interruption or tampering with operational controls

Risk: Unsafe operating conditions and downtime, leading to supply disruption and revenue loss

Fig. (4): The Cyber Threat in Upstream, Midstream and Downstream [11].

4. Cyber Security:

Cyber security refers to methods for protecting a user's or organization's cyber environment that are frequently recorded in published materials [12]. It oversees the tactics used to prevent unauthorized access to networks, applications, and data.

The problems posed by the integration of information technology and operations technology for any organization in the oil and gas industry are exacerbated by two fundamental issues. First, compared to many other industries, there is more dependency among the stages of the industry chain. The oil industry is a complex ecosystem with upstream, midstream, and downstream enterprises and organizations, as well as organizations involved in various parts of business, complicating the security situation. Private oil corporations, state-owned oil companies, small businesses that specialize in a single commodity, and a variety of service providers and other parties all contribute to this environment. This integration creates a stable environment for many entrance points and gaps.

Second, new and sophisticated technologies are rapidly entering the oil and gas industries. On top of the highly complex interoperable industries already dealing with integrated IT and OT systems, new technologies on the horizon could complicate a task for which both the Chief Information Officer (CIO) and the Chief Information Security Officer (CISO) are responsible for ensuring enterprise security. Digital oilfields linked to cloud platforms for big data analytics, the use of drones to extract oil and gas for surveys or environmental monitoring, and third-party companies that host 3D modeling for quality and field planning are just a few of the new technologies entering the industry that could create additional flaws [13]. Recently, the most common technology used to give a high level of cyber security is blockchain technology which discusses in the next section, and how to use it in the oil industry.

5. Blockchain Technology:

A Blockchain is a decentralized distributed technology for the ledgers or the records that include all transactions or events that are verified by special algorithms (Proof of Work, Proof of Stake, and Proof of Authority) [14]. Once a transaction has been validated, it cannot be altered or even erased. Digital cryptocurrencies such as Bitcoin, Ethereum are the common application of Blockchain technology, but this technology can be used in other areas such as healthcare and IoT.

5.1 Layers of Blockchain Technology

Data Layer: This layer specifies the essential structure of data including digital activities, blocks, and cryptographic keys, arranges them into blockchains, transaction pools, and wallets, and manages a wide range of data functions (read/write/cache/encrypt/decrypt)[15].

Network layer: The technology of point-to-point transmission (P2P network technology is another name for peer-to-peer network technology), mechanisms of propagation, and methods of verification are the major components of this technology. Consensus techniques, encrypted signatures, data storage, and other features are included. The network layer's main goal is to create a chain of information communication between nodes in a network [16].

Smart Contract Layer: The contract layer encompasses a variety of script codes, algorithmic processes, and smart contracts that create regulated and auditable contract specifications [16]. Smart contract flaws include a disordered exception, reentrancy, dependency on timestamps, reliance on block numbers, appeal for a damaging delegate, and freezing, to name a few. Hackers can easily exploit smart contracts owing to faults and weaknesses. A single trusted verifier or a group of trusted verifiers can confirm a smart contract. Smart contract development, on the other hand, lacks discipline and consistency. Program testing can be performed to discover the presence of bugs. However, it is unable to determine whether or not bugs exist. Given the financial nature of smart contracts, vulnerabilities or faults in their systems could have disastrous effects. Smart contracts can benefit from the formalized process. It may be able to detect a variety of errors and inaccuracies in existing semantics. It may also be used to determine whether the code fulfills the specifications mathematically. used formal methods and game theory to validate decentralized two-party smart contracts. It does not, however, address how to codify multi-party smart contract verification in Blockchain-based platforms [17].

Consensus Layer: The network maintainers of this layer validate digital activity and generate new blocks for system consensus. Consensus mechanisms fall into two categories when it comes to describing the trade-off between security and expense: • Any entity can be a maintainer for permissionless consensus. Permissionless consensus can help to promote network neutrality and democracy, but it can also add a lot of overhead.

Application layer: The application layer, as the uppermost layer, provides clients, SPs, and developers with trusted application programming interfaces (API), as well as supporting a variety of DApps such as ubiquitous access, edge services, and trusted intelligence[15].

5.2 Blockchain Classification

There are several types of Blockchain technology, the most important of which are [18]:

❖ ***Permissionedless or Public Blockchain:*** They are chains open to the public in which any individual can become a member and can participate in decision-making. In this type of Blockchain, no participant has a ledger because it is accessible to everyone. The instructors use a distributed consensus mechanism in decision-making to keep a copy of the ledger on their contract.

❖ ***Permissiond or Private Blockchain:*** This type of blockchain is not available to the public. It is open to a group of people only and the ledger is shared with the participating members only.

❖ ***Semi-Private Blockchain:*** In this network, some parts of the network are organized and managed by a group, and some parts are available for the public to participate in.

5.3 Blockchain Algorithms

In this section, a brief explanation of the most prominent blockchain algorithms is provided.

❖ **Proof of Work (PoW):** The combination of encryption and processing power in a PoW protocol establishes consensus and ensures the authenticity of data stored on the blockchain. To prove that a block is valid and that work has been done, network nodes (known as miners) use their computational power to validate transactions (ensure that a sender has sufficient funds and is not engaging in double-spending) and, more significantly, compete in a race to solve the protocol's cryptographic challenges. The term for this procedure is mining [19].

❖ **Proof of stake (PoS):** One of the most promising strategies for replacing PoW while maintaining similar resilience qualities is PoS. Despite the fact that PoW necessitates the honesty of a (qualified) majority of computer power, PoS assumes that honest participants control the majority of the money in the system. Individuals with significant interests in the system have a financial motive to keep the system working according to the protocol specifications because they risk losing their shares if the coin loses trust [20]. To accomplish the leader's election and maintain network consensus, PoS makes use of virtual resources such as a node's stake. Because the mining resources are virtual, the PoS-based consensus process is instantaneous and has no costs [21].

Proof of Authority (PoA): It is a permissioned blockchain consensus algorithm family that has grown in popularity due to improved efficiency over traditional Byzantine Fault Tolerant (BFT) algorithms due to lighter message exchanges. PoA was first proposed as part of the Ethereum ecosystem for private networks [22]. Because it permits different blocks to be appended to the same index of the chain, the standard Ethereum protocol based on PoW can fork. If not identified early enough, this forking condition can lead to security issues such as double spending. Alternative protocols aimed at avoiding forks, known as PoA protocols, have recently been implemented into the most extensively deployed versions of Ethereum, parity, and Geth, and are now utilized worldwide. PoA has grown in popularity, and it is currently available from major SaaS providers and used on several blockchain networks [23].

5.4 Ethereum

Ethereum is an open-source computer platform based on Blockchain technology. The key feature of Ethereum is that it allows programmers to create Decentralized Applications (Dapps) that operate on the Ethereum Blockchain[24]. Ethereum’s core innovation is Ethereum Virtual Machine (EVM), which is a Turing-complete software that allows anyone to create and run their application regardless of programming language. The platform gives developers the ability to build and run their applications without having to build an entire blockchain from scratch. The EVM, Ethereum's P2P network, is a set of computers operated by users of the Ethereum network. They combine their computing power to run the Ethereum Blockchain's P2P network. An important characteristic of the EVM is its capacity to defend against Distributed Denial-of-Service (DDoS) attacks. Because there is no central server or point of entry for hackers to exploit, launching a successful DDoS attack is nearly impossible [25].

5.5 Smart Contract

Smart Contract (SC) is a piece of computer code that may run autonomously and perform specific functions when certain conditions are met. A distributed ledger can be used to store and process the code, and any modifications will be written to the ledger [26]. SC's main purpose is to give better protection than traditional contract law while also cutting transaction costs. SC has the following features:

- Solely electronic nature.
- Software implementation.
- Increased certainty.
- Conditional nature.
- Self-performance.
- Self-sufficiency.

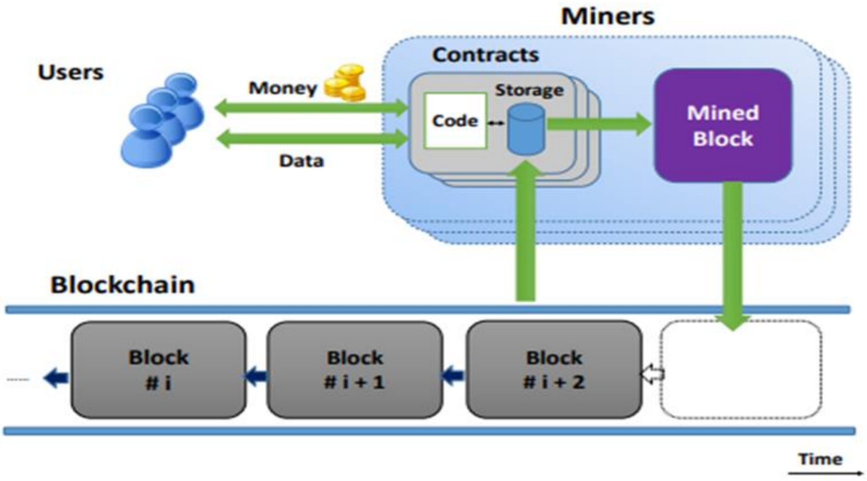

Fig. (5): Smart Contract [27]

In Ethereum, a special development transaction is used to deploy an SC. This is the first time a contract has been added to the Blockchain. The contract is given a unique

address and its code is uploaded to the Blockchain during this process. It is defined by a contract address once it has been successfully established. Any person involved in the transaction is given an Ethereum address. Each contract is associated with a predefined executable code and contains a certain amount of virtual coins. Since cryptography is used for compliance, it plays a critical role in this. A transaction's initiator pays a charge (gas) for its execution, which is also measured in units of gas.

SC automatically carries out the contract terms based on the information they collect. The parties come to an understanding of the contract's contents, and the contracts are carried out according to the actions written in the computer algorithms. SC is self-executing and self-verifying agents that cannot be modified after they have been deployed on the Blockchain. The SC checks to see if the parties in a transaction follow the SC's rules. The transaction is validated if they do; otherwise, it is denied. SC's may be used to move large amounts of money. As a result, they must be implemented in a secure and bug-free manner [28].

6. Tools & Devices for cyber-attack treatment:

In this section, reference is made to the most prominent hardware and software that can be used to address cyber-attacks to gain access to a system that is protected from these attacks.

6.1 The security tools for a cyberattack:

These tools are software or programs, the goal of which is to protect against any cyberattack, and these tools may differ in strength and function, but their purpose, is protection from electronic piracy, and this research presents the most famous tools in this topic. There are both free and paid network tools on the market that can be used to improve networking security. The following items are listed below:

Nexpose - John the Ripper –Metasploit- Wire shark- Kali Linux- Nikto--KisMAC-Burp Suite-Spelunk -Nets tumbler -Aircrack-ng-Tor-Nagios-OSSEC Cain and Abel-Tcpdump-Force point-Paros Proxy-Nmap-Nessus

Professional-POF-Snort-Acunetix-Argus-GFI LanGuard-Solar

Winds Security Event Manager-Bitdefender-Malware bytes-VIPRE-Avira-Life Lock-Mime cast-Web root.

6.2 Cyberattack devises treatment:

Also, the devices used are intended to protect against electronic piracy and achieve cyber security, and each of these devices has an active role in the protection process, but it should be noted that the skill in using and employing these devices is much more important than the number of devices. Below are the devices used, which represent a system to protect against cyber-attacks:

1-remotes devices

2-senors

3- Monitors

4-networkgateway

5-control devices

6- Exploration device

7-bridges

8- data analyses devices

7. Discussion and Implementation:

As mentioned above, the oil sector can be divided into three phases:

1- The stage of drilling and production.

2- The stage of refining and storage.

3-The stage of transportation and distribution.

And between these three stages is the stage of transferring between the three stages.

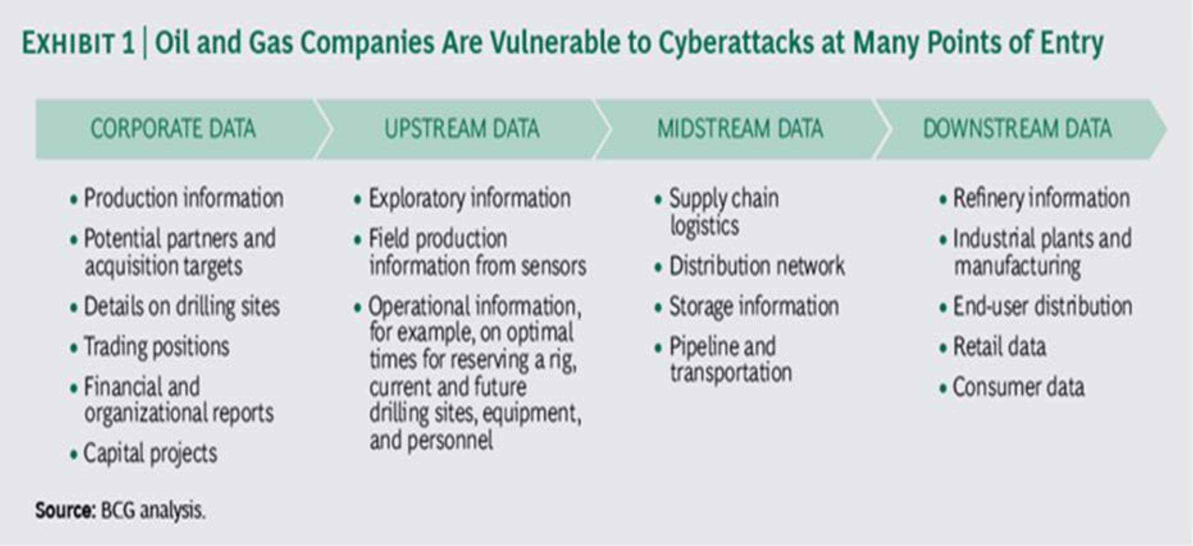

EXHIBIT 1 | Oil and Gas Companies Are Vulnerable to Cyberattacks at Many Points of Entry

CORPORATE DATA
- Production information
- Potential partners and acquisition targets
- Details on drilling sites
- Trading positions
- Financial and organizational reports
- Capital projects

UPSTREAM DATA
- Exploratory information
- Field production information from sensors
- Operational information, for example, on optimal times for reserving a rig, current and future drilling sites, equipment, and personnel

MIDSTREAM DATA
- Supply chain logistics
- Distribution network
- Storage information
- Pipeline and transportation

DOWNSTREAM DATA
- Refinery information
- Industrial plants and manufacturing
- End-user distribution
- Retail data
- Consumer data

Source: BCG analysis.

Fig. (6): Vulnerable pointes in oil and gas companies [4].

After knowing the stages (loops) that can be made making internal security for them, and using the simulation system, it is possible to achieve a higher performance of cyber protection.

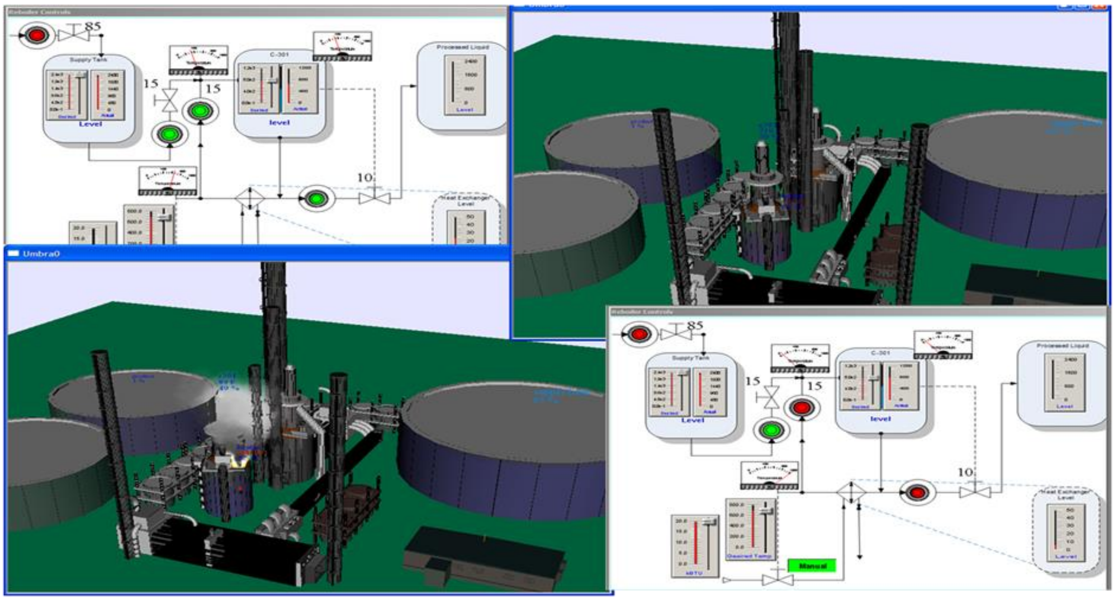

Fig. (7): Shown control circle and devises

The idea is to make an internal cyber protection for each stage separately, considering that each stage can be divided into smaller stage (loop) and securing all these stages internally using blockchain technology that includes creating a smart contract for each stage (loop). These smart contracts (SC) are linked to an application for the oil sector, which receives the data, processes it, and then sends the data to the smart contract(SC) for each stage (loop), and the rest of the contracts are notified of the status that took place in this stage. After that, the data is stored in the blockchain network (Ethereum, for example) for the purpose of protecting it.

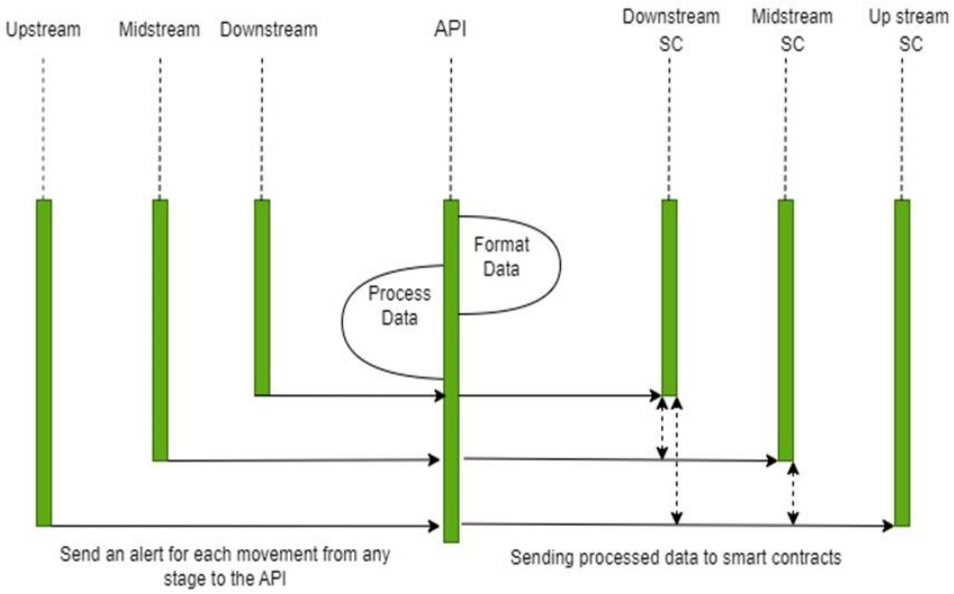
Upstream
Midstream
Downstream
API
Downstream SC
Midstream SC
Up stream SC
Format Data
Process Data
Send an alert for each movement from any stage to the API
Sending processed data to smart contracts

Fig. (8): Sequence diagram for oil industry system

The first smart contract (SC) is created for the upstream stage, as it receives data from the fields for the upstream stage in the application for the oil sector. The data is sent from the application to the smart contract via web3, to be stored after that in the blockchain network.

```
Algorithm 1: Smart Contract for Upstream:
Input:
Upstream US: Upstream Record
Begin:
    1. Set Upstream Record
    2. Check whether PS >= 0.7.0 and PS < 0.8.0
    3. Check whether Upstream US [upstream.eth_address] == address(0x0)
    4. Add Upstream US to the SC
    5. Otherwise, Ignore
    6. End if
    7. End loop
    8. End algorithm
```

The second smart contract (SC) is linked to the second phase of the oil sector, which is the (Midstream) stage. Where the data from the fields for this stage in the application is sent to the smart contract after processing it, and the smart contract for this stage receives the movements that occurred in the upstream stage by calling the smart contract(SC)t for this stage to the (Midstream) stage. After verifying the addresses, the data is accepted and saved in the blockchain network, in addition to saving the data of the (Midstream) stage contract.

```
Algorithm 2: Smart Contract for Midstream:
Input:
Midstream MS: Midstream Record
Import Upstream SC
Begin:
        1.  Set Midstream Record
        2. Check whether PS >= 0.7.0 and PS < 0.8.0
        3. Check whether Midstream MS [midstream.eth_address] == address(0x0)
        4. Add Midstream MS to the SC
        5. End if
        6. End loop
        7. Check whether Upstream SC
        8. Add information to Midstream SC
        9. Otherwise; Ignore
        10. End if
        11. End loop
        12. End algorithm
```

The third contract is for the last stage, which is the downstream stage. As is the case in the previous two contracts, the contract for this stage receives its data from the oil sector application by filling in its fields in the application. After processing the data, it is sent to the smart contract for the downstream stage. Data for the previous two contracts (upstream, midstream) is also received and saved in this contract after verifying the addresses of the previous two contracts are correct.

Algorithm 3: Smart Contract for Downstream:

```
Input:
Downstream DS: Downstream Record
Import Upstream SC
Import Midstream SC
Begin:
Set Downstream Record
Check whether PS >= 0.7.0 and PS < 0.8.0
Check whether Downstream MS [downstream.eth_address] == address(0x0)
 Add Downstream DS to the SC
 End if
 End loop
 Check whether Upstream SC
 Add information to Downstream SC
 Otherwise; Ignore
 End if
 Check whether Midstream SC
 Add information to Downstream SC
  Otherwise; Ignore
 End if
 End loop
 End algorithm
```

The exchange of data between the smart contracts of the three stages is very important. As based on blockchain technology that does not allow changing or manipulating the data through the immutability feature provided by this technology. The movements between these three stages will be safe and protected and cannot be hacked or tampered.

8. Economic and technical feasibility (Aims):

The feasibility of cybersecurity from a technical and economic point of view cannot be ignored at all, because it causes severe damage to all sectors, including the petroleum sector, and economic feasibility, of course, means saving a lot of money, as piracy operations have caused losses the trillions, especially in the recent period. Equipment, assets, engineering, and administrative operating systems, which in turn lead to substantial material losses. It is therefore important that the mandatory disclosure of control system incidents and intrusions, the compilation of electronic espionage reports, and their submission to the WTO. This paper presented a classification of the most prominent cyber-attacks targeting various fields of the oil industry, whether they were websites of companies or oil equipment. And then designing a protection system for companies and equipment that prevents these attacks depends mainly on the principle of the loops and each loop is linked with a separate smart contract that represents a blockchain technology used in the oil industry.

9. Conclusion:

Protecting oil sector data, especially for oil-producing and exporting countries, is extremely important because of its direct impact on the economy of countries. This paper presented a study of the most prominent electronic attacks on the oil sector and their impact on the three stages of oil production and export (upstream, midstream, and downstream). After that, the paper presented a model for protecting the data of these stages on the use of blockchain technology by creating a smart contract for each stage. Data is exchanged between these contracts to ensure that they are not tampered with by taking advantage of the immutability feature provided by blockchain technology. Communication between these contracts takes place through an application created for the oil sector that represents the data of the three phases. This application represents an ideal model for protecting the data of the oil sector, thanks to the use of the best data protection technology at the present time, which is blockchain technology.

Reference:

[1] G. Stergiopoulos, D. A. Gritzalis, and E. Limnaios, “Cyber-Attacks on the Oil Gas Sector: A Survey on Incident Assessment and Attack Patterns,” *IEEE Access*, vol. 8, pp. 128440–128475, 2020, doi: 10.1109/ACCESS.2020.3007960.

[2] F. Hacquebord and C. Pernet, “Drilling Deep A Look at Cyberattacks on the Oil and Gas Industry,” *Drilling Deep: A Look at Cyberattacks on the Oil and Gas Industry*, pp. 1–35, 2019.

[3] I. H. Mackay, “Oil and Gas.,” *CIM Bulletin*, vol. 69, no. 769, pp. 73–82, 1976.

[4] K. Rick and K. Iyer, “Countering the threat of Cyberattacks in oil and gas,” *Bcg*, 2016.

[5] C. G. Xarhoulacos, A. Anagnostopoulou, G. Stergiopoulos, and D. Gritzalis, “Misinformation vs. Situational awareness: The art of deception and the need for cross-domain detection,” *Sensors*, vol. 21, no. 16, 2021, doi: 10.3390/s21165496.

[6] A. S. Azman, M. Y. Lee, S. K. Subramaniam, and F. S. Feroz, “Mesh WSN in midstream and downstream of oil and gas industry,” *Lecture Notes in Mechanical Engineering*, no. August 2021, pp. 456–465, 2020, doi: 10.1007/978-981-13-9539-0_44.

[7] S. Angraal, H. M. Krumholz, and W. L. Schulz, “Blockchain Technology: Applications in Health care,” *Circ Cardiovasc Qual Outcomes*, vol. 10, no. 9, pp. 1–3, 2017, doi: 10.1161/CIRCOUTCOMES.117.003800.

[8] R. U. I. Guo, H. Shi, Q. Zhao, and D. Zheng, “Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems,” *IEEE Access*, vol. 6, pp. 1--11, 2018.

[9] W. Ahmad, K. Salah, R. Jayaraman, I. Yaqoob, and M. Omar, “Blockchain in Oil and Gas Industry: Applications, Challenges, Blockchain in Oil and Gas Industry: Applications, Challenges, and Future Trends and Future Trends Blockchain in Oil and Gas Industry: Applications, Challenges, and Future Trends,” 2021, doi: 10.36227/techrxiv.16825696.v1.

[10] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, “A Survey of IoT-Enabled Cyberattacks: Assessing Attack Paths to Critical Infrastructures and Services,” *IEEE*, vol. 20, pp. 3453–3495, 2018, doi: 10.1109/COMST.2018.2855563.

[11] D. Bundi and M. J. Maranga, “EFFECTS OF CYBERCRIME ON OIL AND GAS INDUSTRY,” vol. 8, no. 6, pp. 322–331, 2020.

[12] C. A. S. Zeadally, “Critical Control System Protection in the 21st Century,” *IEEE*, vol. 46,

pp. 74–83, 2013, doi: 10.1109/MC.2013.69.

[13] Jason Holcomb, “Definitive Guide to Cybersecurity for the Oil & Gas Industry,” pp. 1–28, 2019.

[14] D. P. Oyinloye, J. Sen Teh, N. Jamil, and M. Alawida, “Blockchain consensus: An overview of alternative protocols,” *Symmetry (Basel),* vol. 13, no. 8, pp. 1–35, 2021, doi: 10.3390/sym13081363.

[15] X. Ling, J. Wang, Y. Le, Z. Ding, and X. Gao, “Blockchain Radio Access Network beyond 5G,” *IEEE Wirel Commun*, vol. 27, no. 6, pp. 160–168, 2020, doi: 10.1109/MWC.001.2000172.

[16] Y. Xu, X. Li, X. Zeng, J. Cao, and W. Jiang, “Application of blockchain technology in food safety control：current trends and future prospects,” *Crit Rev Food Sci Nutr*, vol. 0, no. 0, pp. 1–20, 2020, doi: 10.1080/10408398.2020.1858752.

[17] P. Zhang and M. Zhou, “Security and Trust in Blockchains: Architecture, Key Technologies, and Open Issues,” *IEEE Trans Comput Soc Syst*, vol. 7, no. 3, pp. 790–801, 2020, doi: 10.1109/TCSS.2020.2990103.

[18] S. S. Sarmah, “Understanding Blockchain Technology,” *Computer Science and Engineering*, vol. 8, no. 2, pp. 23–29, 2018, doi: 10.5923/j.computer.20180802.02.

[19] S. Seang and D. Torre, “Proof of Work and Proof of Stake Consensus Protocols: a Blockchain Application for Local Complementary Currencies,” *France: Universite Cote d’Azur-GREDEG-CNRS. Str 3.4*, pp. 1–21, 2018.

[20] C. Ganesh, C. Orlandi, and D. Tschudi, “Proof-of-Stake Protocols for Privacy-Aware Blockchains,” vol. 00169, no. 669255, pp. 1–21, 2020.

[21] W. Li, “Securing Proof-of-Stake Blockchain Protocols,” *Data Privacy Management, Cryptocurrencies and Blockchain Technology. Springer, Cham, 2017*, pp. 297–315, 2017, doi: 10.1007/978-3-319-67816-0.

[22] S. De Angelis, L. Aniello, and R. Baldoni, “PBFT vs Proof-of-Authority : Applying the CAP Theorem to Permissioned Blockchain,” *university of southampton*, pp. 1--12, 2017.

[23] P. Ekparinya and G. Jourjon, “The Attack of the Clones Against Proof-of-Authority,” *arXiv preprint*, pp. 1--14, 2020.

[24] S. Luck, “Design and Implementation of a Smart Contract Creator Framework for IoT Devices,” University of Zurich, 2017.

[25] E. M. Hreinsson and S. P. Blondal, “The Future of Blockchain Technology and Cryptocurrencies,” *PhD Thesis*, pp. 1--63, 2018.

[26] J. Earls, M. Smith, and R. Smith, “Smart Contracts: Is the Law Ready?,” *CHAMBER OF DIGITAL COMMERCE*, pp. 1--62, 2018.

[27] K. Delmolino, M. Arnett, A. Kosba, A. Miller, and E. Shi, “Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab,” *International conference on financial cryptography and data security. Springer, Berlin, Heidelberg, 2016*. pp. 79–94, 2015.

[28] M. N. O. Sadiku, K. G. Eze, S. M. Musa, R. G. Perry, P. V. A, and P. View, “Smart Contracts: A Primer,” *Journal of Scientific and Engineering Research*, pp. 1--5, 2018.