Risk Assessment of Blockchain Technology

Giacomo Morganti, Enrico Schiavone✉, Andrea Bondavalli
Department of Mathematics and Informatics, University of Florence, Florence, Italy
giacomo.morganti@stud.unifi.it,{enrico.schiavone, bondavalli}@unifi.it

Abstract— Recently, blockchain has attracted a great interest, and today it is considered not only as an innovative technology, but as a potential revolution for the world of business. The motivation of this enthusiasm is due to its capability of enabling new forms of records-keeping, transactions, and interactions between decentralized and mistrusting entities. Indeed, blockchain is driving companies to huge investments and strategic acquisitions, and it is raising innovation and research across industries and academia. However, besides the opportunities offered, this technology may expose institutions and interacting parties to new risks that have to be discovered, understood, and, where possible, eliminated or at least reduced. In this paper we identify the main threats of blockchain and assess their related impact. Then, applying a NIST-compliant approach, we perform a qualitative risk assessment. Finally, we review the possible countermeasures, where existing, for each threat analyzed, and discuss open challenges and future directions.

Keywords—Blockchain; Security; Risk Assessment; Threats.

I. Introduction

The term *blockchain* is especially used when talking about cryptocurrencies, between which bitcoin [1], 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 for 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 [2]. The potential impact attributed to the blockchain is so huge that is considered by many, not only a disruptive technology, but a real revolution for business, and society [2], [16].

The explanation of the general enthusiasm surrounding this technology, which in some cases can resemble a real fever, is its ability of empowering fully decentralized interactions between mistrusting entities, applications, and systems, making unnecessary the involvement of trusted intermediaries. Blockchains are actually decentralized and trustless databases of records, distributed applications or smart contracts that can be shared and executed among peers. Such technology provides key properties, including but not limited to: integrity, non-repudiability, pseudo-anonymity, fault tolerance as a consequence of redundancy, and transparency. Typical applications of blockchains are: financial services, ownership or provenance tracking of physical and digital assets, voting, etc.

Motivation. However, with the increasing use of blockchain, the number and severity of security accidents will go hand in hand. To give an idea of the seriousness of the damage, the analysis published in [45] estimates that, only in 2017, consumers in blockchain sector lost nearly 490 million dollars. The cause of the incidents were multiple, from wallet theft, to software vulnerabilities. Similarly, Blockchain Graveyard[1], which is a list of all massive security breaches or thefts involving blockchains, calculated from publicly available data that since 2011 there have been 58 incidents. The victims were mainly customers of cryptocurrency institutions which suffered from intrusions, credential reuse, account takeover or application vulnerability.

In our opinion, it is clear that security of blockchain technology is a really relevant and urgent issue. However, most of the security analyses existing so far in literature focus on specific cryptocurrencies as bitcoin [8], [9] or platforms as Ethereum. To our knowledge, there is a lack of works considering the blockchain technology as a whole and addressing also alternative blockchains. In addition, none of them performs a proper risk assessment, thus attributing the likelihood of occurrence of the threats, neither the impact nor a resulting risk.

Our Contribution. This work addresses threats which may adversely impact blockchains, not exclusively focusing on bitcoin's blockchain. Surveying the literature, and collecting information from websites reporting news about recently discovered blockchains vulnerabilities and accidents, we identify a list of the most relevant threats. For every threat source, we perform a qualitative risk assessment based on the methodology of NIST SP-800-30 [6]. The goals of this assessment are: (i) giving a broad view to users and designers on possible risks in adopting this technology; (ii) understanding strengths and weaknesses of a typical blockchain and how the latter may be exploited by attackers; (iii) exploring solutions and countermeasures, where they exist, to make the blockchain more secure and resilient. To our knowledge this is the first work applying a NIST compliant risk assessment to blockchain technology.

Paper Organization. The remainder of this paper is organized as follows. Section II discusses properties and technical aspects of blockchain technology, aiming at making the core of the paper understandable also for those readers not expert in this topic. It is especially focused on security relevant aspects. Related work is in the same section. Section III presents the risk assessment itself. Starting from the basic definitions from NIST, we introduce the assessment methodology, describe the threat agents, and list the threat events. For every threat event, we report a detailed analysis which motivates the attribution of the risk. Tables summarizing the assessment are in appendix at [50].

[1] https://magoo.github.io/Blockchain-Graveyard/

978-1-5386-8489-4/18/$31.00 ©2018 IEEE

Finally, Section IV concludes the paper and indicates future directions.

II. Background on Blockchain

In this section, we introduce the basic blockchain technological aspects constituting the background required to fully understand the contribution of the paper [1]-[3]. In particular, we focus on fundamental properties, and possible categorization of the blockchains. Then, we discuss and compare the most relevant consensus algorithms proposed so far, especially from the security and adversary tolerance aspects.

The blockchain is a technology characterized by a shared database (or ledger) distributed across a peer-to-peer network. The term recalls its structure, a chained sequence of blocks, where each block contains a set of transactions and, except for the first one called *genesis* block, it is linked to its predecessor by means of a cryptographic hash[2]. Blocks are linearly and chronologically added to the chain and they can be seen as links of a constantly growing chain, hence the name *blockchain*.

Each node of the network possesses a local replica of the blockchain, which is updated every time after appending a block to the chain. The process of committing a block takes the name of *mining*, and the nodes which are taking care of validating transactions, collecting them into blocks and appending the blocks on the ledger, are called miners. Nodes are typically independent peers capable of reaching an agreement on the status of the blockchain, that is, the latest block to be appended, without the involvement of any central authority. This agreement is called *consensus*, and there are many different algorithms designed for reaching it (some are detailed in Section II.B).

The first application of blockchain has been financial transactions of cryptocurrencies, known as *blockchain 1.0* [2], and Bitcoin [1] is the most widespread and famous implementation. More recent alternatives enable systems and applications to record other kinds of information on the ledger. One example is distributed applications or smart contracts, executed and shared among participating entities, in which case the transaction includes the result of a function call. The smart contracts can be self-executing, and for a general purpose, thanks to the Turing-completeness property provided in some cases, as for Ethereum [4]. These fundamental extensions of capabilities brought to the so-called second generation of blockchains, or *blockchain 2.0*.

A. Fundamental Properties

Hereafter, we describe the fundamental properties typically provided in every distributed ledger. However, their provision may be only partial for some categories of blockchains [39].

Immutability. Due to the presence of cryptographic hashes in the blocks, transactions stored in the distributed ledger cannot be later tampered, reversed, or deleted without altering the hash values, thus without being detected.

Integrity. Cryptography, together with algorithmic constraints, provides integrity on messages from users or between nodes and ensures that operations are only performed by authorized entities. In fact, Public Key Infrastructure (PKI) and digital signatures provide accounts identification and transactions authorization.

Non-repudiation. It is the ability to protect against the denial of an action, e.g., having originated a transaction [5]. In the blockchain context, its initiator digitally signs a transaction: in this way, the origin of every transaction is traced so that there is no dispute about it neither on their sequence in a distributed ledger. This property guarantees accountability of monetary expenditures, smart contracts executions, and so on.

Transparency. Each participating entity has access to the distributed ledger and can verify transactions without a central intermediary.

Decentralization. There is no central authority deciding on the recording of a particular data in the ledger or not. Also, decentralization avoids single points of failure.

Pseudo-anonymity. In general, each user can interact with the blockchain with a generated address. The address is a pseudonym which does not reveal the real identity of the user.

B. Consensus Mechanisms and their Comparison

The way nodes reach an agreement on the status of the ledger is one of the most important components of a blockchain: it affects security, as well as performance (as transactions throughput and latency), and scalability. A multitude of alternatives already exists, each with its own advantages and disadvantages. Table I gives a comparison between the mechanisms presented in the remainder of the paper, which are the most widely used state-of-the-art consensus mechanisms [39]-[43] highlighting their capability to tolerate adversaries.

Proof of Work (PoW). Every block contains a field named *header*, composed of metadata including, but not limited to, a timestamp and the hash of the previous block. Each miner node has to compute the header hash of the block to be appended. Solving this problem is not a trivial thing: the block header is constantly changing, and the value must be equal or smaller than a given value. However, when a miner produces the PoW, all other nodes can easily verify the correctness of the value. After that, transactions in the proposed block are validated by peers, to avoid frauds. If confirmed, the new block is added to the blockchain. This is a real competition since the calculation is a time and energy consuming process. Thus a reward is given to the winning miner. This is the algorithm used in Bitcoin and Ethereum blockchains, named Hashcash [3] and Ethash [4] respectively. Block interval depends on different parameter setting. In Bitcoin, a block is generated about every 10 minutes while in Ethereum about every 17 seconds. *Proof of Stake (PoS).* This algorithm requires the mining node to prove the ownership of some amount of cryptocurrency. The selection is based on

[2] A hash is a fixed length number derived from a given message or document.

[3] https://en.bitcoin.it/wiki/Hashcash

[4] https://github.com/ethereum/wiki/wiki/Ethash

TABLE I. A COMPARISON OF POPULAR BLOCKCHAIN CONSENSUS MECHANISMS [39], [40]

	PoW	PoS	BFT and variants	Ripple - Stellar Federated BFT
Trust model	Untrusted	Untrusted	Semi-trusted	Semi-trusted
Adversary Tolerance	< 51% of computing power	< 51% of stake (Depends on specific implementation)	< 33.3%	< 33% <20% faulty nodes in Ripple's UNL
Examples	Bitcoin, Ethereum	Peercoin	Hyperledger Fabric	Ripple, Stellar

stake size combined with a random factor or alternative solutions as coin age-based selection. PoS saves more energy and is more effective, while latency is shorter than PoW. However, the mining cost is close to zero and it may attract attackers (nothing-at-stake) [41]. Ethereum is testing its PoS algorithm with the project called Casper [51], a solution that proposes to: solve the nothing-at-stake problem [42], be tamper-proof, and offer protection against Sybil attack.

Byzantine Fault Tolerance (BFT) and variants. The so-called Practical Byzantine Fault Tolerance (PBFT) algorithm is the first solution to the problem of achieving consensus in presence of Byzantine failures[5], thus despite arbitrary behavior from some nodes. It uses the concept of replicated state machine and voting by replicas for state changes. This algorithm requires "3f+1" replicas to be able to tolerate "f" failing nodes. BFT-based blockchain offers a much stronger consistency guarantee, lower latency, higher throughput and it requires that all participants agree. Today, more than 700 variants and optimizations of BFT exist.

Ripple is based on the notion of Unique Node List (UNL). Every server s considers only votes of its own UNL to determinate consensus. The algorithm is divided in rounds and each round has four steps: 1) each server collects and insert all the transactions in a set of candidates; 2) each server joins the sets of its own UNL and vote about transactions genuinely; 3) transactions with minimum score go to next round, others are rejected; 4) Final round requires 80% of agreement the UNL of server s. Transactions that satisfy the requirement are added to the registry, which at the end is closed to compose a block of the chain.

Stellar and Federated Byzantine Agreement (FBA). Stellar Consensus Protocol (SCP) is a Ripple evolution and it is built for a Byzantine agreement. It is based on the concept of *quorum*, a set of nodes sufficient to reach agreement, and quorum *slices*, subsets that can convince one particular node about the agreement. A single node can appear on multiple quorum slices. Slices and quorums are based on real life business relationships between various entities thereby leveraging trust that already exists. FBA is divided into phases: initial voting, accept vote, ratifying and confirmation. Stellar FBA reaches global consensus in the entire systems if quorums intersect. Overall consensus is reached globally from decisions made by individual nodes.

Other popular consensus algorithms that we analyzed but we do not detail here because it is out of the scope of this paper are: Proof of Elapsed Time, Proof of Activity, Proof of Deposit, Proof of Burn, Proof of capacity, Tendermint, Quorum Chain, Raft Based Consensus, Multichain Consensus, BFT-SmaRT [39]-[43].

C. *Related Work*

A number of contributions analyze in detail single security issues specific for one blockchain as bitcoin [9],[13][18],[21],[23],[24],[27],[32], or Ethereum [10], [12],[22], or both [34]. Other works offer a more complete view on the possible threats for one platform [8] or another [15],[37]. To our knowledge, the unique works considering the blockchain technology as a whole and trying to consider the security issues not for a single implementation of blockchains are [25] and [49]. However, their contribution is limited to a small number of attacks. In addition, there are no works in literature which perform an assessment of the risks related to blockchain technology. Our analysis, surveys the most relevant threats, trying not to focus on a specific platform, assesses the risk related to each of the threats, and describes the respective countermeasures available so far or desirable in the future.

III. THE RISK ASSESSMENT

In this section we perform a qualitative risk assessment of blockchain technology, based on the methodology of NIST SP-800-30 [6].

The goals of this assessment are:

- Giving a broad view to users and designers on possible risks in adopting this technology;
- Understanding strengths and weaknesses of a typical blockchain and how the latter may be exploited by attackers;
- Exploring solutions and countermeasures to make the blockchain more secure and resilient.

A. *Definitions*

In order to describe the details of the risk assessment, we first introduce some useful definitions from NIST SP-800-30 [6].

- A *threat* is any circumstance or event with the potential to adversely impact a system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service. *Threat events* are caused by *threat sources*, i.e. hostile cyber or physical attacks; human errors of omission or commission; structural failures of organization-controlled resources (e.g., hardware, software, environmental controls); and natural or man-made disasters, accidents, and failures beyond the control of the organization.

[5] The loss of service delivery due to a Byzantine fault in systems that require consensus. Byzantine refers to the Byzantine Generals' Problem.

TABLE II. LEVEL OF RISK DETERMINATION, FROM NIST SP-800-30 [6].

Likelihood (Threat Event Occurs and Results in Adverse Impact)	**Level of Impact**				
	Very Low	**Low**	**Moderate**	**High**	**Very High**
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

- *Vulnerability* is a weakness in the system security procedures, internal controls, or implementation that can be exploited by a threat source.
- The *likelihood of occurrence* is a weighted risk factor based on an analysis of the probability that a given threat is capable of exploiting a given vulnerability (or set of vulnerabilities). The likelihood risk factor combines an estimate of the likelihood that the threat event will be initiated with an estimate of the likelihood of impact (i.e., the likelihood that the threat event results in adverse impacts). For adversarial threats, an assessment of likelihood of occurrence is typically based on: (i) adversary *intent*; (ii) adversary *capability*; and (iii) adversary *targeting*.
- The level of *impact* from a threat event is the magnitude of harm that can be expected to result from the consequences of unauthorized behavior.
- *Risk* is a function of the likelihood of a threat event's occurrence and potential adverse impact should the event occur. It is determined following Table II.

B. Assessment Methodology

Threat Sources. During the assessment, we choose to address adversarial threat sources only, as opposed to non-adversarial like human errors, structural failures or natural disasters.

Threat Agents. The characteristics of the identified attackers are summarized in Table III and this characterization is based on the Threat Agent Library (TAL) in [17].

- "Criminal Organization" (CO) represents an external attacker, with government level resources (e.g., a corporation, a terrorist organization or an adverse nation-state entity), and having good technological skills. This attacker maps agents 6, 7, 10, 15, and 18 in [17].
- "Hacker" (Hk) represents an external individual having high technological skills, and moderate/low resources. This attacker maps agents 5, 8, 14, 16, and 21 in [17].

In each of our assessments, we specify the threat agent that we consider most likely capable of conducting the attack. As an example, some threats involve the control of multiple nodes by the same entity, and we think it would be easier for a corporation as a CO having at its disposal more resources. On the other hand, other threat events require fewer resources but more capabilities, and those are the attacks for which we indicate Hk as threat agent.

TABLE III. ATTACKERS AND THEIR CHARACTERISTICS [17]

	Criminal Org. (CO)	**Hacker (Hk)**
Access	External	External
Resources	Government	Moderate
Capabilities	Operational	Adept

The threat events that we consider can be divided in the following four categories:

- Network Threats: *Distributed Denial-of Service (DDoS), Timestamp Hacking and Poison Pill, Sybil attack, Eclipse attack, Partitioning attack, Packet Sniffing, Delay attack or Tampering*;
- Double Spending Threats: *Majority attack, Malleability attack, Race attack, Finney attack, Vector 76 attack, Alternative History (or Brute Force);*
- Private Key Threats: *Wallet Theft, Man-in-the-middle (Address attack), Vulnerabilities in the Cryptography, ;*
- Smart Contracts Threats: *Criminal Smart Contracts, Vulnerabilities in Smart Contracts*;

In the following sections, we will rate the likelihood of occurrence as a combination of i) the likelihood that a threat is initiated, possibly related to the attack gain, and ii) the likelihood that a threat event, once initiated, will result in adverse impact. The likelihood of occurrence determination is based on authors' experience and confirmed by the CVSS framework [44]. This framework provides a way to capture the principal characteristics of a threat and produces a numerical score which can be then translated into a qualitative representation.

In our assessment, as proposed by NIST, the overall likelihood is expressed in a qualitative scale: *Very Low (VL)*, if the threat event is highly unlikely to occur and have adverse impact, *Low (L)* if it is unlikely, *Moderate (M)* if it is somewhat likely, *High (H)* if it is highly likely, *and Very High (VH)* if it is almost certain.

Impacts from threat events are determined considering (i) the characteristics of the threat sources that can initiate the events; (ii) the vulnerabilities/predisposing conditions identified, and (iii) the susceptibility reflecting the safeguards/countermeasures planned or implemented to impede such events. The assessment scale is Very Low (VL); meaning that the adverse effect is negligible; Low (L), if the impact is expected to be limited; Moderate (M), if the threat event is expected to have a serious adverse effect; High (H), in case of severe or catastrophic impact; and Very High (VH), if the threat event is expected to have multiple severe or catastrophic adverse effect.

The level of risk is determined as a combination of: (i) the impact resulting from the events; and (ii) the likelihood of the events occurring, as summarized in Table II.

C. *Network Threats Analysis*

In this section, we address threat events in blockchain networks which exploit weaknesses in their communication protocols, design, or implementation.

Distributed Denial-of-Service (DDoS)

This attack is characterized by an explicit attempt to prevent the legitimate use of a service. A Distributed Denial-of-Service (DDoS) attack deploys multiple attacking entities - constituting a botnet- to attain the goal, and is typically targeted to single point of failures. This type of attack is highly more complex to be conducted against a blockchain, thanks to the decentralized nature of this technology; in fact, by eliminating a middle man between the nodes of the network, the single point of failure disappears. Moreover, according to many sources (e.g., [46], [47]) a blockchain itself can be considered as a mitigation for DDoS, or even capable of making this attack obsolete. However, examples of successful DDoS already exist. Consider the mining competition in the bitcoin blockchain: to increase their chances of obtaining freshly mined bitcoins, miners typically join pools to collaborate on the computations. A mining pool may trigger a DDoS attack against an adversary pool to eliminate their chances of winning the next competition. In [9] authors empirically analyzed DDoS attacks, and documented 142 unique events against 40 Bitcoin services; they also found that 7% of all known operators were attacked.

Also blockchains 2.0, as Ethereum, suffered from DDoS attacks. One example is a computational DDoS [10]: an attacker took advantage of a combination of underpriced operations and not efficient client (known as *geth*) implementation to create "bad transactions". The effects were a reduction in the rate of block creation, meaning a slowdown in the network, and an increase of I/O on the clients, some of which were unable to synchronize with the blockchain. It has been fixed with a hard fork and changes in the protocol and gas costs, making the transaction spamming more expensive and ineffective [12].

All considered, the assessment is the following.

Attacker: Criminal Organization. Target: Adversary Mining Pool. Likelihood: High. Impact: Moderate. Risk: Moderate

Countermeasures: Proof-of-Activity (PoA) protocol, fast verification, signature based authentication [8], improve IoT devices security.

Timestamp Hacking and Poison Pill

In the Bitcoin blockchain, each node internally maintains a counter that represents the network time. This is based on the median time of a node's peers which is sent in the version message when peers connect. However, if the median time differs by more than 70 minutes from the system time, the network time counter reverts to the system time. An attacker could potentially slow down or speed up a node's network time counter, by connecting as multiple peers and reporting inaccurate timestamps. An advanced attack, known as Timestamp Hacking or Poison Pill would involve speeding up the clocks of a majority of the network's mining resources while slowing down the target's clock. Since the time value can be skewed by at most 70 minutes, the difference between the nodes would be 140 minutes [13].

In Ethereum, the timestamp of a block must be greater than that of the referenced previous block. Moreover, nodes need to have an accurate clock; otherwise they will not be able to connect to peers and to the network. As an example, if one node's time gets 12 seconds away from Coordinated UTC Time, its number of peers will reduce and eventually it will have zero peers and be disconnected from the network [14]. However, the timestamp of the block should not be used for critical components of the smart contract, as it can be manipulated by the miner [15].

In our opinion the impact of this attack is again *Moderate*, as for DDoS. The likelihood is Moderate, as this is just a potential attack, which occurrence has not been report in a real attack.

Attacker: Criminal Org. Target: Miners/Mining Pools. Likelihood: Moderate. Impact: Moderate. Risk: Moderate.

Countermeasures: Use the node's system time instead of the network time; tighten the acceptable time ranges, use only trusted peers [13], adopt NTP (Network Time Protocol) [8].

Sybil Attack

Distributed networks, especially where participation is open and peer nodes are anonymous or covered under pseudonym, are vulnerable to an attack known as "Sybil Attack" [19]. To disrupt the network, an attacker creates and controls a set of misbehaving nodes, making them seem like real independent ones. The goal is to isolate a user (hence a DDoS) from the honest network nodes and lay the foundations for the execution of other attacks. Some examples: (i) refuse to forward transactions originated by an honest node, which then are not confirmed by the network, and the input of those transactions could be reused for double-spending; (ii) prepare a timing attack, that is observing the transmissions directed to the attacker's ISP and originated from the victim, with the goal of overcoming the low latency encryption and anonymization of the transmissions [20].

In our opinion, the Impact is *High* because an attack of this kind may have relevant side effects as double spending, and

de-anonymization. The likelihood, however, is *Moderate*: to our knowledge no real cases of Sybil have been reported yet.
Attacker: Criminal Org. Target: User and blockchain network. Likelihood: Moderate. Impact: High. Risk: Moderate.
Countermeasures: In private blockchains (as well as in centralized systems) they can be avoided through heuristics: requiring that an individual IP cannot create too many user accounts in a given time interval. In Bitcoin the primary countermeasure is limiting the outbound connections to one IP address per /16 (x.y.0.0). Xim, which is a two party mixing protocol, is another possible mitigation [8].

Eclipse Attack

In typical blockchains, a node leverages on connections to its peers to get a full view of the network. With an eclipse attack, a malicious node obscures a user, taking control of all the connections originating from and targeted to the victim. This way, an attacker prevents the victim from obtaining full information about the topology of the network. An eclipse attack can be not only a way to co-opt the mining power of the network around consensus, but also useful in a double-spend attack. As an example, a customer can pay for a transaction and use the eclipse attack to obscure the receiver, preventing the latter from discovering the double spending. Researchers have demonstrated that conducting Eclipse attack against Bitcoin's blockchain [21] is feasible. More recently, also Ethereum has been discovered vulnerable to it [22]. In both cases the study proposed countermeasures, several of which have been incorporated in the respective upgrades. For this last consideration, the likelihood, nowadays, can be reduced to Moderate.
Attacker: Hacker. Target: Users. Likelihood: Moderate. Impact: High. Risk: Moderate.
Countermeasures: Typical countermeasures are (1) disabling incoming connections and (2) choosing 'specific' outgoing connections to well-connected peers or known miners (i.e., use whitelists) [21]. However, more sophisticated countermeasures are in [21] and [22].

Partitioning Attack

A partitioning attack (as known as BGP hijacking [25]) consists in deviating and cutting all the connections between a set of nodes and the rest of the network, in order to disconnect and isolate them. In [24], the authors describe how an attacker can verifiably isolate a selected set of nodes in the Bitcoin network hijacking the BGP[6] (Border Gateway Protocol) routing protocol. The procedure requires only the knowledge of the IP addresses of the nodes the attacker wants to isolate, thus can be conducted by a CO. The impact of a partitioning attack depends on the number of isolated nodes and on their mining power. Isolating a few nodes essentially constitutes a DoS attack. Disconnecting a considerable amount of mining power can lead to the creation of two different versions of the blockchain, with consequences as: block discarded, transactions reversed, as well as loss for the miners, risk of double spend and selfish mining attacks [24]. In this last case, the Impact is High. Likelihood is High as well, and its feasibility has been demonstrated in [24].
Attacker: Criminal Organization. Target: Users, Miners and Network. Likelihood: High. Impact: High. Risk: High.
Countermeasures: BGP security extensions, monitoring systems [25]

Packet Sniffing

An attacker capable of observing the Internet traffic of a node can monitor transactions, when they are received and forwarded, or sent, which means originated. Some existing clients for Bitcoin blockchain, as Bitcoin-QT, have good integration with Tor browser[7]. We assess the likelihood of this attack as *Moderate*, considering that some existing blockchains already integrate methods for data flow protection. The impact is *Moderate* as well, because the transaction content usually is not a sensitive information about the user [20].
Attacker: Hacker. Target: Single User. Likelihood: Moderate. Impact: Moderate. Risk: Moderate.
Countermeasures: The partial integration with anonymous communication systems (i.e., Tor) would reduce to a *Low* level the likelihood of tracking personal information on the blockchain, thus also the resulting risk would be *Low*.

Delay Attack or Tampering

A typical blockchain network assumes that information about mined blocks is broadcast to the other nodes and quickly reaches them. The goal of delay attack is to slow down this propagation. Studies which demonstrate the feasibility of this attack already exist: in [23], the authors proved that the adversary can reach the goal by introducing congestion in the network or making a victim node busy by sending requests to all its ports [8]. Similarly, in [24] the authors describe an attack procedure against Bitcoin in which the delivery of blocks is delayed by up to 20 minutes. This is obtained modifying some key messages while making sure that the connections are not disrupted.
This attack, also known as tampering [8], can lay the foundations for other subsequent threats as double spending or DoS.
Attacker: Criminal Org. Target: Users, network. Likelihood: High. Impact: Moderate. Risk: Moderate.
Countermeasures: possible mitigations are in [24], e.g., monitoring round-trip time (RTT), or using UDP heartbeats.

D. Double Spending Threats Analysis

This section describes the assessment of the most relevant threat events of double spending category. A *double spending* attack is the intentional creation of two conflicting

[6] Regulates how IP packets are forwarded to their destination

[7] https://www.torproject.org

transactions that attempt to spend the same funds in order to defraud a third party [18].

Majority Attack

This is a network attack (sometimes labeled 51% attack or >50% attack) which has been mentioned as a potential security issue also in [1]. In PoW-based blockchains, if a single organization is able to control the majority of the network mining power (in particular the hashrate). Doing so, it can attempt writing its own blocks, deciding which transactions are approved or excluded, their order, fork the blockchain, and perform several other types of attacks including double spending, eclipse, and DoS [25][8]. In PoS-based blockchains, the majority attack is also possible if a single entity owns more than 50% of the total coins in the network.

A majority attack is potentially feasible – especially with the rise of mining pools. However, it was more feasible in the past when most transactions were worth significantly more than the block reward and when the network hash rate was much lower and prone to reorganization with the advent of new mining technologies. A majority attack has never been successfully executed on the Bitcoin network, but it has been demonstrated to work on some small altcoins [26]. At current network mining difficulty levels, not even large-scale governments could easily mount a majority.

For these reasons we assess its likelihood as *Low*. Considering all the consequent attacks it can permit, the potential impact of majority attack is *High*. Thus, the resulting risk we obtain is *Moderate*.

Attacker: Criminal Organization. Target: Blockchain network, users, miners. Likelihood: Low. Impact: High. Risk: Moderate.

Countermeasures: insert observer nodes, communicating double spending alerts, discourage large mining pools [8].

Malleability Attack

The malleability attack belongs to the category of double spending attacks. In this case, however, the attacker is the receiver of a transaction, while the victim is the sender. The attacker would cause the latter to create a transaction that transfers some funds to a second address controlled by the attacker itself [18]. Then, the attacker modifies the identification hash without invalidating the transaction. The new transaction is then sent to the network, except from the nodes seeing the original transaction. Either of the two transactions may later be confirmed. A malleability attack is successful if the modified version of the transaction is later confirmed. The attacker would have effectively doubled the coins the victim sent it [18].

In Bitcoin, custom implementations were vulnerable [8] to this attack. As an example, in 2014, MtGox, once the largest Bitcoin exchange, closed and filed for bankruptcy claiming that attackers used malleability attacks to drain its accounts. Nowadays, however, the reference implementation is immune to malleability attack, so we assess the likelihood to *Low*.

Attacker: Hacker. Target: User. Likelihood: Low. Impact: Moderate. Risk: Low.

Countermeasures: Canonical signature, signature independent id, nonce [48]

Race Attack

In PoW-based blockchains, a race attack affects a vendor which accepts a payment before the transaction confirmation, just before that the same transaction is reversed. In fact, this attack can be performed by a malicious node which sends a payment to a recipient user, while a conflicting transaction addressed to the attacker's own account is broadcast to the network. The second transaction will likely be confirmed, mined into a block and accepted as genuine by nodes in the network.

This is not very elaborate attack, so can be conducted even by an attacker with minimal skills. Moreover, the authors of [27] show that the Bitcoin protocol allows a high degree of success by an attacker in performing race attacks. For the aforementioned reasons, we assess as *High* the likelihood related to this threat. Possible effects of a race attack are: loss of a product by a vendor, blockchain forks generation, as well as honest users being banned [8]. Thus, the impact is *Moderate*. The risk of a race attack is then *Moderate* as well. However, it cannot be eliminated: therefore, the cost/benefit of the risk needs to be considered when accepting payment on *0/unconfirmed*.

Attacker: Hacker. Target: Vendor. Likelihood: High. Impact: Moderate. Risk: Moderate.

Countermeasures: The recommendations in [27] for merchants include disabling incoming connections and to choose specific outgoing connections. Other countermeasures in the literature are [8]: inserting observers in network, communicating double spending alerts among peers, nearby peers should notify the merchant about an ongoing double spend as soon as possible.

Finney Attack

Similarly to race attack, the Finney attack is a double-spend attack which requires a vendor to accept unconfirmed transactions. It works as follows: in a PoW-based blockchain, an attacker is mining blocks occasionally. In each block mined, he includes a transaction which sends coins back to another of his addresses. But he does not broadcast the mined block (thus, neither the fraudulent transaction). In the meanwhile, the attacker buys an object or a service from the merchant, which eventually waits a few seconds to protect from other double spend attacks, then transfer the goods. Once the payment is accepted and the service is irreversibly provided, the attacker broadcasts his block, and the fraudulent transaction will take precedence over the other one and override the unconfirmed payment.

Attacker: Hacker. Target: Vendor. Likelihood: Moderate. Impact: Moderate. Risk: Moderate.

Countermeasures: merchants can take some precautions as waiting for multiple confirmations before accepting the payment and sending the product. The risk of a Finney attack cannot be eliminated, while the countermeasures would contribute to make this attack harder.

Vector 76 Attack

This attack, sometimes called also one-confirmation [8], combines race and Finney attacks to make reversable even transactions with one confirmation [29]. Because of this characteristic, in our opinion, the likelihood is slightly higher here, but this does not significantly change the result of the risk assessment, which is *Moderate* also in this case.

Attacker: Hacker. Target: vendors. Likelihood: Moderate/High. Impact: Moderate. Risk: Moderate.

Countermeasures: The countermeasures of race attack are applicable also here: (no incoming connections, explicit outgoing connection to a well-connected node). These actions significantly reduce the risk [28].

Alternative History (Brute Force)

This attack, also known as Brute Force [8], constitutes an advancement of Finney attack, as it may potentially work even if the vendor waits for n confirmations. However, it requires a relatively high hash rate, and causes high electricity consumption. The attacker controls multiple nodes in the network, which collectively mine an alternative blockchain fork. The fraudulent user sends the transaction to the seller, which after waiting for n confirmations provides the product or service. If the attacker has mined more than n blocks, releases the fork and obtains the coins back, concluding the double spend. Otherwise, the attacker can try to continue extending the fork or the attack fails.

The probability of success [30] depends on attacker's hash rate (as a proportion of the total network hashrate) and the number of confirmations the merchant waits for [28]. Performing a risk assessment is particularly difficult in this case, at least without making assumptions. Supposing the attacker disposes of high resources –the threat agent is a CO- the attack is potentially possible even if the vendor waits for multiple confirmations. In PoW-based blockchains of small size, with a total network hashrate relatively low, we assess its likelihood to a *Moderate* level, and consequently the risk becomes *Moderate* too.

Otherwise, in a blockchain of high dimension as Bitcoin, the assessment is the following.

Attacker: Criminal Organization. Target: Vendor. Likelihood: Low. Impact: High. Risk: Low.

Countermeasures: inserting observers in the network or notifying the vendor about an ongoing double spend [8].

E. Private Key/Wallet Threats Analysis

The private key of a blockchain user is critically important: it constitutes the credential for authentication. Since there is no TTP, if a user loses the key, irreversibly loses the coins. Moreover, if the key is stolen, it may be also cause of identity theft and account tampering. In fact, once a criminal steals the account, it becomes very difficult to track their behavior and recover the modified blockchain information.

Wallet Theft

Many users maintain their cryptographic keys with the help of wallets to store the cryptographic keys associated with the account. Most common of them are online or hosted software wallets, while other types of implementations have been proposed, as hardware, paper and brain wallets [8]. Their thefts can occur because of system hacking, bugs in the software, malwares [33], or incorrect usage. As stated in [32], many users have already lost their coins due to poor usability of key management and security breaches, such as malicious exchanges and wallets.

Even if recent studies are proposing more secure alternatives to software wallets, the usage of the latter ones is still high. Therefore, in general, the likelihood of a wallet theft is *High*, while the impact is *Moderate*, considering that typically one theft affects only one user. The resulting risk is thus *Moderate*.

Attacker: Hacker. Target: User. Likelihood: High. Impact: Moderate. Risk: Moderate.

Countermeasures: Possible solutions, apart from hardware wallets, are [8]: Password-Protected Secret Sharing (PPSS), and threshold signature based two-factor security.

Man-in-the-middle (Address Attack)

In some cases, the attacker does not target private keys directly. Instead, it acts as a “man in the middle,” altering the recipient address of a transaction before it is signed. The malware replaces it with the thief’s address. Victims who do not notice the replacement send the coins to the attacker [33]. A recently discovered attack of this kind, is an *Address Attack* directed against hardware wallets users [31]. As discussed before, hardware wallets are considered one of the most secure way of storing cryptocurrencies and protecting cryptographic keys. In fact, they eliminate attack vectors typical of Internet connections. However, in order to send funds or issue a receiving address, a hardware wallet has to be plugged in to an internet-enabled device, and researchers have discovered a vulnerability that affects them[8] at this stage. With a malware, the attacker can simply replace the code responsible for generating the receive address with its own address, causing all future deposits to be sent to the attacker [31].

In our opinion, the man in the middle attack for the purpose of address altering, has *High* likelihood, as it can be conducted in many ways, some of which have been already detected [31]. Again, the impact is *Moderate* because limited to the single victim. The risk is thus *Moderate*.

Attacker: Hacker. Target: User. Likelihood: High. Impact: Moderate. Risk: Moderate.

Countermeasures: Prevention strategies for man-in-the-middle, e.g., IDS (Intrusion Detection Systems).

[8] In particular, affects hardware wallets manufactured by Ledger

Vulnerabilities in the Cryptography

To authorize transactions, Bitcoin and Ethereum use the Elliptic Curve Digital Signature Algorithm (ECDSA). As well as SHA-256, also ECDSA is considered very strong currently, but this does not guarantee they might be broken in the far future. Moreover, mathematical complexity does not necessarily guarantee the security of a cryptographic algorithm when it is implemented in a real-world situation. Implementation can dramatically lower the security level [34]. And this may have a dramatic impact in private key security. In [34], the authors discovered a vulnerability in ECDSA scheme, through which an attacker can recover the user's private key because it does not generate enough randomness during the signature process.

Thus, the likelihood of breaking the cryptography is, in our opinion, *Very Low*, at least for the computational power available even for a CO. However, for this assessment we consider the likelihood of exploiting a vulnerability in the implementation of a cryptographic algorithm. It is slightly higher: *Low*. The impact, instead, is High because the vulnerability can cause the loss of private keys for every user of a blockchain with that particular implementation.

Attacker: Criminal Organization. Target: User. Likelihood: Low. Impact: High. Risk: Low.

Countermeasures: they are specific for addressing implementation related vulnerabilities. Some examples from [34] are: ladder implementation, uniform formulas, distinguishability for the points on the curve.

F. Smart Contracts Threats Analysis

Smart contracts are programs written in Turing-complete cryptocurrency scripting languages which enable general fair exchange without a TTP. This capability, however, can effectively guarantee payments also for committed crimes. In addition, they are prone to specific vulnerabilities not possible for blockchain 1.0. In this section, we address the threats that are emerging as most dangerous and diffused in the field of blockchain 2.0.

Criminal Smart Contracts

Smart Contracts can facilitate a range of malicious activities as the leakage of confidential information, theft of cryptographic keys, and various real-world crimes (e.g., murder, arson, terrorism, etc.) [25]. In [35], the authors propose an example of smart contract for password theft, which can be exploited for a fair exchange between contractor C and perpetrator P. C will pay a reward to P if and only if P gives a valid password to C. The entire transaction process can be done without any TTP involved. Authors show that their solution can be easily extended for conducting other malicious activities, as 0-day vulnerability transactions [25], [35].

Attacker: Criminal Organization. Target: User. Likelihood: High. Impact: High. Risk: High.

Countermeasures: Still an open research question [35], there is a need for policies and technical safeguards.

Vulnerabilities in Smart Contracts

As programs running in the blockchain, smart contracts may have security vulnerabilities caused by program defects. Authors of [36] conduct a systematic investigation of 12 types of vulnerabilities in smart contracts. In [37], the tool called Oyente is proposed to find 4 kinds of potential security bugs. The research highlighted that 8833 out of 19,366 Ethereum smart contracts are vulnerable. The 4 bugs are following: (i) transaction-ordering dependence; (ii) timestamp dependence, (iii) mishandled exceptions, and (iv) reentrancy vulnerability [25],[37]. The latter, is a vulnerability which has been exploited for attacking the DAO contract. Thanks to it, the attacker took 3 millions of ETH, causing and hard fork in order to cancel the effect of the attack and prevent the withdrawal of funds to the victims [38].

Attacker: Hacker. Target: User, Network. Likelihood: High. Impact: High. Risk: High.

Countermeasures: Usage of a tool for finding vulnerabilities, e.g., Oyente [37].

IV. Conclusions and Future works

Blockchain technology has already become one of the most interesting areas of research and the potential impact attributed to it is so huge that it is considered a revolutionary innovation. However, its growth and notoriety, especially driven by bitcoin, has attracted hackers and criminal organizations. According to our research, the number of threats to blockchains which may concretely lead to a significant risk of adverse impact (thus Moderate or higher) is 76.47%. Fortunately, for some of the attacks, possible mitigations already exist. Nevertheless, for all the threats, and especially for the remaining 23.53%, it is important to investigate always new ways of mitigation and, where possible, prevention. In particular, we think that the area of threats regarding smart contracts and blockchain 2.0 is the one which is more exposed to risks and as a future work we plan to investigate countermeasures for those vulnerabilities. Finally, future works include: (i) enriching the assessment with more attackers (e.g., insiders); (ii) comparing the results with real case studies, and (iii) considering additional blockchain types focusing on threats relevant to them.

Acknowledgment

This work has been partially supported by the projects TOSCA-FI (FAR-FAS 2014), and SISTER (POR FESR Toscana 2014-2020) both funded by the Tuscany Region.

References

[1] S. Nakamoto. Bitcoin: A Peer-to-Peer electronic cash system, 2008.

[2] M. Swan, *Blockchain: Blueprint for a new economy*. " O'Reilly Media, Inc.", 2015.

[3] Cloud Standards Customer Council, “Cloud Customer Architecture for Blockchain.” July 2017.

[4] G. Wood, Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper*, *151*, 1-32. 2014.

[5] Schiavone, E., Ceccarelli, A., & Bondavalli, A. (2017, August). Continuous Biometric Verification for Non-Repudiation of Remote Services. In *Proceedings of the 12th Int. Conf. on Availability, Reliability and Security* (p. 4). ACM.

[6] NIST. *Guide for Conducting Risk Assessments*. NIST SP-800-30, Rev.1, 2012

[7] Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review*, *34*(2), 39-53.

[8] Conti, Mauro, Chhagan Lal, and Sushmita Ruj. "A survey on security and privacy issues of bitcoin." *arXiv preprint arXiv:1706.00916* (2017).

[9] Vasek, M., Thornton, M., & Moore, T. (2014, March). Empirical analysis of denial-of-service attacks in the Bitcoin ecosystem. In *International Conference on Financial Cryptography and Data Security* (pp. 57-71). Springer, Berlin, Heidelberg.

[10] The Ethereum network is currently undergoing a DoS attack https://blog.ethereum.org/2016/09/22/ethereum-network-currently-undergoing-dos-attack/

[11] Transaction spam attack: next steps https://blog.ethereum.org/2016/09/22/transaction-spam-attack-next-steps/

[12] Defeating the Ethereum DDos Attacks https://medium.com/@tjayrush/defeating-the-ethereum-ddos-attacks-d3d773a9a063

[13] Timejacking & Bitcoin http://culubas.blogspot.it/2011/05/timejacking-bitcoin_802.html

[14] Connecting to the Ethereum Network http://www.ethdocs.org/en/latest/network/connecting-to-the-network.html#common-problems-with-connectivity

[15] Ethereum Smart Contract Best Practices. Known Attacks https://consensys.github.io/smart-contract-best-practices/known_attacks/

[16] D. Tapscott, A. Tapscott. Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world. Penguin, 2016.

[17] T. Casey, “Threat Agent Library Helps Identify Information Security Risks,,” White Paper, Intel Corporation, Sept. 2007.

[18] Decker, C., & Wattenhofer, R. (2014, September). Bitcoin transaction malleability and MtGox. In *European Symposium on Research in Computer Security* (pp. 313-326). Springer, Cham.

[19] Douceur, John R. "The sybil attack." *International workshop on peer-to-peer systems*. Springer, Berlin, Heidelberg, 2002.

[20] https://en.bitcoin.it/wiki/Weaknesses

[21] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, “Eclipse attacks on bitcoin’s peer-to-peer network,” in Proceedings of the 24th USENIX Conference on Security Symposium, ser. SEC’15. USENIX Association, 2015, pp. 129–144.

[22] Marcus, Y., Heilman, E., & Goldberg, S. Low-Resource Eclipse Attacks on Ethereum’s Peer-to-Peer Network.

[23] Gervais, A., Ritzdorf, H., Karame, G. O., & Capkun, S. (2015, October). Tampering with the delivery of blocks and transactions in bitcoin. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* (pp. 692-705). ACM.

[24] Apostolaki, M., Zohar, A., & Vanbever, L. (2017, May). Hijacking bitcoin: Routing attacks on cryptocurrencies. In *Security and Privacy (SP), 2017 IEEE Symposium on* (pp. 375-392). IEEE.

[25] Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2017). A survey on the security of blockchain systems. *Future Generation Computer Systems*.

[26] https://en.bitcoin.it/wiki/Majority_attack

[27] Karame, G., Androulaki, E., & Capkun, S. (2012). Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin. *IACR Cryptology ePrint Archive, 2012*(248).

[28] https://en.bitcoin.it/wiki/Irreversible_Transactions

[29] The vector76 attack. Originally in https://bitcointalk.org/index.php?topic=36788.msg463391#msg463391.

[30] Online calculator for the probability of success in Alternative History (Brute Force) double spending attack. https://people.xiph.org/~greg/attack_success.html

[31] Ledger Addresses Man in the Middle Attack That Threatens Millions of Hardware Wallets https://news.bitcoin.com/ledger-addresses-man-in-the-middle-attack-that-threatens-millions-of-hardware-wallets/

[32] K. Krombholz, A. Judmayer, M. Gusenbauer, and E. Weippl, “The other side of the coin: User experiences with bitcoin security and privacy,” in Financial Cryptography and Data Security: 20th International Conference, FC 2016, Christ Church, Barbados. Springer Berlin Heidelberg, 2017, pp. 555–580.

[33] P. Litke and J. Stewart, “Cryptocurrency-stealing malware landscape,” 2014.

[34] Mayer, H. (2016). ECDSA security in bitcoin and ethereum: a research survey. *CoinFaabrik, June, 28*.

[35] Juels, A., Kosba, A., & Shi, E. (2016, October). The ring of gyges: Investigating the future of criminal smart contracts. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (pp. 283-295). ACM.

[36] N. Atzei, M. Bartoletti, T. Cimoli, A survey of attacks on ethereum smart contracts (sok), in: International Conference on Principles of Security and Trust, 2017, pp. 164–186.

[37] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, A. Hobor, Making smart contracts smarter, in: The 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 254–269.

[38] V. Buterin, Critical update re: Dao vulnerability, 2016. URL https://blog.ethereum.org/2016/06/17/critical-update-re-dao-vulnerability/.

[39] M. Staderini, E. Schiavone, A. Bondavalli, A Requirements-Driven Methodology for the Proper Selection and Configuration of Blockchains, to appear in Proceedings of SRDS 2018, the 37th IEEE International Symposium on Reliable Distributed Systems

[40] Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., ... & Rimba, P. (2017, April). A taxonomy of blockchain-based systems for architecture design. In *Software Architecture (ICSA), 2017 IEEE Int. Conf. on* (pp. 243-252). IEEE.

[41] Zheng, Z., Xie, S., Dai, H. N., & Wang, H. (2016). Blockchain challenges and opportunities: A survey. *Work Pap.–2016*.

[42] Baliga, A. (2017). *Understanding blockchain consensus models*. Tech. rep., Persistent Systems Ltd, Tech. Rep.

[43] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. In *Big Data (BigData Congress), 2017 IEEE Int. Congress on* (pp. 557-564). IEEE.

[44] CVSS Common Vulnerability Scoring System SIG https://www.first.org/cvss/

[45] Nikhilesh De 2017. Hacks, Scams and Attacks: Blockchain's 2017 Disasters https://www.coindesk.com/hacks-scams-attacks-blockchains-biggest-2017-disasters/

[46] Cyber Security with Blockchain. Prevention of DDoS attacks with Blockchain technology

[47] Rodrigues, B., Bocek, T., Lareida, A., Hausheer, D., Rafati, S., & Stiller, B. (2017, July). A Blockchain-Based Architecture for Collaborative DDoS Mitigation with Smart Contracts. In IFIP International Conference on Autonomous Infrastructure, Management and Security (pp. 16-29). Springer, Cham.

[48] Transaction malleability in cryptocurrencies, 2016. https://iohk.io/blog/research/transaction-malleability-in-cryptocurrencies/

[49] Lin, I. C., & Liao, T. C. (2017). A Survey of Blockchain Security Issues and Challenges. IJ Network Security, 19(5), 653-659.

[50] Appendix of this paper. http://rcl.dimai.unifi.it/~enrico/blockchain-ra

[51] V. Zamfir, “Introducing casper the friendly ghost,” Ethereum Blog URL: https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost/