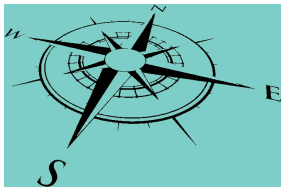
Blockchain secure deployment 10-step process

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.

This white paper has been published by the World Economic Forum as a contribution to a project, insight area or interaction. The findings, interpretations and conclusions expressed herein are a result of a collaborative process facilitated and endorsed by the World Economic Forum, but whose results do not necessarily represent the views of the World Economic Forum, nor the entirety of its Members, Partners or other stakeholders.

Contents



World Economic Forum (WEF)

Stakeholder(s):

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

Soichi Furuya :
Lead Author — Senior Researcher, Hitachi (and World Economic Forum Fellow), USA

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

Craig Chatfield :
Contributor — Blockchain Architect and Security Consulting Manager, Accenture, UK

Dominique Guinard :
Contributor — Co-Founder and Chief Technology Officer, EVRYTHNG, Switzerland

Francis Jee :
Contributor — Manager, Deloitte Consulting LLP (and World Economic Forum Fellow), USA

Hanns-Christian Hanebeck :
Contributor — Founder and Chief Executive Officer, Truckl.io, USA

Partha Das Chowdhury :
Contributor — Head, Blockchain CoE, VARA Technology, India

Ramón Gómez-Ferrer :
Contributor — Head of Strategy and Innovation, Valencia Port Authority, Spain

Sheila Warren :
Contributor — Head of Blockchain and DLT, World Economic Forum (Centre for the Fourth Industrial Revolution), USA

Sumedha Deshmukh :
Contributor — Project Specialist, World Economic Forum (Centre for the Fourth Industrial Revolution), USA

Jaka Mele :
Commentator — Chief Digital Officer, CargoX, Slovenia

Vision

A successful security practice

Mission

To provide deployment guide for blockchain technology

Values

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

Expectations: Trust is derived from clear expectations.

Predictability: As such, digital trust stems from predictability – the knowledge that the technologies we use will work as they should.

Security: Predictability, in turn, is enforced by security.

Step 1. Expertise

Acquire blockchain expertise

Stakeholder(s)

Consortia :
In the case of a consortium, for instance, it may be necessary to create a distributed security operations centre (SOC).

Security Operations Centres

Security Services :
Given the recency of the technology's development, only a limited number of third-party security services and training materials exist.

Blockchain Training Alliance :
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.

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

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.

1.1. Oversight Teams

Create security oversight teams.

End goal: the creation of a security oversight team that will be in charge of driving the next steps.

Stakeholder(s):

Security Oversight Teams :
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.

Chief Information Security Officers (CISO)

Chief Information Officers (CIO)

Consortia :
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. Goals

Define security goals

Stakeholder(s)

Port of Valencia :

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).

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?

2.1. Requirements & Priorities

Identify the major requirements of security from the CIA's point of view, and how are they prioritized

2.2. Anonymity

Determine the importance of ensuring the anonymity of customers.

Stakeholder(s):

Customers

2.3. Reputations

Evaluate how badly the reputation of the organization would be affected by system glitches or data leaks.

2.4. Plans

Outline the important goals in simple language.

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

Step 3. Blockchain Type

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.

3.1. Advantages & Trade-Offs

List the security and business advantages and trade-offs of the various blockchain types considered.

Step 4. Risk Assessment

Perform a risk assessment

Stakeholder(s)

Port of Valencia :

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 block-chain 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. – Hackti-vists could be drawn to the network.

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

4.1. Actions

Compile a prioritized list of actions to manage the risks identified.

This step should conclude with a prioritized list of actions to manage the risks identified. 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.

Step 5. Security Controls

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.

5.1. Functional Specifications

List the security functional specifications of the blockchain.

5.2. Security Controls

List the recommended security controls for the development team.

Stakeholder(s):
Blockchain Development Teams

Step 6. Security Governance

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.

6.1. Risk

Base governance processes the degrees of risk.

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.

6.2. Staffing

Base staffing on the security controls to be implemented and monitored.

The more security controls there are to implement and monitor, the more staff will be required.

6.3. Coordination

Coordinate appropriately with solution developers, operators, executive system owners and ecosystem participants.

The more distributed the risks, the more coordination with solution developers, operators, executive system owners and ecosystem participants will be required.

Stakeholder(s):

Blockchain Developers

Blockchain Operators

Blockchain Ecosystem Participants

Executive System Owners

6.4. Continuity & Recovery Plans

Revise and update business continuity and disaster recovery plans as appropriate.

End goal: revised business continuity and disaster recovery plans.

Step 7. Vendors

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. Security

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.

8.1. Penetration Testing

Embed penetration-testing in the development of blockchain solutions.

8.2. Code Auditing

Embed smart code auditing in the development of blockchain solutions.

8.3. Architecture Analysis

Embed architecture analysis in the development of blockchain solutions.

Step 9. Monitoring & Auditing

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

9.1. Penetration Testing

Conduct regular penetration-testing of the infrastructure and applications.

First, regular penetration-testing of the infrastructure and applications that interact with the solution is essential.

9.2. Contracts

Audit smart contracts.

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.

9.3. Security Operations Centres

Enable security operations centres (SOC) to monitor blockchain solutions along with other organizational assets.

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.

Stakeholder(s):

Security Operations Centres

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

9.4. Audits

Periodically conduct audits to ensure security procedures and systems are up to date and best fitted to current systems and environments.

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.

Step 10. Incidents

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... End goal: timely mitigation of security incidents.

10.1. Post-Mortem Assessments

Conduct post-mortem assessments to improve the overall security posture and limit the risk of incidents reoccurring.

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.

10.2. Security Plans

Integrate blockchain-specific procedures into security plans.

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.

10.3. Incident-Response Exercises

Conduct incident-response exercises.

It is of the utmost importance to conduct an incident-response exercise before such an event occurs.

Stakeholder(s):

Heinrich Heine :
Finally, in the words of the German poet Heinrich Heine: "Experience is a good school, but the fees are high."

10.4. Training

Training staff to respond to incidents.

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

10.5. Decision-Making Processes

Test distributed decision-making processes.

Administrative Information

Start Date:
End Date:

Publication Date: **2020-07-09**
Source: http://www3.weforum.org/docs/WEF_Inclusive_Deployment_of_Blockchain_for_Supply_Chains_Part_5.pdf

Submitter:

Given Name: Owen
Surname: Ambur
Email: Owen.Ambur@verizon.net
Phone: