Cybersecurity Risks of Blockchain Technology

Ihab M. Abdelwahed
Department of Information Systems and Technology
Faculty of Graduate Studies for Statistical Research

Nagy Ramadan
Department of Information Systems and Technology
Faculty of Graduate Studies for Statistical Research

Hesham Ahmed Hefny
Department of computer Science
Faculty of Graduate Studies for Statistical Research

ABSTRACT
Blockchain technology has become a paradigm shift to digital transactions. It has brought massive potentials in many fields, such as financial services, energy, healthcare and Internet of Things. As often occurs with innovative technologies, it has suffered from several critical Cybersecurity threats and vulnerabilities. The complicated relation between Cybersecurity risk management and companies strategic and operational objectives which make identifying, analyzing, and controlling the relevant risk events as a major challenge. In this paper, the researchers classify those incidents against the Cybersecurity vulnerabilities in Blockchain technology and explain the methods of risk measures according to the Information Security Risk Assessment (ISRA) Models.

Keywords
Cybersecurity; Risk Assessment; Blockchain; Threat; Vulnerabilities

1. INTRODUCTION
The Revolution of industry 4.0 have a great effect from digital twin to the digital transformation. Almost every business is transforming itself by adopting leading technologies and innovative data-driven business models. On this large, remarkable wave of digital transformation, Cybersecurity, operations are an essential element of every enterprise's success. IT solutions must have the proper functionality, availability, usability, and security. Most of the new IT solutions give the security factor little weight and focus on a business value. So many researchers highlight a security issue and the associated risks as an important concern. From this point the researchers should evaluate, asses the risks and threats associated with any solutions. Risk is a universal term, and it has a direct relation of day-today tasks 'The term risk is used in variety of context and domains' A risk assessment is the examination of a business's assets, the threats to those assets and the adequacy of the controls in place to protect them from misuse, or compromise. Risk assessments are the foundation of every security the best practice and are the first step in the formulation of an effective risk management program [1]. However, the researcher can predict, prevent and reduce its consequences of applying analysis techniques, and rational decision-making method.

Risk analysis includes processes such as identification of activity, threat analysis, vulnerability analysis and guarantees. One of the completed phases in information security risk assessment process is risk analysis. It required doing strategies as a part of Information Security Risk Management (ISRM) (see Figure.1) requires wellsprings of exact information, measurable quantities of unforeseen occasions, and so forth to assess and acquire precise outcomes. Moreover, chances evaluation is a multifaceted activity which requires numerous parameters, and a considerable lot of those are hard to measure. The risk assessment process consists of gathering relevant information, risk analysis, and evaluating, to obtain the best possible decision basis regarding planned activities. One of the latest IT solutions that require information security risk management (ISRM) and considered not only as an innovative technology, but as a potential revolution in the business is Blockchain. The term, "Blockchain" is especially used when talking about Crypto currencies, between which bit coin, the one which pioneered this technology, is certainly the most known. Nowadays, however, the Blockchain has already become one of the most interesting areas of research in academics, companies, and investors not only operating in the finance area, but also in many other domains: e.g., scientific, social, humanitarian, medical, and so on. However, with the increasing use of Blockchain, the number and severity of security accidents will go hand in hand [2]. To give an idea of the seriousness of the damage, the analysis published in estimates that, only in 2017, consumers in Blockchain sector lost nearly 490 million dollars [3]. The cause of the incidents was multiple, from wallet theft, to software vulnerabilities. Similarly, Blockchain Graveyard1, which is a list of all massive security breaches or thefts involving Blockchain, calculated from publicly available data that since 2011 there have been 58 incidents [3].

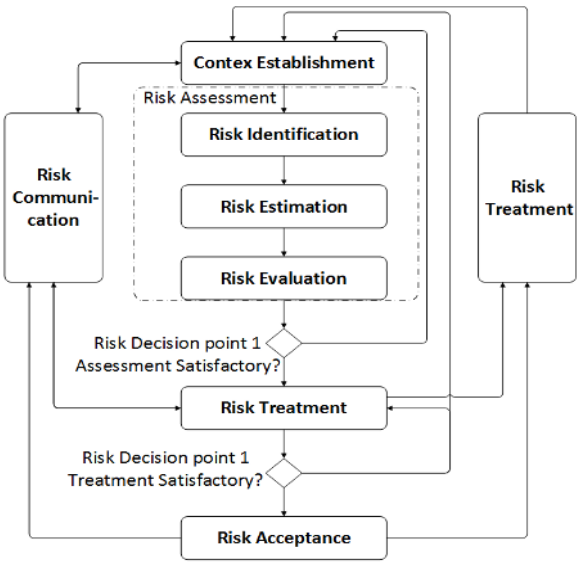

Fig 1: The ISO/IEC 27005:2011 Information Security Risk Management process.

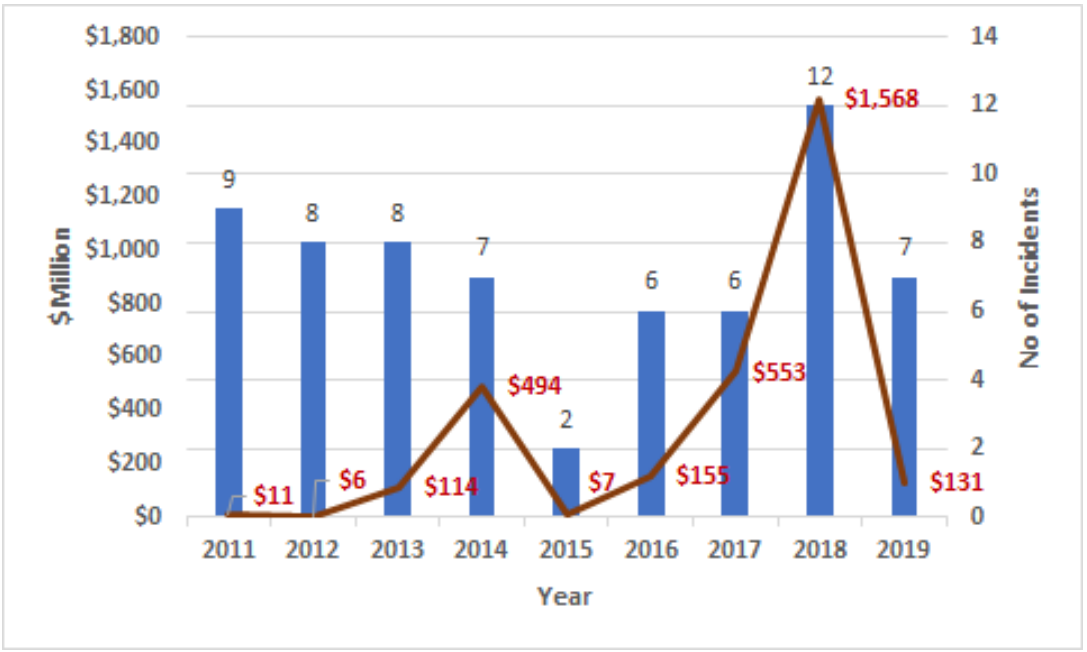

Fig 2: Blockchain Incidents 2011 to 201

In Figure 2 indicates on the average, their square measure seven incidents per twelve months bit by bit diminished to 2015 reached the backside with 2 incidents solely [5]. This drop coincides with the call the charge of Bitcoin therein year. The speed of Bitcoin often climbed up once 2015 and then because the variety of assault incidents 2 that extended increasingly to 12 incidents in 2018.the amount of loss to the incidents accompanied the two identical designs from US$7 million in 2015 expand to a high of US$1.6 billion in 2018.the primary six months in 2019 has already reached seven incidents with the quantity loss is US$131 million solely. However, the researcher tend to believe this selection can amplify within the second half-year of 2019 [5].

2. BACKGROUND ON BLOCKCHAIN

In this section, the researcher introduce the basic Blockchain technological aspects constituting the required background. The successful adoption and operation of any new technology is a dependent on the appropriate management of the risks associated with that technology [6]. Distributed Ledger Technologies (DLT) have the potential to be the backbone of many core platforms in the near future. Blockchain or DLT, were primarily designed to facilitate distributed transactions by removing central management. As a result, Blockchain, for example could help to address the challenges faced by decentralized energy systems [7]. The Blockchain/DLT technology has many attractive features, such as

- Cannot be corrupted
- Decentralized Technology. ...
- Enhanced Security. ...
- Distributed Ledgers. ...
- Consensus. ...
- Faster Settlement.

(See Figure 3). Consequently, these features make Blockchain/DLT a promising solution for many applications problems (cryptocurrency, IoT) [8]. Any transfer of value between two parties and the associated debits and credits are captured in the Blockchain ledger for all parties to see. The cryptography consensus protocol ensures the immutability and irreversibility of all transactions posted to the ledger.

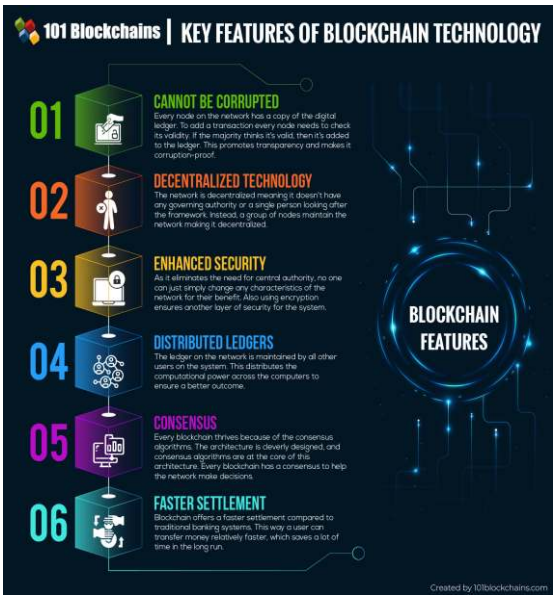

Fig 3: Blockchain features

3. QUANTITATIVE / QUALITATIVE RISK ASSESSMENT METHODS

Any organization can use quantitative and /or qualitative analysis methods as fundamental methods in risk analysis. But there are some Advantages and disadvantages of both information risk assessment methods (as shown Table 1), [9]. Quantitative, where estimation of chance esteem is connected with application of numerical measures — esteem of resources is characterized in sums, the recurrence of threat occurrence within the number of cases, and helplessness by the esteem of likelihood of its loss, those strategies present results within the shape of the markers. Qualitative description of assets' value, determination of qualitative

scales for the frequency of threat occurrence and susceptibility for a given threat or: − Description of so-called threat scenarios by prediction of the main risk factors.

Table 1. Qualitative / Qualitative methods

	Quantitative Methods
Advantages	• It allows for the definition of the consequences of incidents occurrence in quantitative way. • The realizations of costs and benefits analysis during the selection of protections. • It obtains more accurate image of risks
Disadvantages	• Quantitative measures must depending on the scope and accuracy of defines measurement scale. • Analysis's results may not precise and event confusing • It must be enriched in qualitative description • Analysis conducted with the application of those methods is generality more expensive, demanding greater experience
	Qualitative Methods
Advantages	• It allows for the determination of areas of greater risk in short time and without bigger expenditures • Analysis is relatively easy and cheap.
Disadvantages	• It does not allow for the determination of probabilities and results using numerical measures • Costs benefits analysis is more difficult during the selection of protections

4. MULTI-CRITERIA DECISION ANALYSIS/ MAKING (MCDA/MCDM)

MCDM and MCDA are often used interchangeably [3] set forth seven guidelines in selecting a MCDM methodology [10]. Multi-Criteria Decision Analysis has a lot amount of use over last several decades. It is role in the different applications areas has increased significantly. MCDA methods are concerned with the task of ranking a finite number of alternatives.

Applying MCDA techniques in information security include the following Advantages: It can be used in the information security domain of risk-based decision-making, risk metrics associated with a triplet of threat, vulnerability, and consequences (TVCs) [10]. TVC are quantified in their natural units or on a constructed scale and integrated based on values associated with the importance of these metrics to specific goals.

- It has the capability to characterize risk in highly complex and uncertain situations are to move from the use of traditional risk assessment to risk-based decision -making that utilizes multi-criteria decision analysis (MCDA).
- Easier to compare alternatives whose overall scores are expressed as single numbers [11].
- Choice of an alternative can be transparent if the highest scoring alternative is chosen [12].
- Does not require the reduction of all criteria to a unit.

5. RELATED WORK

The content of this section consists of several works that suggest the framework for comparing information security risk analysis methodologies while assessing the way risks are valued and prioritized.

In [13], the authors particularly focus on how a system security state can evolve as an outcome of cyber-attack-defense interactions. This survey concerns how to measure system-level security by proposing a security metrics framework based on the following four sub-metrics: (1) metrics of system vulnerabilities, (2) metrics of defense power, (3) metrics of attack or threat severity, and (4) metrics of situations. To investigate the relationships among these four sub-metrics, the researcher propose a hierarchical ontology with four sub-ontologies corresponding to the four sub-metrics and discuss how they are related to each other.

In [14], the authors introduce a present decision-analysis-based methodology that measures risk, threat, vulnerability and outcomes through a lot of criteria intended to survey the general utility of cyber security the executives yet there is a requirement for practical, contextual investigation representing the way toward assessing and positioning five cyber security improvement systems options. The proposed system conquers any hindrance between risk assessment, and risk management, enabling an investigator to guarantee an organized and straightforward procedure of risk management alternatives.

In [15], the authors exhibit a technique dependent on granular processing to help leaders in investigating and to support decision makers in analyzing and protecting large-scale infrastructures, or urban areas from external attacks by identifying a suitable partition of the infrastructure or the area under analysis The technique takes a shot at a very constrained arrangement of data identifying with the vulnerabilities of segments, and the likelihood data in regard to how vulnerabilities can affect the significant segments and probability information regarding how vulnerabilities can impact the meaningful partitions.

In [16], the author introduces a handy guide of surveying digital dangers, a guide that underlines the significance of building up an organization and culture-explicit risk and resilience model. The analyst built up a structure for a Bayesian system to demonstrate the financial loss as a function of the key drivers of risk and resilience. The researcher used qualitative scorecard assessment to determine the level of cyber risk exposure and evaluate the effectiveness of resilience efforts in the organization. The researcher highlights the importance of capitalizing on the knowledge of experts within the organization and discusses methods for aggregating multiple assessments.

In [17], the authors look at an approach to determine that employments a set of weighted criteria,

where the security engineer design sets the weights based on the organizational needs and constraints. The approach is based on a capability-based representation of cyber security mitigations. The paper talks about a gather of artifacts that compose the approach through the focal point of Plant Science, inquire about, and reports execution comes about of an instantiation artifact. It doesn't investigate ways to join instability and affectability examination into the approach.

In [18], the authors propose the appropriation of an asset-driven viewpoint and a model-based approach to SECRA, the researcher distinguish current holes. In specific, , the researcher examine (i) CPS (security) modeling languages and methodologies, (ii) vulnerabilities cost models, and the network of public repositories of vulnerabilities, (iii) attacker models and profiles, and (iv) complex cyber-physical attack chain.

In [19], the authors propose a risk assessment method to enable the analysis and evaluation of a set of activities combined in a business process model to ascertain whether the model conforms to the security-risk objectives. To achieve this objective, the researcher use a business process extension with security-risk information to: 1) define an algorithm to verify the level of risk of process models; 2) design an algorithm to diagnose the risk of the activities that fail to conform to the level of risk established in security-risk objectives; and 3) the implementation of a tool that supports the described proposal

In [20], the authors propose a strategy for deciding and prioritizing the foremost fitting security controls or domestic computing. Using Multi-Criteria Decision Making (MCDM) and subject matter expertise, , the researcher recognize, analyze and prioritize security controls utilized by government and industry to decide which controls can substantively make strides domestic computing security. , the researcher apply our strategy utilizing cases to illustrate its benefits.

In [21], the author illustrates a part of Blockchain (BC) within the Internet of Things (IoT) could be a novel innovation that acts with decentralized, dispersed, freely and real-time record to store exchanges among IoT Hubs. The IoT hubs are distinctive kind of physical, but keen gadgets with inserted sensors, actuators, and programs and able to communicate with other IoT hubs. The part of BC in IoT is to supply a method to handle secured records of information through IoT hubs.

In [22], the authors illustrate a part of Blockchain innovation has been created for more than ten a long time and has gotten to be a drift in different businesses. As the oil and gas industry is steadily moving toward insights and digitalization, numerous expansive oil, to talking and gas companies were working on Blockchain innovation within the past two a long time since of it can altogether make strides the administration level, effectiveness, and information security of the oil and gas industry. This paper does a precise audit to talk about the application prospects of Blockchain innovation within the oil and gas Industry.

In [23], the author explores the number of threats to Blockchain which may concretely lead to a significant risk of adverse impact (thus Moderate or higher) is 76.47%. Fortunately, for some attacks, possible mitigations already exist. Nevertheless, for all the threats, and especially for the remaining 23.53%, it is imperative to examine continuously better approaches of relief and, where conceivable, anticipation. The paper does not examine the countermeasures of those vulnerabilities.

6. BLOCKCHAIN CYBER SECURITY ATTACKS

In this section, via KPMG member firms' in-depth experience, they've got known ten key risk classes related to Blockchain implementations [24]. A number of those risk dimensions are inter-dependent, driving the collective maturity of the Blockchain implementation. These dimensions conjointly take on completely different variations throughout the life cycle of a Blockchain. Also, the researcher address the related risk events to Blockchain technology (BT) which exploit weaknesses in their communication protocols, design, or implementation (see Figure 4) [24]. The vulnerabilities associated with BT classified (see Figure .5) [25], into three categories in the viewpoint of the Blockchain generation:

(a) The first- generation Blockchain 1.0.

(b) The second- generation Blockchain 2.0)

(c) The third- generation Blockchain 3.

The following is a classification of Blockchain risks:-

- Blockchain 1.0 And 2.0 General Risks
- Double spending.
- The 51% attack or Gold finger.
- Wallet security (private key security).
- Specific flaw in PoS .
- Network- level attack.
- Malleability attack.
- Real DOS attack against the Ethereum network
- Specific flaw in DPoS
- Block producers collude
- Exploit law voter turnout
- Attacks at scale
- BLOCKCHAIN 2.0 VULNERABILITIES
- Re‐entrance vulnerability (DAO attack)
- Parity multisig wallet
- King of the ether throne
- Governmental

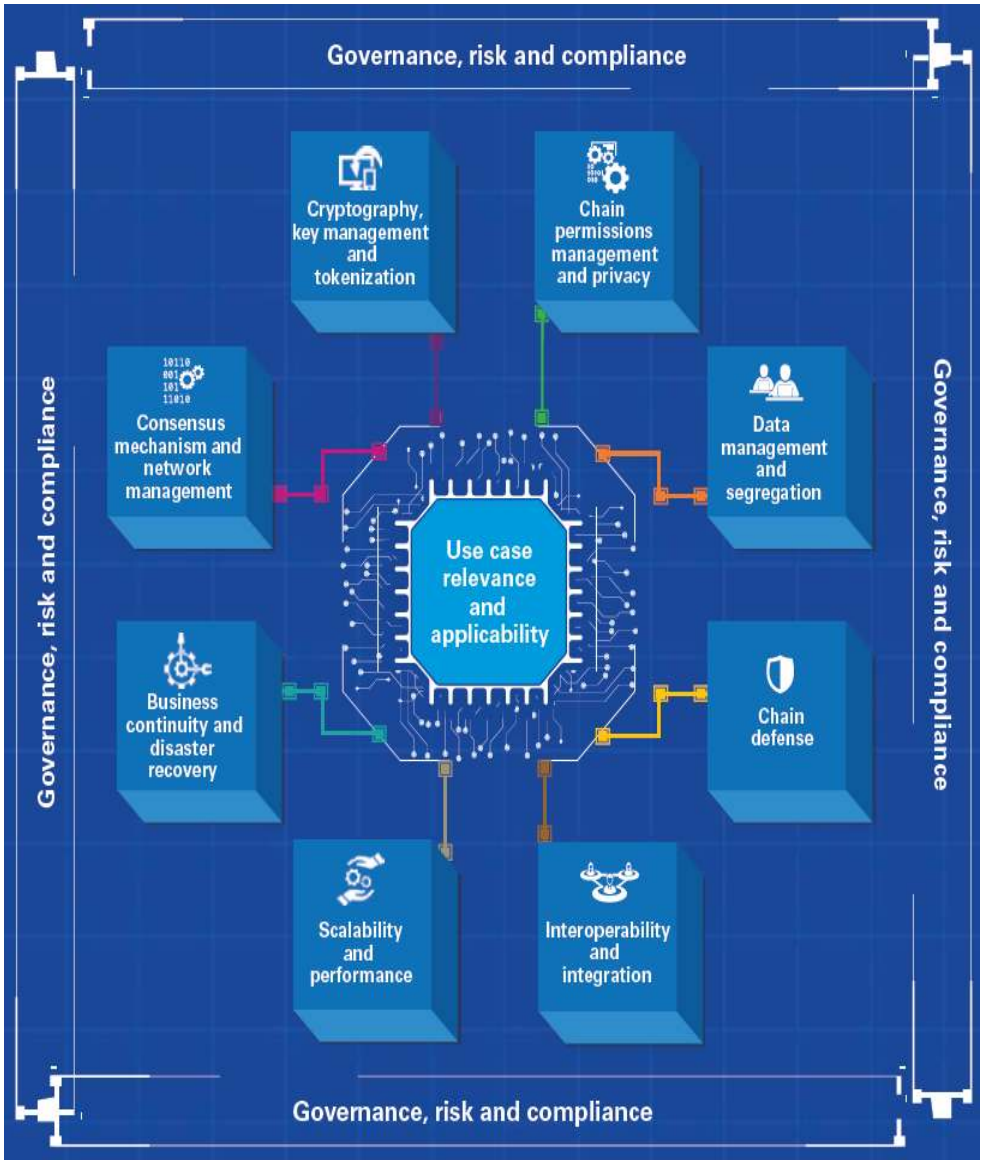

Fig 4. KPMG blockchain technology risk assessment framework — Key risk areas

- BLOCKCHAIN 3.0 VULNERABILITIES
- Attack against Hyper ledger Fabric
- Generals risk on private Blockchain implementation

These vulnerabilities in (see Figure.5) lead to the execution of the various security threats to the normal functionality of the Blockchain platforms.

7. CONCLUSION AND FUTURE WORK

This paper is trying to highlight the impact of Blockchain security function as well as other functions that may lead to threats. The paper explores the real attacks on the Blockchain systems. Also, it is crucial to understand the scope, and impact of security and privacy challenges in Blockchain to predict the possible damage. The future Blockchain researches still promising in different applications. One of the important research topic is Bitcoin because it's used on a daily basis in cryptocurrency transaction. Consequently, it will attract the industry and academia to conduct more researches. But there are other domains the researchers can use Blockchain Technology like (IoT, Healthcare, Voting mechanism) still has a remaining challenges and open research issues needed to be solved .The suggested Blockchain Technology future researches are: Healthcare , public sector ,Blockchain as a Service (BaaS) ,IoT, Energy-aware, large-scale applications, Smart Contracts, Consensus mechanisms

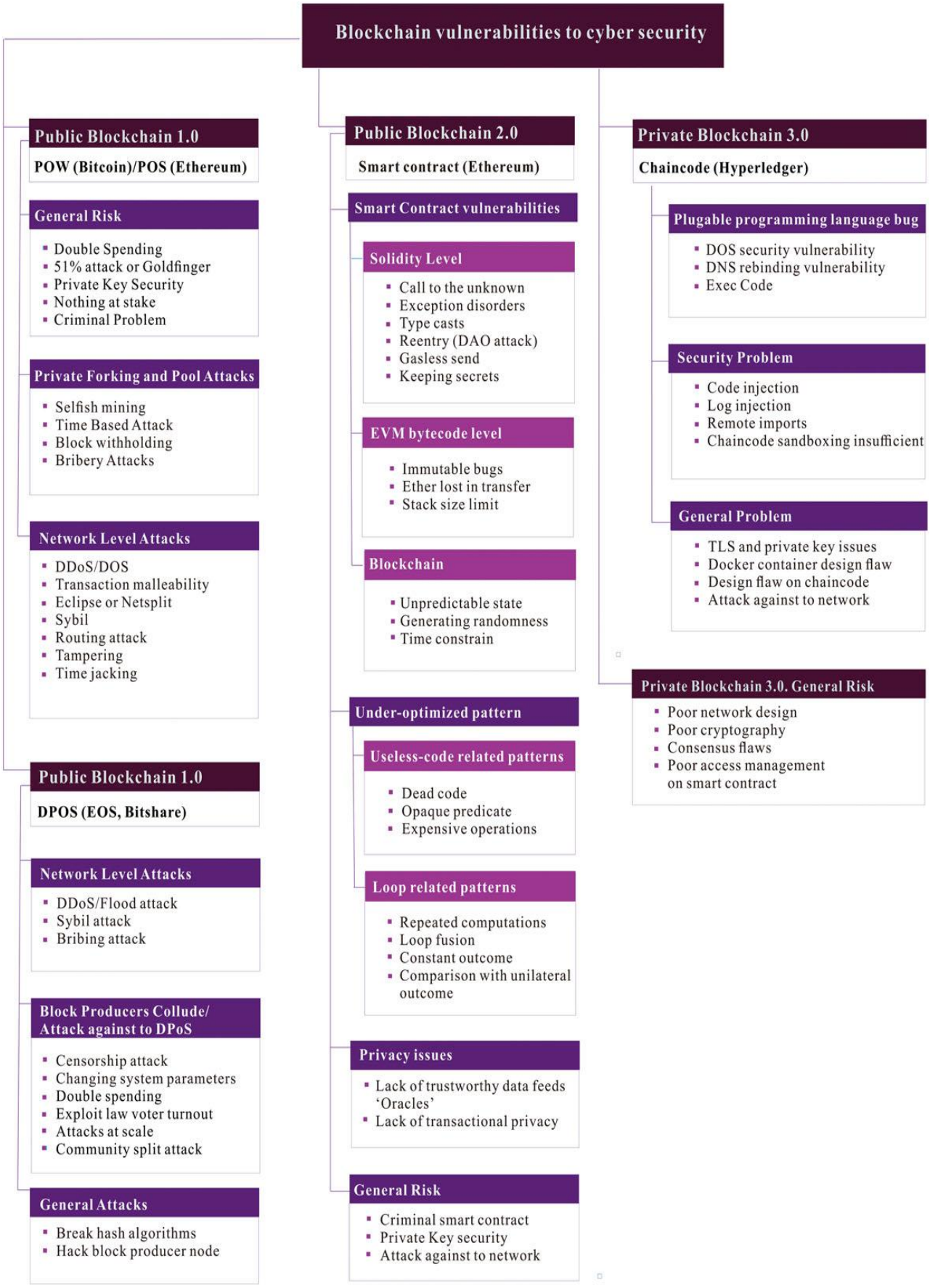

Fig 5: Blockchain vulnerabilities.

8. REFERENCES

[1] Turstwave Resource Library 2017,"Information Security Risk Assessment -Industry Best Practices to Keep Your DataSecure",retrievedfromhttps://www.trustwave.com/enus/resources/library/documents/evaluating-your-it-risk-assessment-process-does-it-stand-up-to-current-best-practices/.

[2] Legal News & Analysis, Asia Pacific Banking & Finance 2018.Break Through with Blockchain – "How Can Financial Institutions Leverage a Powerful Technology?" Retrieved from https://conventuslaw.com/report/break-through-with-blockchain-how-can-financial/

[3] Giacomo, M, Enrico S, Andrea B, 2018. Risk Assessment of Blockchain Technology .In 2018 Eighth Latin-American Symposium on Dependable Computing (LADC), 87 - 96.

[4] Information technology, security techniques, information security risk management, ISO/IEC 27005:2011.

[5] Alkhalifah, A. Ng, A Kayes, J Chowdhury, M Alazab 2019," A Taxonomy of Blockchain Threats and Vulnerabilities "retrieve from www.preprints.org.

[6] Deloitte 2018 .Risks posed by blockchain-based business models is your organization prepared? "Retrieve from https://www2.deloitte.com/us/en/pages/risk/articles/blockchain-security-risks.html.

[7] Merlinda A., Valentin R., David F., Simone A., Dale G., David J., Peter M.& Andrew 2019. Blockchain technology in the energy sector: A systematic review of challenges Renewable and Sustainable Energy Reviews, and opportunities – Elsevier, 100, 143–174.

[8] Claudio, L. 2018, 'Developing Open and Interoperable DLT/Blockchain Standards", Blockchain Engineering Council; IEEE Blockchain Standards Working Group, 106 - 111.

[9] Stroie E. R. 2011,"Advantages and Disadvantages of Quantitative and Qualitative Information Risk Approaches ", Chinese Business Review, Vol. 10, No. 12, 1106-1110.

[10] Alexander A. G.,Phuoc Q., Mahesh P., Zachary A. C,.Jeffrey M. K., Dayton M., & Igor L. 2017 'Multicriteria Decision Framework for Cyber security Risk Assessment and Management ",Wiley Online Library , DOI: 10.1111/risa.12891 .

[11] Linkov I, Satterstrom FK, Kiker G, Seager TP, Bridges T, Gardner KH, Rogers SH, Belluck DA & Meyer A. 2006."Multicriteria Decision Analysis: A Comprehensive Decision Approach for Management of Contaminated Sediments", Cambridge Environmental Inc. 26(1):61-78.

[12] Linkov I, Satterstrom FK, Kiker G, Bridges T, Ferguson E. 2006"From comparative risk assessment to multi-criteria decision analysis and adaptive management: Recent developments and applications", environment International ,Elsevier ,Vol 32, Issue 8, 1072-1093.

[13] M Pendleton, R Garcia-Lebron, JH Cho, 2016"A Survey on Systems Security Metrics "ACM Computing Surveys 49(4):1-35.

[14] AA Ganin, P Quach, M Panwar, ZA Collier 2017, "Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management", Wiley Online Library.

[15] Hamido Fujita Angelo Gaeta ,Vincenzo Loia ,Francesco Orciuoli, 2019 " Improving awareness in early stages of security analysis: A zone partition method based on GrC "Applied intelligence volume 49, pages1063–1077.

[16] Z Amin, 2019 "A practical road map for assessing cyber risk" Journal of Risk Research, Taylor & Francis.

[17] Thomas Llansó , Martha McNeil,Cherie Noteboom, 2019" Multi-Criteria Selection of Capability-Based Cybersecurity Solutions" the 52ndHawaii International Conference on System Sciences

[18] Marco Rocchetto ,Nils Ole Tippenhaue,20116 "On Attacker Models and Profiles for Cyber-Physical Systems" ,Conference: European Symposium on Research in Computer Security

[19] Ángel J. Varela-Vaca, Luisa Parody, Rafael M. Gasca1, María T. Gómez-López1, 2019" Automatic Verification and Diagnosis of Security Risk Assessments in Business Process Model" IEEE Access PP (99):1-1 .

[20] Justin Fanelli1, John Waxler ,2019" Prioritizing computer security controls for home users" Retrieve from https://peerj.com/preprints/27540/# .

[21] Tanweer Alam, 2019" Blockchain and its Role in the Internet of Things (IoT)". International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Volume 5 | Issue 1.

[22] Hong fang Lu, Kun Huang, Lijun Guo, 2019," Blockchain Technology in the Oil and Gas Industry: A Review of Applications, Opportunities, Challenges, and Risks", IEEE Access.

[23] Giacomo Morganti, Enrico Schiavone; Andrea Bondavalli, 2018,"Risk Assessment of Blockchain Technology" LADC 2018, 8th Latin-American.

[24] KPMG International, 2017. Securing the chain, retrieve fromttps://home.kpmg.com/xx/ena/home/insights/2017/05/ securing-the-blockchain-fs.html.

[25] Huru H., Ui-jun B., Mu-gon S., Kyunghee C., Myung-Sup K. 2019. A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. The International Journal of Network Management, Vol29, Issue2.1-36. Information Risk Approaches. Chinese Business Review, Vol. 10, No. 12, 1106-1110.