Blockchain Cybersecurity Framework: A Framework for Trust

19 June 2019
Content of Presentation

• A brief introduction on Blockchain
• The need for a framework
• The target audience
• The process & partners
• Security In the blockchain
• The Framework
A brief introduction on blockchain

Blockchain has become a fast rising technological trend.
The Dutch Blockchain Coalition

• Aims to stimulate blockchain technology in the Netherlands

• Over 50 members across academia, private sector and government

• Current landscape in the Netherlands gave room to DBC
Need for a Framework

• Blockchain technology is complicated
• IT risks are difficult to assess

• Organizations want to use the technology, but do not have the resources to have a proper security assessment

• The framework will provide practical security considerations
Target Audience

• Organizations that have chosen to use blockchain for current or new process (public or private)

• We also focus on Small and Medium Enterprises (MKBs)

• Meant to be used by decision-makers in the organization
The Process & Partners

• We consulted several organizations:
• Healthcare sector, municipalities, NGOs and other SMEs/MKBs

• It was important to collect major security concerns from organizations
The Process & Partners

• We counted on the expertise from partners:
The Use-Cases

• The use-cases used for the framework:

• “Mijn zorg log”: Blockchain baby - Healthcare
• Microbiome center Nederland – Healthcare
• Loek! Real estate management – Real Estate
• Grain Initial Coin Offering – Financial, ICO
• Consentus – Healthcare
Security of Blockchain

• Blockchain technology is like any other technology

• “Special” characteristics of blockchain:
  • Can avoid central authority / can eliminate intermediaries
  • Provides real-time settlement
  • Reduced operational costs
  • Has high levels of transparency

• These characteristics amplify and/or reduce security risks
The Framework

- We came up with 24 security considerations

- All “Traditional” security threats apply to blockchain technologies

- Most considerations apply to any other technology
  - Again, blockchain may amplify or reduce certain security risks
Step 1:
Do you really need it?
The Framework

Divided them into categories:

• Blockchain specific
• Network and Infrastructure
• Operational and Organizational
• Management-level
• When Migrating an old process
The Framework

Blockchain Specific:

• Security of Smart Contracts
• Forks
• Cryptographic Algorithms
• Cryptographic key management
• Scalability
The Framework

Operational and Organizational

- Operations and Communications Security
- Systems Acquisition, Dev and Maintenance
- Asset Management & Classifications
- Supplier Relationships
- Human Resource Security
- Incident Management
The Framework

Network and Infrastructure

• Access Control
• Intrusion Detection
• Targeted Attack Resistance
• Data Propagation Attack Resistance
The Framework

Management Level:

• Organization’s Information Security Policy
• Information Security Organization within company
• External and Internal Compliance (Auditing / Industry standards)
The Framework

When Migrating a Process

- Selecting the right blockchain (public/ private/ permissioned/ permissionless)
- Application testing
- Awareness and Training
- Contingency planning
- Peer-reviewing of Smart contracts
- Privacy/ GDPR (User Rights: Erasure, Forgotten, Limit Processing)
Our Main Goal

- Enable users and organizations to understand the risks in this new environment.

- Understanding these risks means you can trust the technology.

- Trusting the technology means confidence in using it.
View / Download it here

Want more information?
Contact:
Nicolas.castellon@cgi.com or Peter.cozijnsen@cgi.com