WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

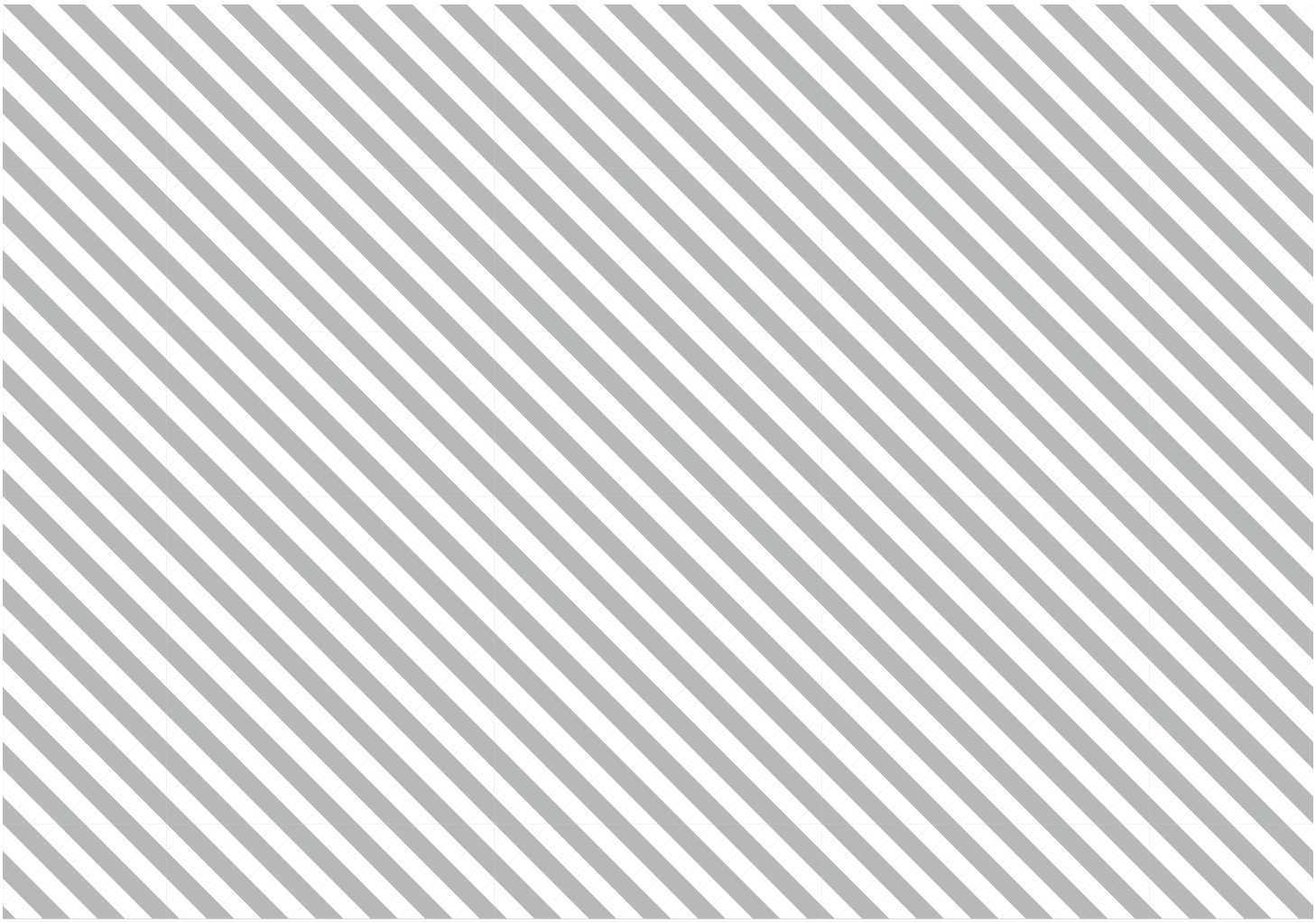
White Paper

Inclusive Deployment of Blockchain for Supply Chains

Part 5 – A Framework for Blockchain Cybersecurity

Prepared in collaboration with Hitachi

December 2019



World Economic Forum
91-93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland
Tel.: +41 (0)22 869 1212
Fax: +41 (0)22 786 2744
Email: contact@weforum.org
www.weforum.org

Contents

Preface

Adrien Ogée, Lead, Technology and Innovation, World Economic Forum (Centre for Cybersecurity), Switzerland

Nadia Hewett, Project Lead Blockchain and DLT, World Economic Forum (Centre for the Fourth Industrial Revolution), USA

Many organizations and supply chain solutions are exploring blockchain and distributed ledger technology (DLT) to drive cost efficiency, better product offerings and new market creation. The extent to which this new technology realizes its potential for organizations greatly depends on how well supply chain actors steward its deployment and development. Due consideration should be given to the critical success factors of deployment.

Security is an enabler, not a disabler. It is one of the foundations of digital trust and leads to sustainability by increasing immunity to cyberattacks. Securing an organization's blockchain solution is also critical to ensure that the benefits of blockchain technology remain inclusive.

Continuing the series, this white paper looks at one of the critical success factors of deployment – blockchain cybersecurity. The paper explores the considerations, proposed principles and recommendations for supply chain organizations and governments in managing the growing complexity of the security of blockchain solutions in support of global trade. It starts from the premise that an organization has already assessed whether there is a real business need to use blockchain.

This is the fifth white paper in a series and part of a broader project focused on the co-creation of a toolkit to shape the deployment of distributed ledger technology in supply chains towards interoperability, integrity and inclusivity. This paper aims to articulate, in simple terms, important blockchain and distributed ledger technology concepts as they relate to cybersecurity considerations.

Introduction

Digital trust is a prerequisite for blockchain technology to embrace its potential as a foundation of future international supply chain systems.

Trust is derived from clear expectations. As such, digital trust stems from predictability – the knowledge that the technologies we use will work as they should.

Predictability, in turn, is enforced by security.

Unfortunately, the hype around blockchain[1] has led to exaggerated security expectations that have affected trust in the technology. Many have believed its cryptographic foundation to be the ultimate answer to security. As a result, they have failed to implement the security controls required for trust in a blockchain to emerge. Conversely, security violations and volatility in crypto markets (e.g. hacking of crypto wallets and volatile coin prices) have adversely affected the brand of enterprise blockchains.

The reality is that, while blockchain technology does bring about a new security paradigm, it still needs to build upon traditional information security practices.

First, this paper investigates the security debate in blockchain technology and why both topics are so closely interlinked.

Second, it discusses the role of cybersecurity in supply chain applications of blockchain technology. It will answer important questions such as: "How can the main concepts of cybersecurity promote predictability in the use of blockchain technologies?"

Third, the paper looks at the blockchain technology stack to shed light on new components that require a new security paradigm.

The paper concludes by introducing a 10-step secure deployment guide, along with important security recommendations. These recommendations build upon a blockchain security risk management framework available in Appendices 1 and 2.

Blockchain is one type of distributed ledger technology. For simplicity, the terms are used interchangeably in this paper to cover all types of distributed ledgers. Furthermore, while the paper covers some distinctions between public and private chains, it focuses on more general considerations.

This paper does not examine the multitude of technical layers, complexities, hypotheticals and exceptions that exist within the blockchain space, especially as there can be vast differences between public and private chains, though the authors recognize their existence and importance.

While this paper can be read alone, basic blockchain concepts and blockchain features attractive for supply chain solutions are covered in the first World Economic Forum white paper in this series – for further reference see *Inclusive Deployment of Blockchain for Supply Chains: Part 1 – Introduction*, March 2019.[2]

1. Is cybersecurity necessary for blockchain?

The debate about blockchain security is polarized. At one end of the spectrum, blockchain technology is perceived to be inherently insecure and unfit for most use cases requiring privacy protections. At the other end, it is viewed as a cryptography-native and hence "unhackable" technology.

The truth lies somewhere in the middle.

There are grounds for the polarization of the blockchain security debate. Indeed, there have been documented security issues with various blockchain use cases, most notably cryptocurrencies and digital exchanges where anyone can trade fiat currencies, bitcoin and other alternative currencies.

Breaches have had an adverse impact on blockchain technology in general – whether for cryptocurrency or enterprise-related use cases.[3]

However, none of these attacks has targeted the fundamentals of blockchain technology. Rather, they have focused on its surroundings: software wallets used to hold digital currencies, codes of smart contracts and websites of digital exchanges.

CoinDash, an Israeli cryptocurrency portfolio management company, offers a telling example. In order to grow, the company sought to raise capital in 2017 through an initial coin offering (ICO) – the unregulated crypto equivalent of an initial public offering. On the day of the ICO, a hacker edited the company's website with a subtle change: he replaced the company's crypto wallet address, where the funds were supposed to be collected, with that of his own wallet. While there was no compromise of the blockchain technology itself, a simple website vulnerability was exploited to steal $7 million.[4]

Blockchain technology needs good security

Blockchain technology, including solutions based on it, is not infallible. Like any other technology, it has pros and cons related to security and can be hacked if the proper measures are not in place. Therefore, it is important that organizations do not store sensitive information on a blockchain without adequate security controls.

Security issues affecting blockchain technology are traditional for the most part and constitute a small number among thousands of cyberattacks around the world each day. Most news and media reporting on security-related topics with blockchain technology concerns the value of assets at stake and the limitation in recourse in the event of loss.

As of now, blockchain technology is considered quite safe. That said, it has not yet stood the test of time. Many algorithms and technologies were deemed secure for decades until a vulnerability was discovered.

Traditional information technology principles apply – the TradeLens example

Following the logic that blockchain builds upon traditional information technology, TradeLens, the industry platform developed by Maersk and IBM, obtained the information security certification of ISO/IEC 27000 series,[5] a respected and comprehensive certification maintained by a joint technical committee of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

In summary, the belief that blockchain technology is inherently insecure does not represent the complete picture, as most of the reported security issues have had more to do with overlooked traditional information security challenges than with technological flaws unique to blockchain technologies.

On the opposite side, more than two-thirds of enterprises believe that blockchain technology offers inherent security guarantees.[6] This line of thought is equally problematic, as it can lead to a lack of due diligence. Just looking at the list of blockchain-specific risks in Appendix 2 reveals the importance of due cybersecurity dilligence.

Digital-asset exchange Quadriga, for example, was managing $137 million in crypto assets, but failed to implement business continuity principles. When the chief executive officer passed away suddenly, no one could retrieve these funds.[7] What if the illusion of security led to poor business continuity practices in the shipment of military weapons or the traceability of precious stones?

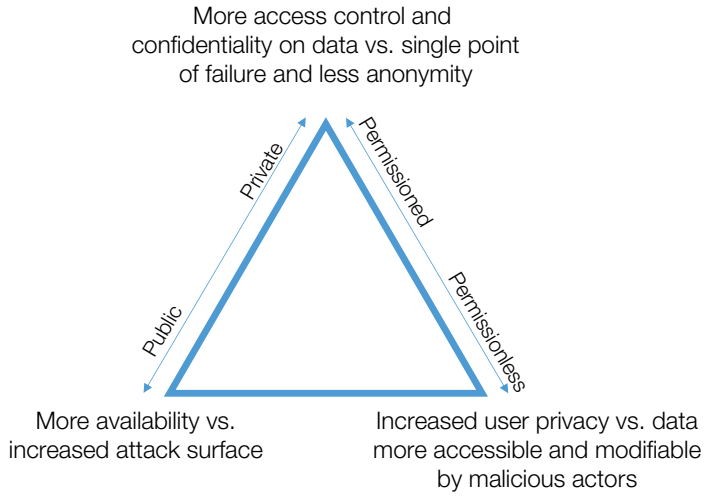
This is not to say that a blockchain does not offer any security advantages. It does. But its cryptographic foundation is not a security panacea. While it has its advantages, security is always a matter of trade-offs – and blockchain technology must be evaluated as one tool within a broader digitization toolkit.

Blockchain supports digital transformation

A blockchain brings to the digital era activities that were, or still are, paper-based, and hence prone to counterfeiting. In short, blockchain technology enhances and improves its impact on information security, and helps information security frameworks cast a wider net.[8] It can help to protect against information tampering such as altered invoices and false claims of arrival times in records. Supply chain disputes can cause large penalties for companies. For example, if a supply chain actor is responsible for the late delivery of a container and misses the terminal gate-in deadline, it pushes the arrival date back by a couple of weeks. That party can then be held liable for airfreight fees or other penalties. Using a blockchain as a single source of verifiable and secure information can help with dispute resolution in such cases where there is a need to know the real check-in time and which party is responsible for the delay.

2. Key cybersecurity concepts of relevance in blockchain

Figure 1: Trade-offs across various blockchain types



Cybersecurity is defined as the ability to protect or defend the use of cyberspace from cyberattacks.[9] There are half a dozen cybersecurity concepts that are particularly relevant when deploying blockchain.

Concept 1: Confidentiality
What it is: a security goal that aims to ensure only those who are authorized to access a piece of information can access it.

Application to blockchain: Different implementations of a blockchain offer varying degrees of confidentiality, but the general rule is that a blockchain might offer only the same level of confidentiality as a traditional database.[10] Public blockchains generally offer less confidentiality.

Concept 2: Integrity
What it is: a security goal that aims to ensure information is trustworthy and accurate.

Application to blockchain: DLTs are designed to guarantee integrity but depend on the quality of the data input: garbage in, garbage out. Take milestone updates provided by an ocean carrier to an importer while cargo is in transit: The accuracy of the estimated time of arrival (ETA) is not guaranteed because it is on a blockchain; integrity still depends on the input source, e.g. an IoT device tracking locations.

Concept 3: Availability
What it is: a security goal that aims to ensure data is available whenever needed.

Application to blockchain: While this pillar benefits from the fault-tolerance native features of blockchain due to its potentially distributed structure, real-time observation, critical for certain supply chain services, may be difficult to achieve for certain blockchain configurations.

Concept 4: The CIA triad
What it is: the combination of confidentiality, integrity and availability. Achieving all three security goals is challenging. This is not to say that information security cannot tackle the three goals, just that non-native goals will need to be retrofitted through security controls. More information about these three security objectives and their associated risks are available in Appendix 2.

Application to blockchain: In the example used above, to increase data integrity and availability of the ETA event, enabling more parties, such as the port, terminal and trucker, to access and verify the data will help. However, this approach may negatively affect data confidentiality as more parties have access to the data (see Figure 1).

Concept 5: Layered approach, so-called defence in depth
What it is: Inspired by the 17th-century French military architect Vauban, who developed a system of defences to improve the protection of fortified positions, is the idea that security benefits from a layered approach. This allows for the detection of unauthorized access long before a system's core is compromised. The results are security controls, e.g. measures taken in combination with each other to create a tight security net.

Application to blockchain: In the blockchain context, this translates into controls during multiple phases: from development to deployment and phase-out; and multiple layers from the node to the smart contract and access points.

Concept 6: Holistic security, design as a whole
What it is: Security controls need to be looked at from the perspective of the wider system, e.g. the military fortification as a whole, rather than each defensive wall or ditch.

Application to blockchain: The absence of technological convergence and standards makes blockchain system design difficult, and makes it more likely that developers will combine elements at the risk of their security features offsetting each other. Security governance then becomes more prominent: Who gets to decide what to do?

Concept 7: Security-by-design and by default

> **Often, I am in situations where I need to educate the client on security, since they would not have brought it up. Interestingly enough, investors also often ask about our approach to security.**

Hanns-Christian Hanebeck, founder and chief executive officer, Truckl.io

What it is: A natural extension of holistic security, security-by-design means that security has been embedded in the foundation of the system and is activated by default – rather than opted-in by end users.

Application to blockchain: There are numerous implications for blockchain, from embedding update features or kill switches into smart contracts to ensuring that security is considered at the very beginning of the life cycle of a solution. For example, at the early stage of the deployment such as proof-of-concept, some aspects of the incident response to a major risk can be tested. This will require implementing such security mechanisms as well as the necessary business operations.

Concept 8: Security as a process
What it is: Security is not a final destination but a process. It requires constant attention, as attackers continuously improve their skills, security researchers uncover new vulnerabilities, end users shift their habits and the technological spectrum grows.

Application to blockchain: While most vulnerabilities in such a nascent technology are yet to be found, the growth in popularity of DLTs will also be accompanied by a growing interest from hackers. Constant system monitoring and security risk management (see Appendix 1) will be vital to securing blockchains.

Concept 9: Security through transparency
What it is: For centuries, secrets were protected by obscuring them, which was called security through obscurity. The idea was that hiding the logic of a security system would prevent enemies from cracking it, e.g. encryption mechanisms to protect information such as industrial communications or copyright-protected media. Experts and users understand more about the advantage of transparency and open source technologies.

Application to blockchain: Modern security advocates the idea that the more transparent a system – the more open the internal logic of how information is protected – the better. The cryptographic algorithms used in DLTs are open-source; the mechanisms are widely tested and used by many industries.

Concept 10: Simple security
What it is: By extension, complexity is the enemy of security.[11] Securing complex systems made of complex parts, hosted in complex environments, is more difficult.

The Verge cryptocurrency implemented a mixture of mining algorithms: This extra complexity made it more difficult to effect security measures and ultimately allowed attackers to play one mechanism against the other to perform a 51% attack.[12]

Application to blockchain: Managing complex blockchain solutions with multiple interacting components will be difficult for chief information security officers – particularly as supply chain management is already complicated. As a result, whatever solution is deployed should seek to simplify operations rather than add complexity. The integration with legacy systems is a complexity driver that will require particular care.

3. Key blockchain concepts of relevance for cybersecurity

This section analyses the important concepts that blockchain introduces from a security perspective.

Concept 1: Decentralization
What it is: The transfer of authority away from a central source of power.

Cybersecurity implications: Security governance has traditionally been a centralized process, so decision-making can be executed quickly in critical situations. Decentralized governance is a paradigm shift that organizations transitioning to blockchain will need to navigate.

The direct consequences of decentralization are a decreased control over systems and oversight, as well as increased difficulty ensuring physical security and shutting down a system if need be. For example, ensuring the security of the DLT nodes may prove difficult when organizations may not even know which nodes are part of the distributed infrastructure.

In addition to decreasing the control of an organization, decentralization increases the attack surface of ledgers – given that, in most blockchain types, all of the nodes hold the same version of the ledger.

Decentralized security is therefore not trivial, and this shared responsibility can sometimes lead to a lack of due diligence: When it's everyone's responsibility, it is no one's.

Oracles, sources of data to be trusted

Oracles are entities outside of the blockchain feeding data to the system. They require a level of trust that is contradictory to the trustless and decentralized nature of blockchain-based protocols.[13] For example, whose responsibility is it to secure a tracking device used on a container or a GPS used to feed information to track-and-trace?

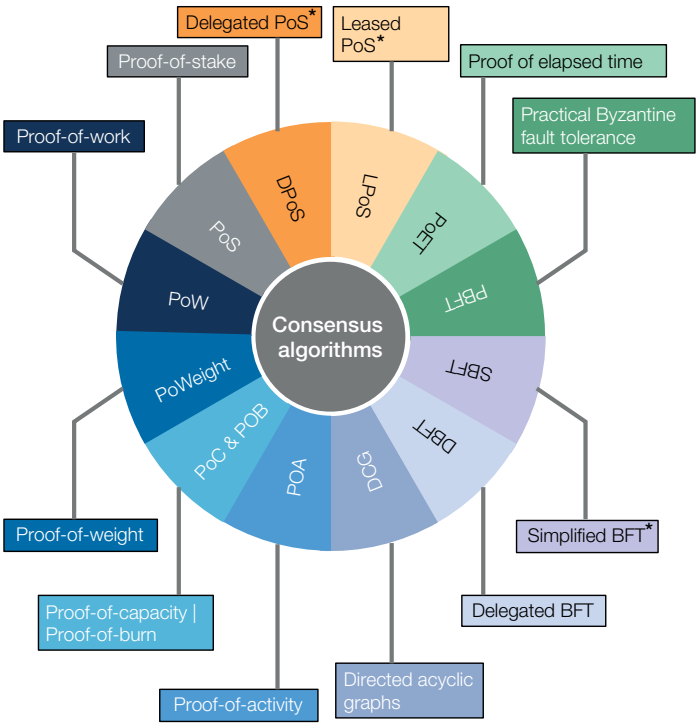
Concept 2: Consensus
What it is: Consensus mechanisms ultimately allow records to be added to the ledger. There are multiple consensus mechanisms that try to solve complex trade-offs, mostly across scalability, collusion resistance, computational cost and real-timeliness (see Figure 2).

Cybersecurity implications: Vulnerabilities in these mechanisms are significant as they could compromise the integrity of the ledger – and, consequently, the trust in the system. And their complexity is a real concern. Different consensus mechanisms lead to different requirements and levels of security. Some blockchains use multiple mechanisms to reach consensus. Security requirements must also consider these in conjunction with each other, as weaknesses may be amplified in this context.

Weak consensus system design

The Verge hack[14] did not exploit any vulnerability in any one of the consensus mechanisms that Verge was using, but rather a vulnerability in the system itself, which consisted of multiple consensus mechanisms added one after the other. Therefore, a lack of proper systems thinking was at the root of this case.

Figure 2: Examples of consensus mechanisms[15]



* PoS: Proof of stake – "BFT: Byzantine fault tolerance
Source: developcoins.com

Concept 3: Smart contracts
What it is: A smart contract is a computerized protocol that automatically executes the terms of a contract upon a blockchain once predefined conditions are met.

Cybersecurity implications: A smart contract is a double-edged sword – the contents are visible to all members of the blockchain, meaning that hackers can freely search for vulnerabilities. At the same time, where relevant entities agree on a smart contract that is immutable and observable by the public, exploiting vulnerability in a smart contract could be considered "fair use" in some cases.

Patching smart contracts is not as straightforward as patching a traditional piece of software, which is why secure coding and auditing are a must. However, the combined shortage of cybersecurity and blockchain talents makes securing smart contracts a real challenge.[16]

Concept 4: Endpoints and key management
What it is: Endpoints are the hardware and software elements used to access blockchains. While these are not entirely specific to a blockchain, the latter is the technology that is making their secure use mainstream.

Cybersecurity implications: Because blockchain technology employs cryptographic algorithms, blockchain users are generally required to create and manage cryptographic keys used to authenticate transactions and ensure a record is associated with a legitimate data-input agent. When a cryptographic key is compromised, a malicious record, e.g. status of cargos and expected arrival time, can be faultily associated with a user. Alternatively, a stolen secret key could be used to manipulate data used to determine who is liable for penalties (e.g. who is at fault for the late delivery of a container to the port, thus missing the gate-in and incurring late-ship fees). Ultimately, they still all use cryptographic keys, and so the securitization of these keys is of paramount importance across blockchains.

4. Blockchain secure deployment 10-step process

When a sound business assessment has been made that blockchain technology is an appropriate tool to address a real business need, an organization must pay careful attention to critical success factors of deployment, including security considerations. This section provides a 10-step secure deployment guide to navigate users towards a successful security practice.

Step 1: Acquire blockchain expertise

The first and probably most important step before considering a blockchain deployment is to acquire blockchain security talent. Depending on the company's resources, and the criticality and objectives of the blockchain use case, this can range from outsourcing to a trusted third party to hiring or training staff with the necessary skills to oversee a secure deployment.

Ensuring the security of a blockchain solution over time requires qualified employees. Beyond business criticality, the degree of internalization of this expertise will depend on the blockchain type. In the case of a consortium, for instance, it may be necessary to create a distributed security operations centre (SOC).

Given the recency of the technology's development, only a limited number of third-party security services and training materials exist. The landscape includes consulting firms and boutique companies as well as a few certification programmes, e.g. the Blockchain Security Professional certification of the Blockchain Training Alliance.[17]

It is worth noting that it may prove easiest to hire cybersecurity experts and train them in blockchain technology rather than doing the opposite.

End goal: the creation of a security oversight team that will be in charge of driving the next steps. It is essential that this team has access to the highest security authority in the organization, be it the chief information security officer (CISO), the chief information officer (CIO) or even the board. If the blockchain is to be developed for a consortium, it is recommended that the security oversight team count on security staff from all organizations that are members of the consortium.

Step 2: Define security goals

A sound security culture within the organization, with a clear understanding of security goals, is a prerequisite for the secure deployment of a technology with so many grey zones. This evaluates the security posture and security goals of the entire organization, not just the blockchain use case.

A good starting place is the organization's strategy, crisis management and business continuity policies. This step should answer some of the following questions:

- What are the major requirements of security from the CIA's point of view, and how are they prioritized?
- Is it important to ensure full anonymity of the organization's customers?
- How badly would the reputation of the organization be affected by an incident such as a system glitch or a data leak?

End goal: a document outlining important goals in simple language. These answers will inform the risk assessment outlined in Step 4.

Importance of security objectives – the Port of Valencia example

The Port of Valencia recently commissioned a blockchain solution to enable different entities working at the port to share data in a much more efficient way. Before developing a proof of concept, the leadership team defined the following high-level security objectives, among others:

- Data confidentiality is critical.
- The availability of the blockchain solution must be better than what we currently have.
- We must be able to identify all entities participating in the business network.
- The blockchain network must be compliant with the General Data Protection Regulation (GDPR).

Step 3: Choose the blockchain type

Depending on the business objectives and the security goals, choose which blockchain type would provide the best platform.

It is quite probable that the business rationale and functional specifications will inform this decision. While this is not security-by-design, it is the reality.

End goal: the creation of a document listing the security and business advantages and trade-offs of the various blockchain types considered.

Step 4: Perform a risk assessment

This step specifically concerns the blockchain use case to be developed. Please refer to Appendices 1 and 2 of this report, Blockchain risk management, and Key blockchain security risks, to perform the risk assessment. This step should conclude with a prioritized list of actions to manage the risks identified.

Threat and vulnerability assessment – Port of Valencia example

To better understand the risks of the blockchain solution it was considering deploying, the Port of Valencia had the opportunity to assess the security risks of a blockchain solution during its proof of concept.

Examples of the main potential vulnerabilities identified

- The case where an attacker rewrites the ledger by compromising a sufficient number of nodes. This will put the business network at serious risk.
- The administrator's secret key becomes accessible to other parties, who can then impersonate the administrator and even change the smart contracts.
- Node administrators are able to access confidential data stored in the node.
- The administrator leaves the company.

Examples of the main potential threats

- A competitor in the business network with administration rights to the node could be accessing confidential data from other companies in the ledger.
- Someone with administration rights can access the data stored in an external database in the node.
- Hacktivists could be drawn to the network.

In order to avoid using a partial and incomplete risk profile in a production environment, it is good practice to undertake this risk assessment as part of a proof of concept.

End goal: a document listing all of the risks and the different management strategies chosen.

Step 5: Define security controls

Security controls may be able to reduce risks before these residual risks are transferred, avoided or accepted. Please refer to the mitigation strategies presented in Appendix 2 for ideas on defining these controls.

End goal: a document listing the security functional specifications of the blockchain and recommended security controls for the development team.

Step 6: Define security governance

The security oversight team, structured in Step 1, is there to oversee the deployment of the blockchain solution, but not its long-term operation. As a result, it is critical for a governance structure and for processes to be defined prior to development kick-off. Once development starts, even a test version of the use case can be a source of security threats.

The governance processes will largely depend on the risks to be monitored. The more risks there are to manage, the more thorough the governance process will need to be. The more security controls there are to implement and monitor, the more staff will be required. The more distributed the risks, the more coordination with solution developers, operators, executive system owners and ecosystem participants will be required.

End goal: revised business continuity and disaster recovery plans.

Step 7: Choose a secure vendor

Choose the right security products and services, then evaluate vendors.

There are several established enterprise solutions out there, all offering some level of security service. In addition, boutique companies and consulting outfits can help.

End goal: one or more contracts with security vendors.

Step 8: Develop securely

Ensure that the developing team follows secure development practices, also known as DevSecOps, and in particular a secure software development life cycle (S-SDLC) methodology.

Secure SDLC ensures that security assurance activities such as penetration-testing, smart code auditing or architecture analysis are embedded in the development of the blockchain solution.

End goal: well-documented source code and planned security activities.

Step 9: Monitor and audit security

As explained in the first section, security is a process. New vulnerabilities are found, attackers become more creative, and thus security needs to be monitored actively.

First, regular penetration-testing of the infrastructure and applications that interact with the solution is essential. Auditing of smart contracts is also required to ensure that no vulnerabilities exist in the smart contract code, or are introduced by the contract's use. These penetration-testing and auditing processes should be ongoing and built into the blockchain solution's operation out of the life cycle.

Second, as previously covered, the security of a blockchain depends not only on the security of the blockchain itself but also on that of the underlying infrastructure that hosts the blockchain platform and solution components. As a result, it is highly recommended that you have a security operations centre (SOC) to monitor the blockchain solution along with the rest of the organization's assets.

There will be an increasing need for consortium blockchains to explore distributed SOCs, which are at present at the forefront of cybersecurity.

To verify its effectiveness, an independent audit, either internal or external, is periodically conducted so that the provisions of these vital steps are up to date and best fitted to the current system and environment.

End goal: active monitoring of the blockchain solution in the SOC.

Step 10: Respond to incidents

Whenever security monitoring activities detect an incident, you need to be able to respond to the incident and attempt to mitigate any damage in a timely fashion. After an incident occurs, it is essential to undertake a post-mortem assessment to improve the overall security posture of the solution and limit the risk of the incident reoccurring. Indeed, while incidents can be sources of disruption, they are also welcome opportunities to build the resilience of your blockchain and organization.

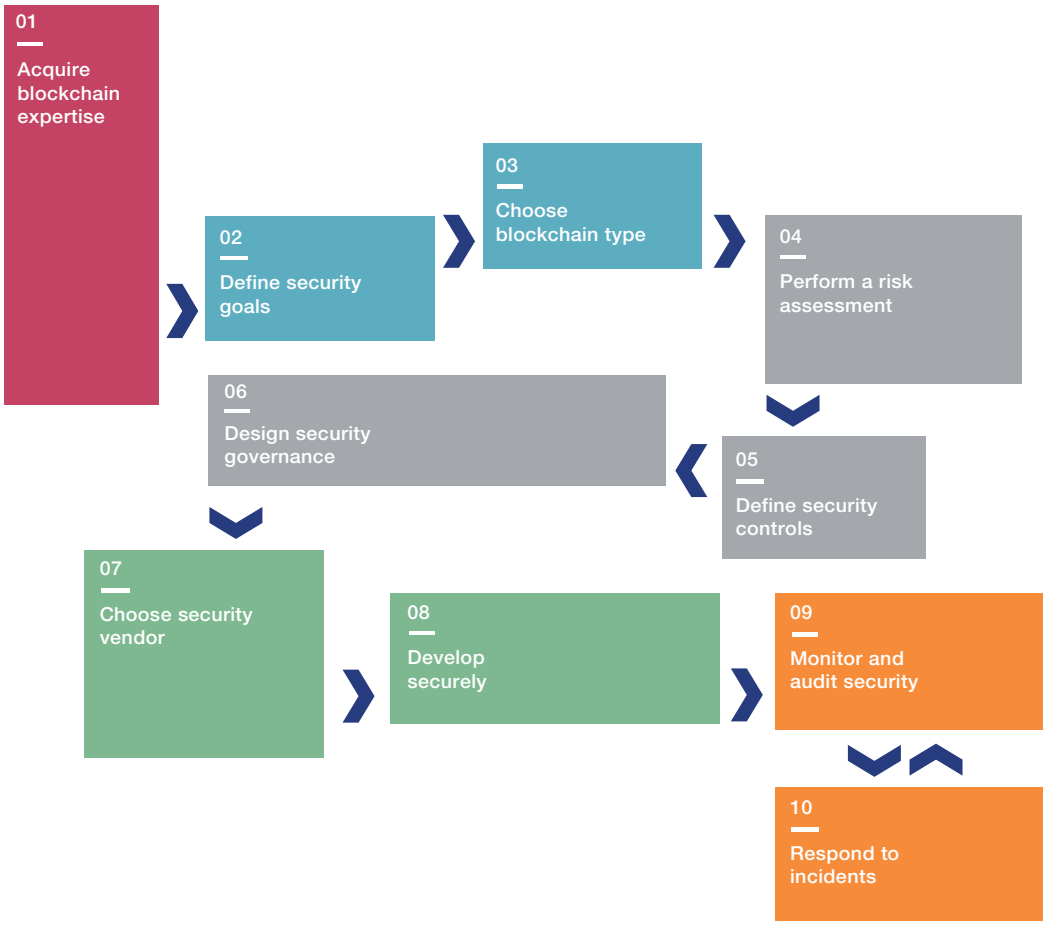
We believe there is no need to have blockchain-specific incident response plans or business continuity plans. Blockchain is a technology like any other, and so it is wiser to integrate blockchain-specific procedures into the organization's existing security plans.

Finally, in the words of the German poet Heinrich Heine: "Experience is a good school, but the fees are high." It is of the utmost importance to conduct an incident-response exercise before such an event occurs.

Training staff to respond to such incidents and testing distributed decision-making processes is critical to managing real incidents and keeping blockchains secure.

End goal: timely mitigation of security incidents.

Figure 3: Secure deployment 10-step process



Conclusion

Blockchain, perhaps more than any other technology, requires cybersecurity to protect the digital trust on which it relies.

While traditional cybersecurity does apply to blockchain, the technology also introduces unique features that require unique security measures. On top of that, blockchain is also a divergent technology: it is a moving target that requires a continuous and agile security process, rooted in field-tested security concepts.

In summary, this paper discusses these major topics and shares useful concepts:

– A blockchain is neither unhackable nor inherently insecure. There are industrial efforts towards good security practices to counter risks that appeared in the past (see Section 1).

– There are security concepts and design approaches that are particularly relevant to blockchain, e.g. defence in depth, holistic security and security as a process (see Section 2).

– There are also unique blockchain features that need to be accounted for in security design, e.g. decentralization, consensus, smart contracts and endpoints (see Section 3).

– Based on traditional information security management, a 10-step process for secure deployment guide will navigate users and other stakeholders to a successful practice (see Section 4).

It is important to note that, while introducing security techniques is critical to increase immunity to cyberattacks, it is not enough.

Blockchain solutions have been, and will be, attacked. Long-term sustainability will necessarily require an ecosystem approach at the business layer. This is probably the biggest challenge that blockchain poses to cybersecurity practitioners. Security has always been a centralized affair and breaking the discipline open, from egosystems to ecosystems, will require a paradigm shift based on an inclusive approach.

If blockchain is the technology that can bring multiple stakeholders to the platforms of the future, it requires a platform to discuss its own future today.

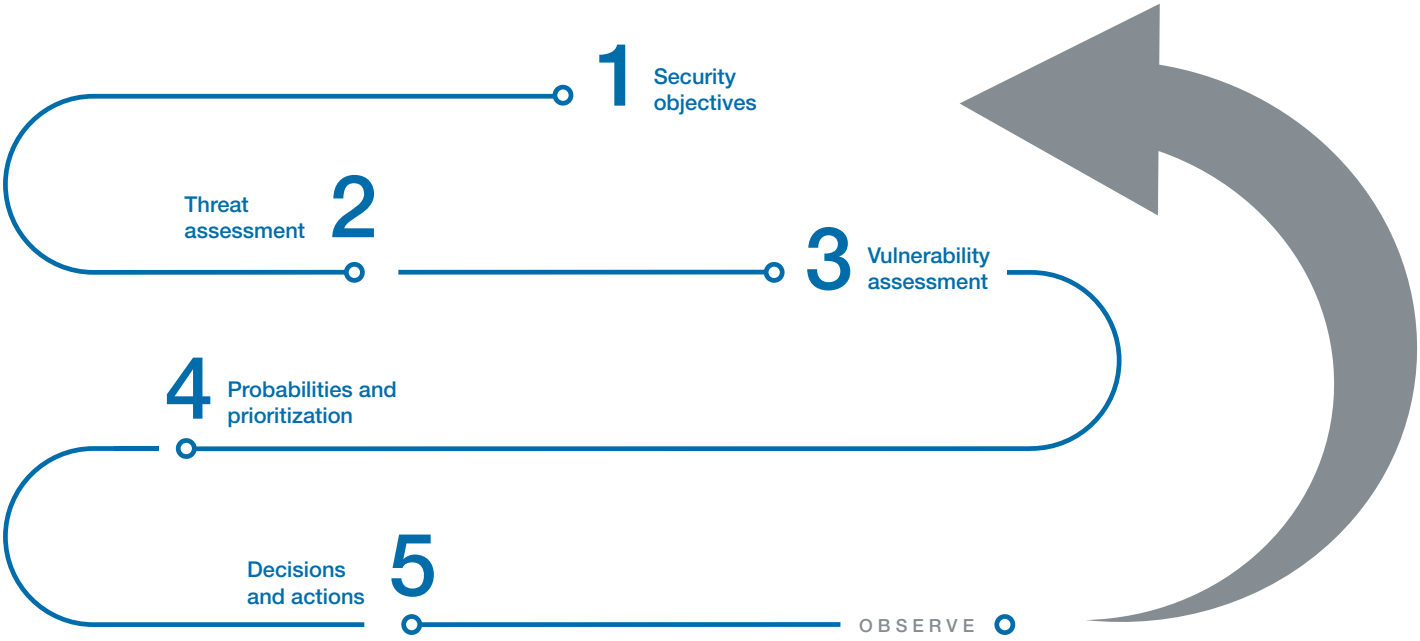
The World Economic Forum is such a platform, where an inclusive and multistakeholder approach can emerge, where new forms of co-option can be defined, and where an open dialogue with regulators and civil society can happen.

Appendix 1: Blockchain security risk management

Deploying a blockchain solution securely requires a sound risk-management process. The following paragraphs provide guiding principles on how to approach this task.

What is a risk? A risk is defined as the probability that a threat uses a vulnerability resulting in a given impact.

Figure 4: Risk management process



Step 1: Security objectives

The first step is to determine the security objectives based on the blockchain use case objectives. Questions that should be considered at this point might include:

- Should the blockchain offer more availability or confidentiality?
- Should anyone be able to mine on the chain or not?
- Should anonymity be guaranteed?
- To what extent would the blockchain use case depend on risks facing other upstream or downstream actors in the supply chain?

Such security objectives will inform much of the risk assessment and subsequent risk management decisions.

Step 2: Threat assessment

After this initial phase, a threat assessment is advised to determine what the system will need to be protected from, ranging from human accidents to natural catastrophes and deliberate cyberattacks. A threat is generally broken down into two components: capability and intent.

Depending on the sensitivity or the type of information stored on the blockchain – for instance, financial information – threats may in turn include cyber criminals but not hacktivists or nation-state actors. All of these factors pose different security challenges and require different controls.

During a threat assessment, it is important to consider the entire blockchain use-case environment. For example, a particular user of the system, such as a city or an NGO, may be a prime target of certain threat actors. In the supply chain context this is very important, given the potential diversity of users up- and downstream.

Differentiating between threats through capabilities and intent is a good way to measure the potential for disruption. For instance, a government agency may have capabilities but no intent to attack a particular blockchain. Hacktivists, by contrast, may be interested in harming the reputation of a particular organization, but lack the ability to overcome certain security barriers.

Step 3: Vulnerability assessment

The next step is to assess potential vulnerabilities in the system, processes, organizational framework, etc. Questions that should be considered at this point might include:

- What weaknesses am I introducing through storing my data in a public blockchain?
- How vulnerable would a custom-made hash algorithm be compared to an established industry standard?
- How difficult would it be to decentralize security governance?
- What are the weak points in my smart-contract auditing process?
- How exposed is my blockchain to physical attacks?

Finding vulnerabilities is difficult, and organizations at large should regularly perform penetration-testing, with total knowledge of the blockchain construct (white-box penetration-testing), partial (grey box) and without any (black box).

Defining a process early on to secure smart contracts is critical, as blockchain security expertise is scarce and in demand. It is also important to consider cost factors. An often overlooked vulnerability is not being able to cover the costs associated with a particular mitigation strategy.

Step 4: Probabilities and prioritization

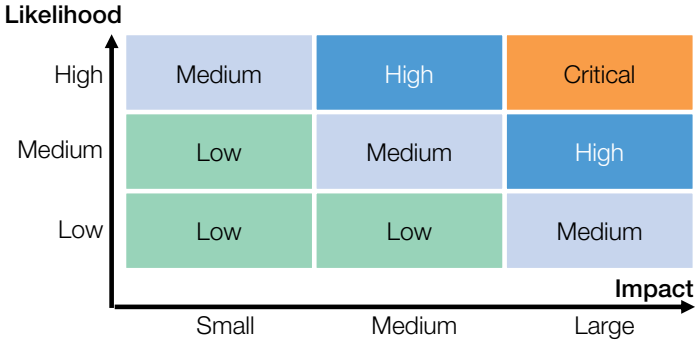
The next step of the risk assessment is to determine risk probabilities and impact.

Given the security objectives defined in the first step, which threats are likely to exploit significant vulnerabilities to cause significant impact?

The impact of a single point of failure in a membership service provider being entirely burned down could have a potentially significant impact on business process operations. As a result, this risk should be considered likely and impactful, and hence mitigated accordingly.

This prioritization exercise needs to be presented in a simple format to help leadership identify high-probability, high-impact risks that would indeed need to be mitigated.

Figure 5: Criticality estimates by likelihood and impact



Step 5: Decisions and actions

Once risks have been identified and prioritized, the last step of the risk-management process is to decide what to do with each of them.

Ideally, the outcome of this process would be the absence of residual risks, but in practice this is hardly ever achieved. Risks can either be mitigated, avoided, transferred or accepted.

Mitigating or reducing a risk consists of adopting various strategies to tackle either a particular threat – through deterrence, for instance – or a particular impact, through containment strategies.

Example: To mitigate the single-point-of-failure challenges posed by a membership services provider of a private chain, one could distribute it over multiple geographies and organizations.

Avoiding a risk consists of reworking the systems approach in order to eliminate a specific security challenge entirely. It generally involves trade-offs and accepting the removal of certain functionalities or users.

Example: If guaranteeing on-chain anonymity poses regulatory risks that would be impossible to mitigate and too costly to accept, it may be more logical to drop the feature of on-chain anonymity in favour of security.

Accepting a risk consists of acknowledging the existence of that risk and budgeting for it should it materialize.

Example: Should a private chain guarantee a maximum transaction confirmation time through a service-level agreement, it may be more cost-efficient to budget for the low probability that this performance objective may not be met, rather than invest time and money in developing an advanced load balancing or DDoS protection mechanism.

Transferring a risk consists of involving a third party, such as an insurance provider or an external provider. Due to the complexity of blockchain, using external expertise to develop a solution, and another entity to review and audit its results, is highly recommended.

Example: Given that the costs of a leak of personally identifying information can bankrupt a company, it may be worth investing in cyber-risk insurance coverage.

All of these steps enable those deploying a blockchain solution to involve leadership in prioritizing the right security controls and then budget accordingly. Security is a process, but so is risk management. Revising risks that the blockchain use case is facing needs to follow a continuous process.

Appendix 2: Key blockchain security risks

Below is a list of the main blockchain security risks, scored per blockchain type. For each risk, the paper provides a series of mitigation strategies should an organization not be in a position to accept, avoid or transfer the risk.

These risk evaluations, being either Critical, High, Medium or Low, are comparable evaluations only within each chart, yet it is the authors' intention that all of the charts should appear equal with respect to the levels across topics. This cannot, however, be universally valid as each case is sensitive to many factors such as use cases, system and platform configurations, design options, implementations, prioritized security goals and relevant management and processes. The aim therefore is to provide an understanding of the top view of demonstrative security risks so that conversations with experts can be conducted quickly and easily.

Confidentiality: The risk that information is fraudulently accessed or inferred from the blockchain tends to be higher for public blockchains, which are more easily analysed. On the other hand, anonymity, a sub-property of confidentiality, may be more difficult to achieve in private or permissioned chains for which identity must be proven. For example, hacking a membership service provider could lead to a breach of confidentiality. It is therefore important to clarify what needs to be confidential: the identity of the parties or information about their transactions?

Mitigation strategies:

- Avoid storing sensitive or private data on a blockchain.
- Consider off-chain storage for sensitive or private data.
- Encrypt information stored on ledgers whenever possible.
- Use advanced cryptographic techniques, such as zero-knowledge proofs and homomorphic encryption.
- Consider that anonymity is superior in permissionless blockchains than it is in permissioned ones, while data confidentiality is superior in private as opposed to public blockchains.

	Public	**Private**
Permissioned	High	Medium
Permissionless	High	Medium

Endpoint and key management: Endpoint security, which is closely related to confidentiality, is a common concern over all types of blockchain solutions. A large part of endpoint security refers to protecting a user's cryptographic keys to access the blockchain.

Permissioned chains warrant better know-your-customer (KYC) protocols and hence offer more opportunities to manage endpoint security.

In public chains, because information is available to anyone, particularly if unencrypted, it is easier for attackers to know which users and endpoints to target.

Mitigation strategies:

- Raise user awareness on security risks associated with storing keys improperly (on an email or webmail, on the cloud, without encryption etc.).
- Actively seek validation that users are aware of the risks they run based on the different options they use to access the chain and what they forfeit if their endpoint security is weak.
- Consider making security updates mandatory for users to be allowed to transact on-chain.

	Public	**Private**
Permissioned	High	Medium
Permissionless	Critical	High

Integrity: The risk that the ledger is fraudulently tampered with is relatively low, given that blockchains are, by design, meant to protect integrity. That said, integrity risks can be more prominent for smaller chains, given that the resources employed by the consensus mechanism are lower and can more easily be attacked. Private chains tend to be smaller.

A bigger risk from an integrity standpoint stems from the lack of access control, e.g. permissionless chains. There have been successful 51% attacks against small, permissionless chains such as Verge, Monacoin and others.

Bear in mind that, as with confidentiality and anonymity, the original integrity features of blockchain come at the expense of some privacy considerations such as the right to be forgotten.

Mitigation strategies:

- Consider using an existing, bigger chain, i.e. the one successfully gathering more mining nodes operated by a wider variety of node owners.
- Avoid storing personally identifiable information on blockchains.
- Embed security controls on to oracles that push data to your blockchain.

	Public	**Private**
Permissioned	Low	Low
Permissionless	Low	Medium

Availability: The risk is that participants cannot use the blockchain. Chain availability depends on the number of nodes available compared to the number of transactions to be recorded. Large chains, especially public chains, tend to offer better availability. However, this can come at the expense of real-timeliness, due to the volume of transactions.

On the other hand, private chains are generally smaller and hence more easily disrupted by traditional DDoS or eclipse attacks. Permissioned chains also introduce points of failure with access control mechanisms that can be targeted and indirectly affect the availability of the chain.

Mitigation strategies:

- Use traditional IT availability measures: load balancing, redundancy, anti-DDoS measures etc.
- Ensure gatekeeping redundancy in the case of a permissioned chain.

	Public	**Private**
Permissioned	Low	Medium
Permissionless	Low	Low

Consensus mechanism: Risks associated with consensus mechanisms are tightly related to the integrity property. Attacks against the consensus mechanism generally aim at validating fraudulent transactions or rewriting past transactions. As mentioned, smaller chains are more prone to fall victim to such attacks – particularly if they are permissionless. It is also important to consider the fact that combining multiple consensus mechanisms may introduce new system-level risks.

Mitigation strategies:

- Think carefully when considering custom consensus mechanisms.
- Existing consensus mechanisms have their pros and cons from a security standpoint –consider them in your risk assessment.
- If you do create your own blockchain, keep consensus mechanisms simple: It may be tempting, for instance, to use several of them, but this added complexity results in risks you may not be aware of.

	Public	**Private**
Permissioned	Low	Low
Permissionless	Medium	Medium

Node security: Nodes bear the same risks as any connected processing unit that can fall victim to cyberattacks such as malware or DDoS. A single compromised node won't lead to direct damage, but an incident may come from aggregated occurrences. Since a node is exposed, security is fundamental. As there are more interactions with externals in public or permissionless chains, they may incorporate higher risks in general.

Mitigation strategies:

- Use traditional IT security measures: anti-virus protection, regular patching, etc.

	Public	**Private**
Permissioned	Medium	Low
Permissionless	Critical	High

Smart contract: When talking about typical use cases in a supply chain such as the bill of lading or financial instruments, automation with smart contracts is the core of blockchain-based solutions. If such automation incorporates vulnerability, it may lead to disturbance of operations or immediate financial misoperation. In public chains, smart contract code is visible to all and hence much more accessible for hackers to browse for vulnerabilities. In contrast, public chains also gather more experts auditing the code and detecting failure. This is exactly the same as has happened with the open-source versus closed-source argument.

Permissionless chains also leave greater opportunities for attackers to interact with the code, as KYC procedures in permissioned chains reduce the likelihood of a validated user attacking the smart contracts.

Mitigation strategies:

- Ensure developers apply secure coding practices.
- Ensure smart codes are audited by a third party before uploading them on a blockchain.
- Consider using multi-signature smart contract-based ownership. Alternatively, consider vote-driven smart contract-based ownership.
- Define processes for smart contracts to be able to be phased out or to self-destruct in certain conditions.

	Public	**Private**
Permissioned	Medium	Low
Permissionless	Critical	Medium

Glossary

51% attack: when one or more persons collectively control more than 50% of a network's computing power and maliciously use their hashing power to reverse confirmed transactions, interfere with the process of recording new blocks, prevent new transactions from gaining consensus, allow double spending of the local currency, or take other actions to undermine the integrity of a blockchain.[18]

Anonymity: characteristic of information that does not permit a personally identifiable information principal to be identified directly or indirectly.[19]

Consensus (mechanism): a process (or a mechanism that implements) to achieve agreement by the majority of peers within a distributed network. Achieving consensus means the group of peers participating in a blockchain have evaluated and agreed on the state of the blockchain, most commonly when there is an addition to the blockchain.[20]

Cryptographic key: a sequence of symbols that controls the operation of a cryptographic transformation. A cryptographic transformation can include but is not limited to encipherment, decipherment, cryptographic check function computation, signature generation or signature verification.[21]

Denial of service (DoS): prevention of authorized access to a system resource or the delaying of system operations and functions, with resultant loss of availability to authorized users.[22]

Hacktivism(-vist): (a person involved in) computer hacking (as by infiltration and disruption of a network or website) done to further the goals of political or social activism.[23]

Know Your Customer (KYC): the requirement, pursuant to the Bank Secrecy Act (BSA), that financial institutions conduct due diligence on their customers prior to engaging in transactions with them. The goal is to avoid inadvertently engaging in criminal activity by furthering money laundering, terrorism finance, other criminal enterprises, or engaging in business with persons on the Office of Foreign Assets Control (OFAC) sanctions list.[24]

Membership service provider (MSP): a modular component that is used to manage identities on the blockchain network. An MSP is used to authenticate clients who want to join the blockchain network. Certificate authority is used in MSP to provide identity verification and binding service.

Oracle: an interface with a data source external to a blockchain that provides input data (e.g. share price information) required for a determination of outcomes under a smart contract.[25]

Penetration-testing (pentesting): the process of probing and identifying security vulnerabilities and the extent to which they are used to a cracker's advantage. Penetration-testing is a critical tool for assessing the security state of an organization's IT systems, including computers, network components and applications. Hackers of the white-hat variety are often hired by companies to do penetration-testing. It is money well spent, computer security experts contend.[26]

Smart contract: Blockchains can be programmed to automate business processes (e.g. making payments) in different entities. A smart contract is a computerized transaction protocol that automatically executes the terms of a contract upon a blockchain once predefined conditions are met.

Vulnerability: a weakness of software, hardware or online service that can be exploited.[27]

Wallet: a non-physical storage device for cryptocurrency that a person downloads as a software file and that remains connected to the internet. A wallet can be downloaded and installed on a computer, run online via the cloud or run on a smart device via a mobile application.

Contributors

The World Economic Forum's Centre for the Fourth Industrial Revolution "Redesigning Trust: Blockchain for Supply Chain" project is a global, multi-industry, multistakeholder endeavour aimed at co-designing and co-creating frameworks to encourage the inclusive and well-thought-through deployment of blockchain technology. The project engages stakeholders across multiple industries and governments from around the world. This white paper is based on numerous discussions, workshops and pieces of research – and the combined effort of all involved; the opinions expressed herein may not necessarily correspond with those of each individual involved with the project.

Sincere thanks are extended to those who contributed their unique insights to this report. We are also very grateful for the generous commitment and support of Hitachi and their fellow at the Centre dedicated to the project: Soichi Furuya (also a lead author of the paper).

Lead authors

Adrien Ogée, Lead, Technology and Innovation, World Economic Forum (Centre for Cybersecurity), Switzerland
Soichi Furuya, Senior Researcher, Hitachi (and World Economic Forum Fellow), USA
Nadia Hewett, Project Lead Blockchain and DLT, World Economic Forum (Centre for the Fourth Industrial Revolution), USA

Contributors

Craig Chatfield, Blockchain Architect and Security Consulting Manager, Accenture, UK
Dominique Guinard, Co-Founder and Chief Technology Officer, EVRYTHNG, Switzerland
Francis Jee, Manager, Deloitte Consulting LLP (and World Economic Forum Fellow), USA
Hanns-Christian Hanebeck, Founder and Chief Executive Officer, Truckl.io, USA
Partha Das Chowdhury, Head, Blockchain CoE, VARA Technology, India
Ramón Gómez-Ferrer, Head of Strategy and Innovation, Valencia Port Authority, Spain
Sheila Warren, Head of Blockchain and DLT, World Economic Forum (Centre for the Fourth Industrial Revolution), USA
Sumedha Deshmukh, Project Specialist, World Economic Forum (Centre for the Fourth Industrial Revolution), USA

Commentator

Jaka Mele, Chief Digital Officer, CargoX, Slovenia

Endnotes

1. http://www3.weforum.org/docs/48423_Whether_Blockchain_WP.pdf
2. http://www3.weforum.org/docs/WEF_Introduction_to_Blockchain_for_Supply_Chains.pdf
3. https://fintechnews.sg/23594/blockchain/cryptocurrency-hack-binance/
4. https://fortune.com/2017/07/18/ethereum-coindash-ico-hack/
5. https://blog.tradelens.com/news/5-key-points-about-tradelens-platform-security/
6. https://deloitte.wsj.com/cio/2019/06/10/emerging-disruptors-lead-the-way-on-blockchain/
7. https://www.bbc.com/news/technology-47454528
8. https://www.forbes.com/sites/danielnewman/2017/10/24/blockchain-and-digital-transformation-go-hand-in-hand/#2721404646f7
9. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf
10. https://hackernoon.com/databases-and-blockchains-the-difference-is-in-their-purpose-and-design-56ba6335778b
11. https://www.schneier.com/blog/archives/2013/01/complexity_and.html
12. https://blog.theabacus.io/the-verge-hack-explained-7942f63a3017
13. https://www.mycryptopedia.com/blockchain-oracles-explained/
14. https://mashable.com/2018/04/05/verge-crypto-hack/
15. https://www.developcoins.com/blockchain-consensus-algorithms
16. https://medium.com/solidified/the-biggest-smart-contract-hacks-in-history-or-how-to-endanger-up-to-us-2-2-billion-d5a72961d15d
17. https://blockchaintrainingalliance.com/products/cbsp
18. Latham and Watkins, *The Book of Jargon: Cryptocurrency & Blockchain Technology*, https://www.lw.com/bookofjargon-apps/boj-CryptocurrencyandBlockchain
19. ISO/IEC 29100:2011
20. Latham and Watkins, *The Book of Jargon: Cryptocurrency & Blockchain Technology*
21. ISO/IEC 19790:2012
22. ISO/IEC 27033-1:2015
23. Merriam Webster, https://www.merriam-webster.com/
24. Latham and Watkins, *The Book of Jargon: Cryptocurrency & Blockchain Technology*
25. Ibid.
26. Lowery, J. *Penetration Testing: The Third Party Hacker*. [Online, February 2002.] SANS Institute Website
27. ISO/IEC 29147:2014

(all links as of 7/11/19)

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744

contact@weforum.org
www.weforum.org