

Blockchain Use in Security

Joanna Moubarak¹ and Maroun Chamoun¹

¹Faculty of Engineering, University of Saint Joseph, Beirut, Lebanon

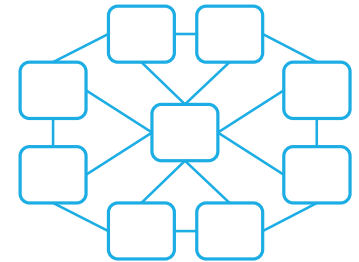
Overview

- Introduction
- Blockchain Development
- Comparison of Blockchains
- Attacks and Challenges
- Creating a k-ary malware using Blockchain
- Blockchain use in industry
- Conclusion

Introduction

Blockchain is defined as:

- a secure, distributed, peer-to-peer environment
- a fault tolerant and reliable software network
- a mathematical and deterministic mechanism
- a public transaction digital ledger
- an ultimate revolution

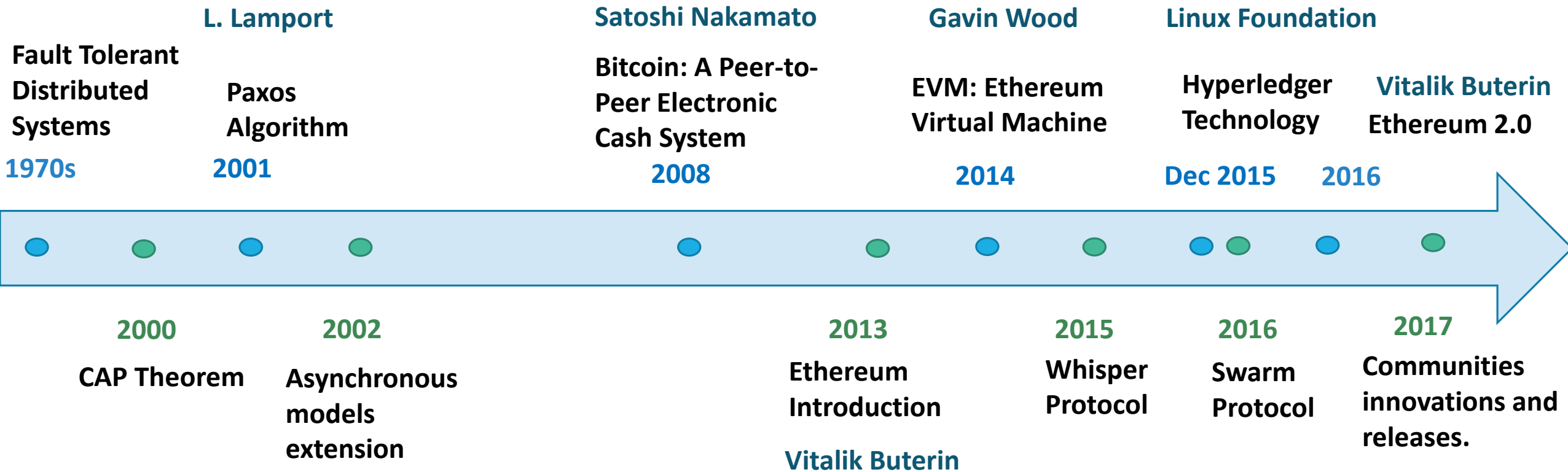


Introduction



Source: EverisDigital

Blockchain Development



Blockchain Structure

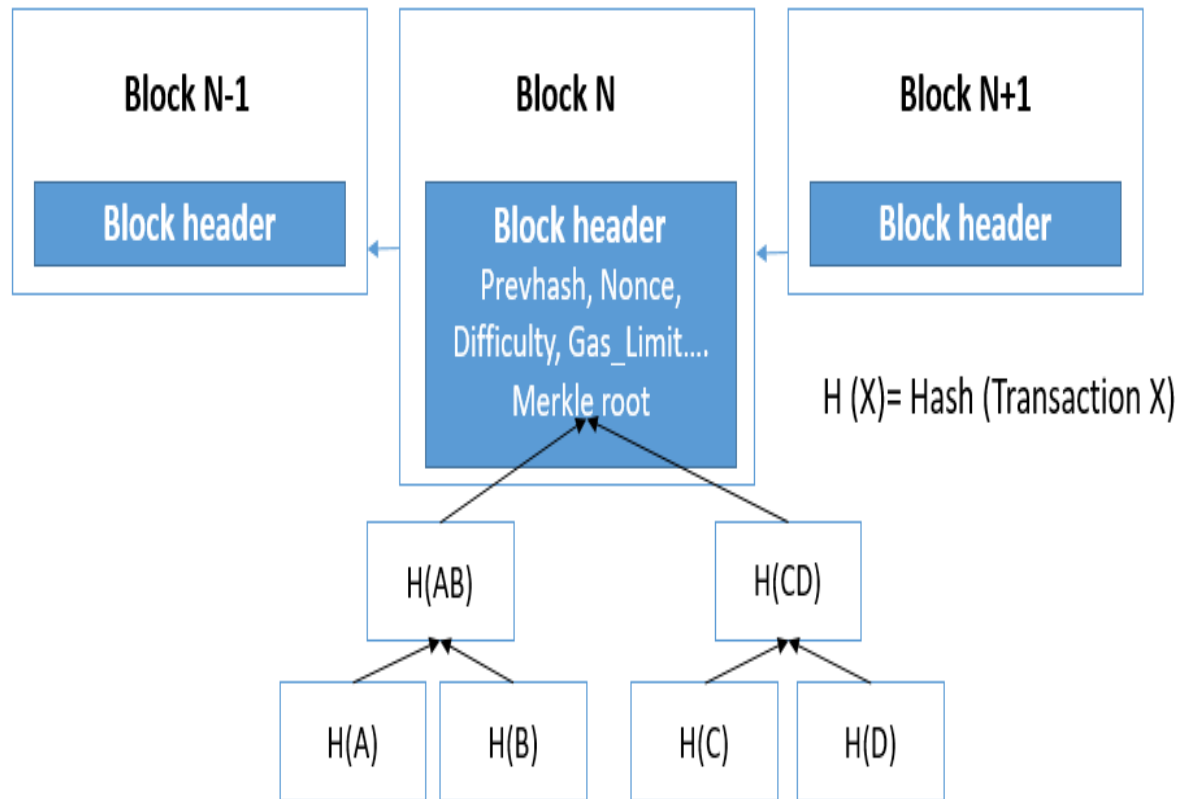


Figure 1 Blockchain structure

- Cryptographic keys
- Transactions
- Hashing
- Miners
- Consensus Algorithm

Comparison of Blockchains

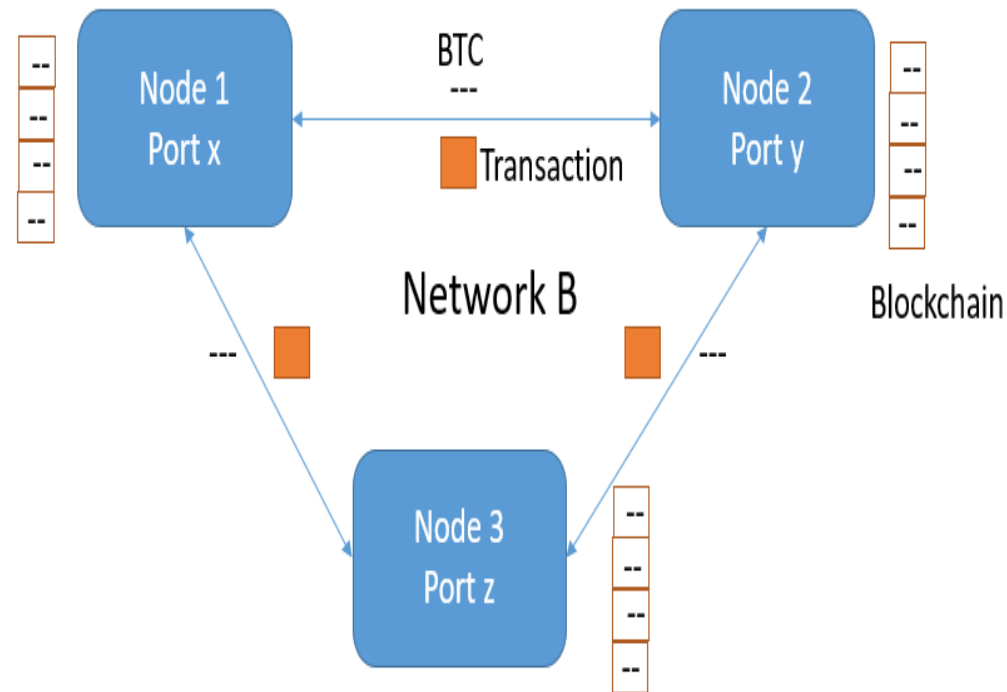


Figure 2 Bitcoin Network

Comparison of Blockchains

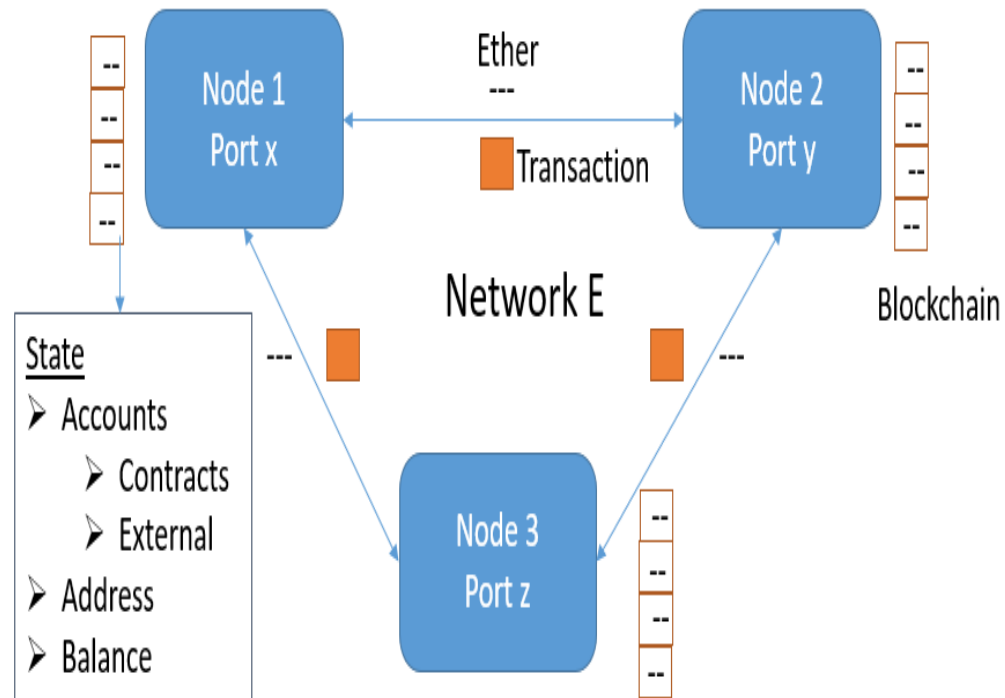


Figure 3 Ethereum Network

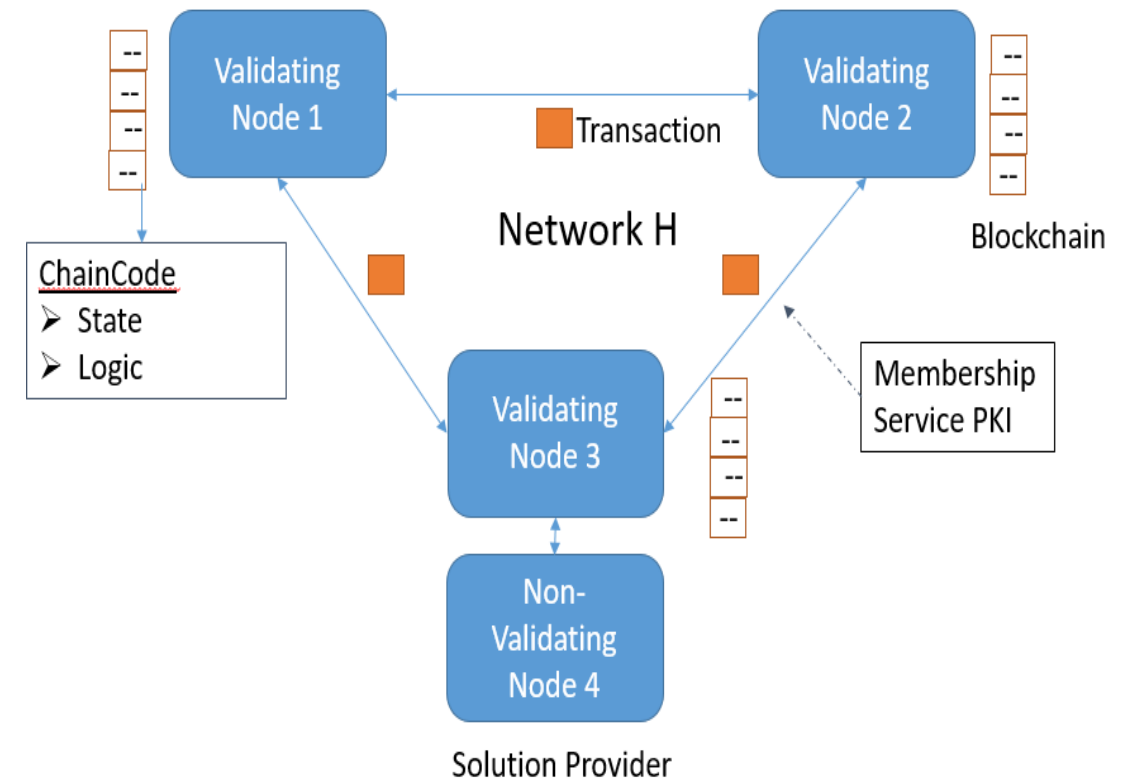


Figure 4 Hyperledger Network

	Bitcoin	Ethereum	HyperLedger
Communities	Bitcoin developers	Ethereum developers	Linux Foundation
Blockchain type	Permission-less	Permission-less	Permissioned
Currency	BTC	Ether	None
Consensus	PoW (based on SHA-256)	PoW (Ethash)	PBFT (excluding Corda)
Private transaction mode	No	No	Yes
Stimulus	Economics incentive, fees and rewards	Economics incentive, fees and rewards	Reputational Risk
Censorship resistance	No	Yes	No
Limit	7 transactions/sec	20 transactions/sec	No
State concept	No	Data	Key-value
Smart contract languages	No	Solidity, Serpent, Mutan, LLL	Chaincode
Cross-contracts	No	Yes	Yes
Scalability	No	No	Yes
Block time	10 min	15 secs	Subject to the peers involved
Variants	+ 700 variants	Olympic, Frontier, Homestead, Metropolis (Future release) and Serenity (To be announced)	Burrow, Fabric, Iroha, Corda, Sawtooth
GPU cost	Yes	Yes	No
Auditing Mechanism	No	No	Yes
Applications	Digital Registry, Crypto Currency	Digital Registry, Crypto Currency, Smart Contracts	Digital Registry, Smart Contracts
Languages	C++	Golang, C++, Python	GoLang, Java

Table 1 DLTs Comparison

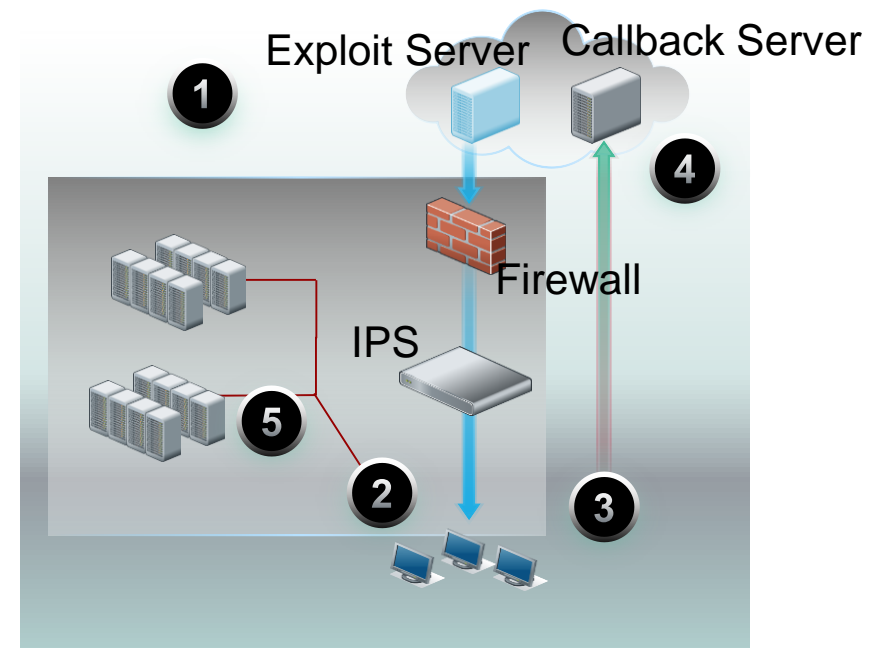
Attacks and Challenges

- Transactions Security
- Spam attacks
- Anonymity
- Targeted DDoS attacks
- Timejacking attacks
- Mining Pools
- Malicious Contracts

Formalization, implementation and testing of new undetectable viral algorithms

Malware Life cycle

1. Exploitation of System
2. Malware Executable Download
3. Callbacks and Control Established
4. Data Exfiltration
5. Malware Spreads Laterally



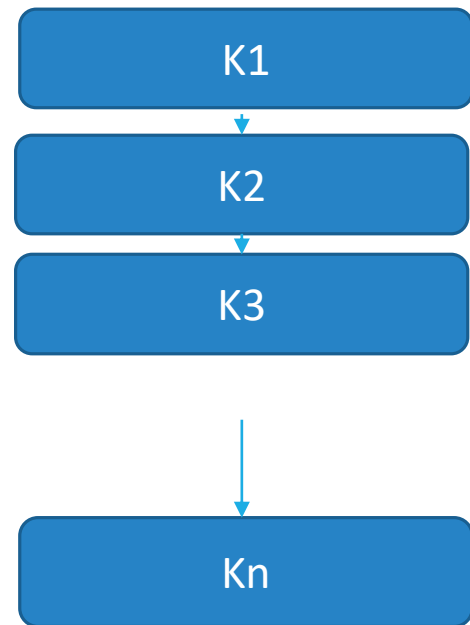
Limitation of Anti-Antiviral Techniques

- **Stealth Techniques** -> Combination of several techniques
- **Polymorphism** -> Difficult to implement and manage
- **Code rewriting** -> Add random instructions, modifies the code but same result
- **Encryption techniques** -> The encryption procedure remain unchanged
- **Code armouring** -> It will delay the analysis but the final result is the same

New Undetectable Viral Algorithm

- **K-ary** viruses: The objective is to scatter the viral information over different files : each of the k constituting part looks like an innocent file and thus does not trigger any alert.

k viruses



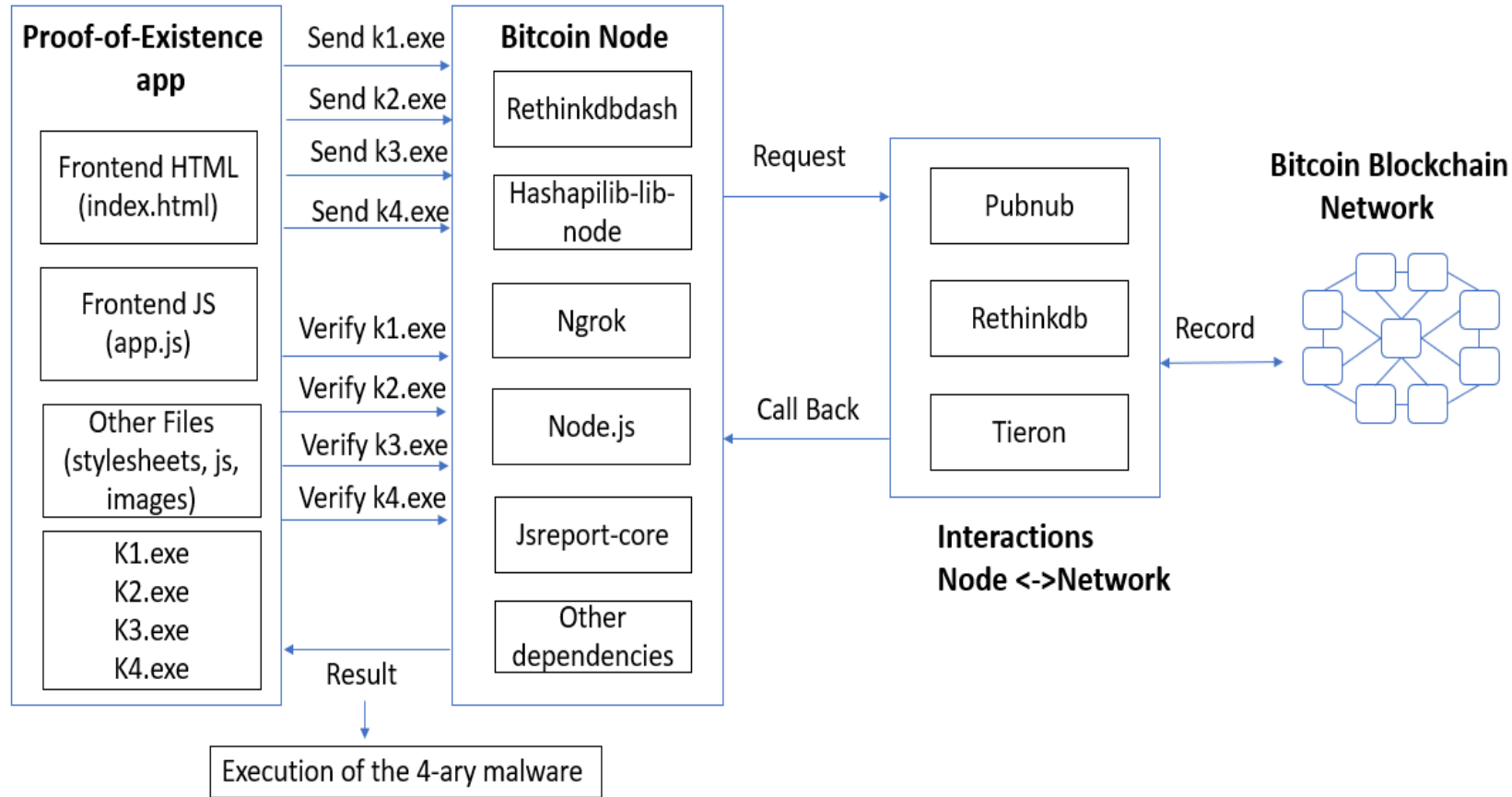
Undetectable Viral Algorithm Challenges

- **Dependency problem**
- **Key Management Problem**
- **Key Generation Problem**
- **Randomization**

A blue bracket on the right side of the list, grouping the four items.

Blockchain

A 4-ary malware workflow



Node.js

```
C:\Users\Joanna\ [redacted] >node server.js
Creating a pool connected to localhost:[redacted]
Creating a pool connected to localhost:[redacted]
Setting up Block Subscription...
Update susbcription
Server up and listening on port [redacted]
{ receiptId: '5a4f81c2b8af0a2f6d787db5', timestamp: 1515160002 }
```



Summary

18

k1.exe block summary

[Block Explorer](#)
[News](#)
[Market](#)
[Bitcoin cash](#)
[Zcash](#)
[Blocks](#)
[Status](#)

[Buy Bitcoin with CC!](#)

✓ Conn · Height
Scan
BTC ▾





Block #502546

BlockHash 00000000000000000006be80290136466f2fcd3bdacbb10758e90d5687ea81ca7

Summary

Number Of Transactions	2835	Difficulty	1931136454487.7163
Height	502546 (Mainchain)	Bits	180091c1
Block Reward	12.5 BTC	Size (bytes)	966611
Timestamp	Jan 4, 2018 4:04:00 PM	Version	536870912
Mined by		Nonce	3725939730
Merkle Root	c14160392a4736d6283bab326db6a...	Next Block	502547
Previous Block	502545		

k1 Execution: Auto-reproduction

Name	Date modified	Type	Size
 juwgohah	1/6/2018 11:49 AM	Application	38 KB
 oiyyhstv	1/6/2018 11:48 AM	Application	38 KB
 typkymvu	1/6/2018 11:50 AM	Application	38 KB
 yeqerjhx	1/6/2018 11:49 AM	Application	38 KB

Our Contributions

- Joanna Moubarak, Maroun Chamoun and Eric Filiol. "***Developping a k-ary Malware Using Blockchain***". **NOMS 2018 IEEE/IFIP Man2Block 2018**, Tapei, April 27th, 2018.
- Joanna Moubarak, Eric Filiol & Maroun Chamoun. "***On Blockchain Security and Relevant Attacks***". **IEEE Menacomm 2018**, Jounieh, Lebanon, April 18th - 20th, 2018.
- Joanna Moubarak, Eric Filiol and Maroun Chamoun. "***Comparative Analysis of Blockchain Technologies and the TOR Network: Two Faces of the same Reality?***" **IEEE-CSNet 2017**, Rio de Janeiro, Brazil, October 18-20th, 2017.
- Joanna Moubarak, Maroun Chamoun and Eric Filiol. "***Comparative Study of Recent MEA Malware Phylogeny***". **ICCCS'2017**, July 11th-14t, 2017, Krakow, Poland.
This paper has received the best presentation award.
- Joanna Moubarak, Maroun Chamoun and Eric Filiol. **Middle East Malware Evolution. 23rd international Scientific Conference of LAAS**, April 6th - 7th, 2017, Beirut, Lebanon.

Modeling a new secure ICS infrastructure based on decentralized architecture

PhD student: Wassef Karimeh

CERN-European Organization for Nuclear Research



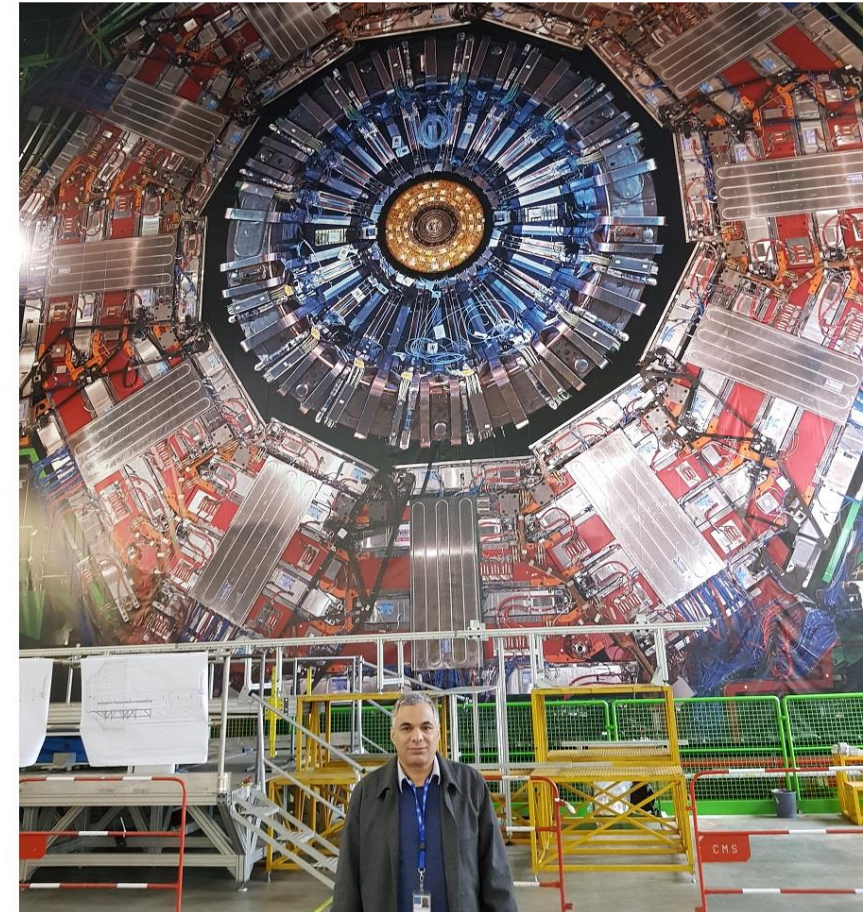
- What is the universe made of? How did it start?
- 4 Big Experiments:
 - ATLAS
 - CMS
 - ALICE
 - LHCb



USJ is CMS member

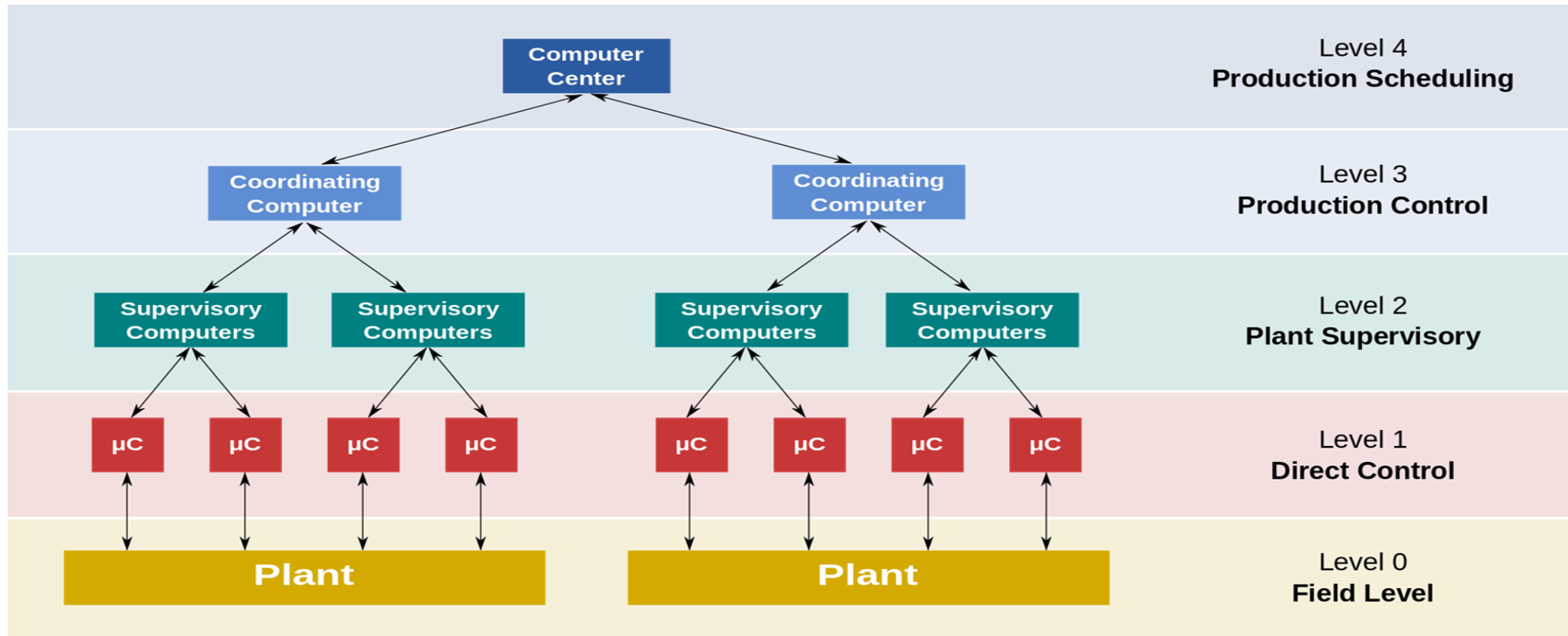
CMS Experiment

- Compact Muon Solenoid
- Layers:
 - Tracker
 - Electromagnetic Calorimeter
 - Hadron Calorimeter
 - The magnet
 - The muon detectors
- Layered DCS (Detector Control System)
- One control view



Supervisory Control And Data Acquisition (SCADA) Functional Architecture

- Tool: Wincc-OA



SCADA Challenges

- Controlling complex distributed systems
- Generating meaningful alarms
- Archiving
- Failure processes and Safety measurements
- Security issues (Stuxnet)

Blockchain is not Bitcoin – it's far more

- Not all blockchains are equal.
- Bitcoin operates within a network of **anonymous** participants
- Authorization in Enterprise blockchains helps manage interactions between **known** parties.
- Enterprise blockchains meet four fundamental requirements:
 - accountability,
 - privacy,
 - scalability
 - security.

Industrial Control Systems (ICS) and Blockchain

- 91% of ICS devices possess a medium or high-risk vulnerability.
- Decentralized structure of Blockchain and built-in verification make it a perfect fit for the IoT environment including Industrial Control Systems (ICS).
- Blockchain technology offer the smart industry ecosystem the following:
 - A way to record and verify each device.
 - Cross-check suppliers and devices
 - Confidentiality of sensitive information.
 - Trusted proof of sensor readings allowing any device to be verified and deactivated if a breach is detected.

Scope of the PhD

- Study the SCADA system in the CMS experiment
- Build a generic model for the SCADA system
- Build a framework using Enterprise Blockchain to integrate security in the new model
- **Challenges:**
 - SCADA systems are domain-specific with private industrial protocols
 - Blockchain is beyond the capabilities of the existing equipment
 - Performance and speed are key factors in a control system

Conclusion

Conclusion

- Distributed Ledger Technologies : Bitcoin, Ethereum, Hyperledger
- Blockchain Challenges and Attacks
- Malicious Blockchain Applications
- Blockchain Potential Application in ICS
- Need of legal and regulatory frameworks to manage blockchains and their uses

Questions ?