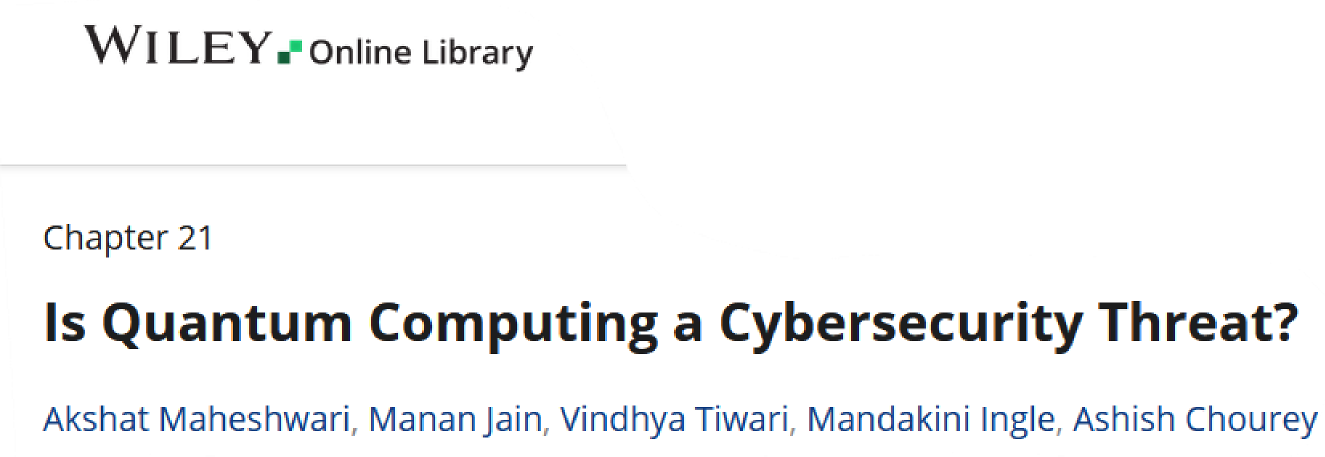
Open Source MANO by ETSI

Orchestration Service for QKD Network Digital Twins

29/11/2023

Blanca López
blanca.lopez@imdea.org

institute imdea networks uc3m | Universidad Carlos III de Madrid

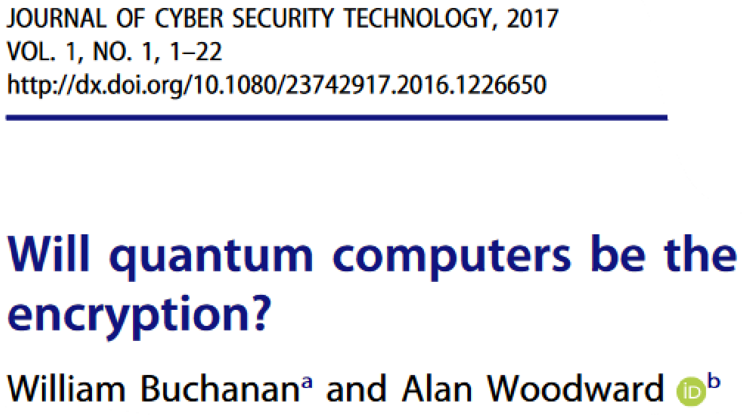


WILEY Online Library

Chapter 21

Is Quantum Computing a Cybersecurity Threat?

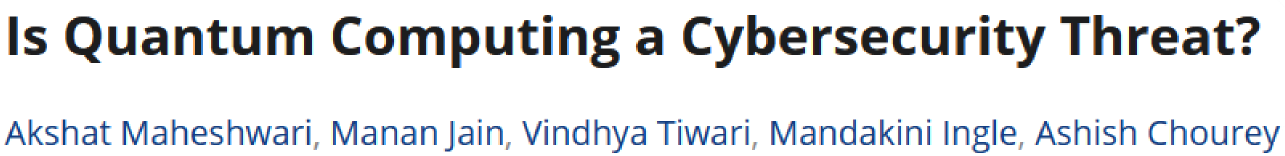
Akshat Maheshwari, Manan Jain, Vindhya Tiwari, Mandakini Ingle, Ashish Chourey



JOURNAL OF CYBER SECURITY TECHNOLOGY, 2017
VOL. 1, NO. 1, 1–22
http://dx.doi.org/10.1080/23742917.2016.1226650

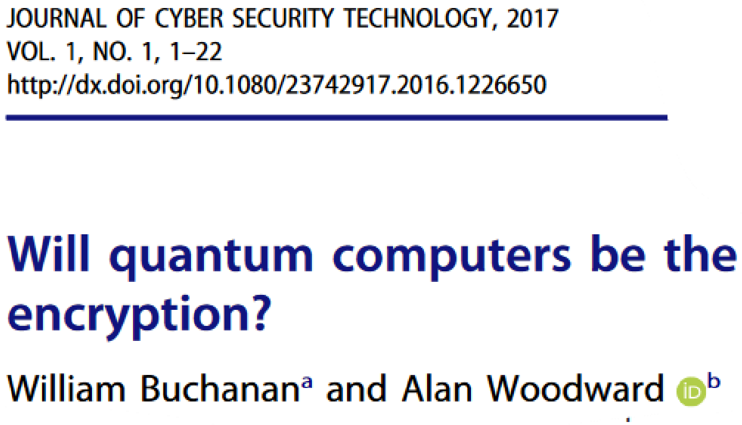
Will quantum computers be the end of public key encryption?

William Buchanan[a] and Alan Woodward[b]



Is Quantum Computing a Cybersecurity Threat?

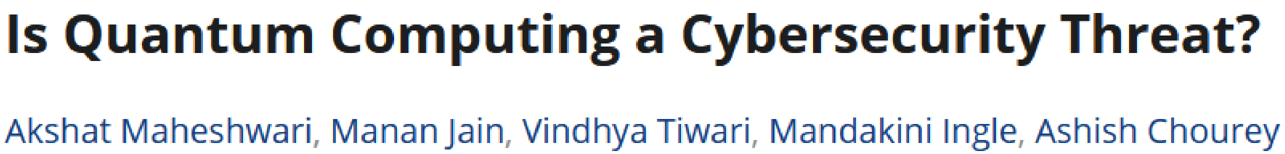
Akshat Maheshwari, Manan Jain, Vindhya Tiwari, Mandakini Ingle, Ashish Chourey



JOURNAL OF CYBER SECURITY TECHNOLOGY, 2017
VOL. 1, NO. 1, 1–22
http://dx.doi.org/10.1080/23742917.2016.1226650

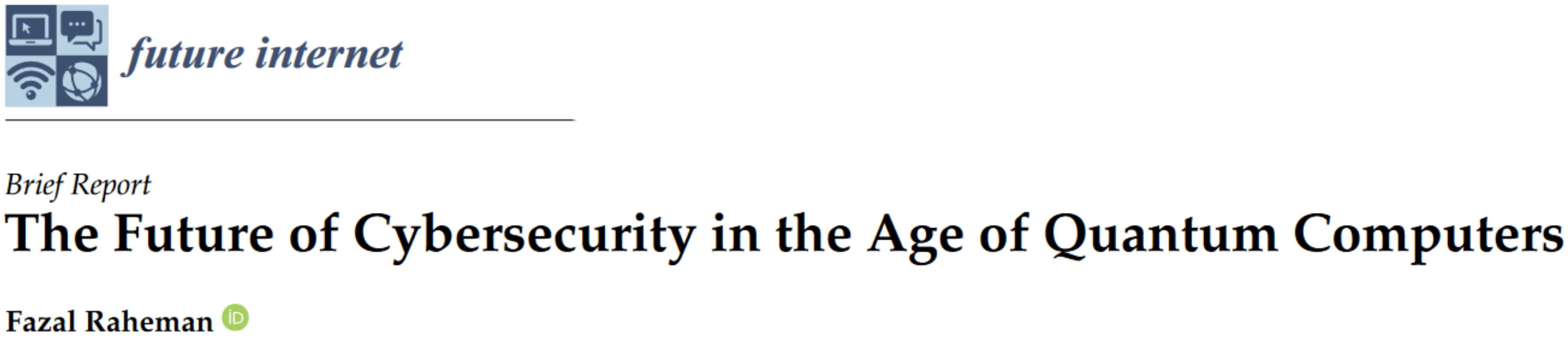
Will quantum computers be the end of public key encryption?

William Buchanan[a] and Alan Woodward[b]



Is Quantum Computing a Cybersecurity Threat?

Akshat Maheshwari, Manan Jain, Vindhya Tiwari, Mandakini Ingle, Ashish Chourey

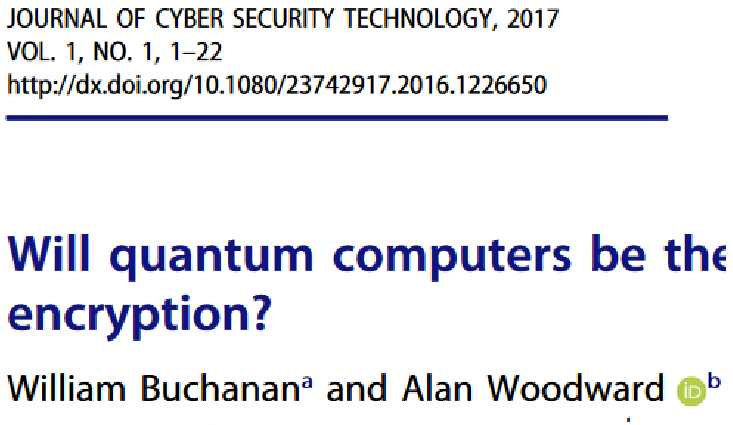


future internet

Brief Report

The Future of Cybersecurity in the Age of Quantum Computers

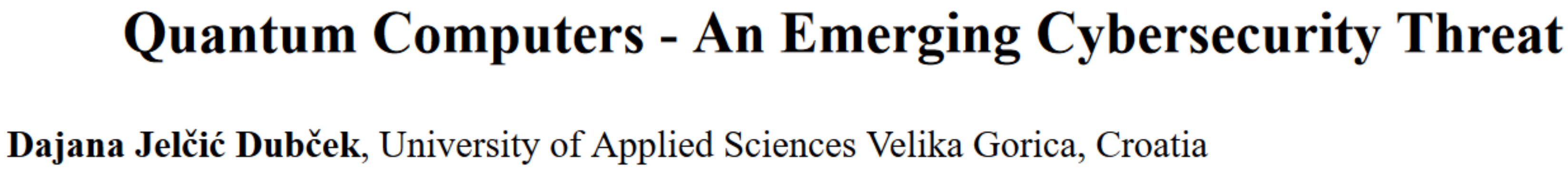
Fazal Raheman



JOURNAL OF CYBER SECURITY TECHNOLOGY, 2017
VOL. 1, NO. 1, 1–22
http://dx.doi.org/10.1080/23742917.2016.1226650

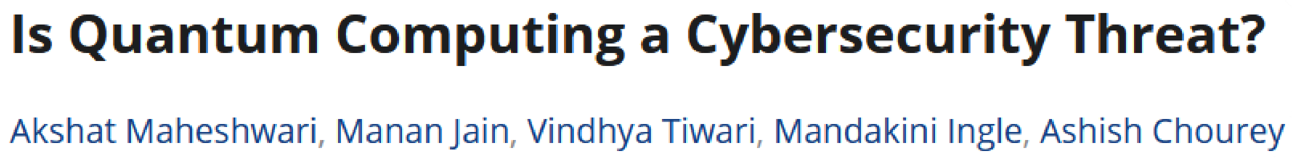
Will quantum computers be the encryption?

William Buchanan[a] and Alan Woodward[b]



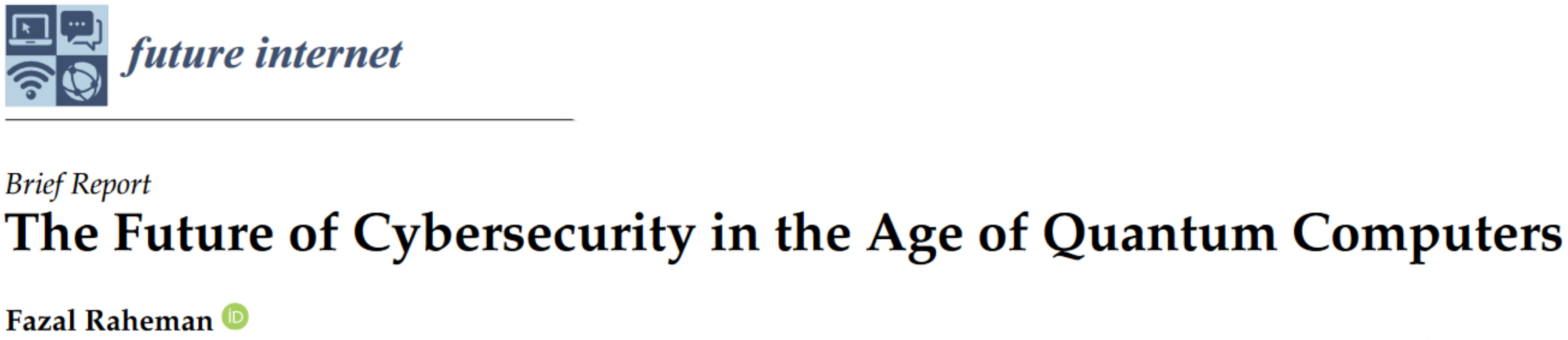
Quantum Computers - An Emerging Cybersecurity Threat

Dajana Jelčić Dubček, University of Applied Sciences Velika Gorica, Croatia



Is Quantum Computing a Cybersecurity Threat?

Akshat Maheshwari, Manan Jain, Vindhya Tiwari, Mandakini Ingle, Ashish Chourey

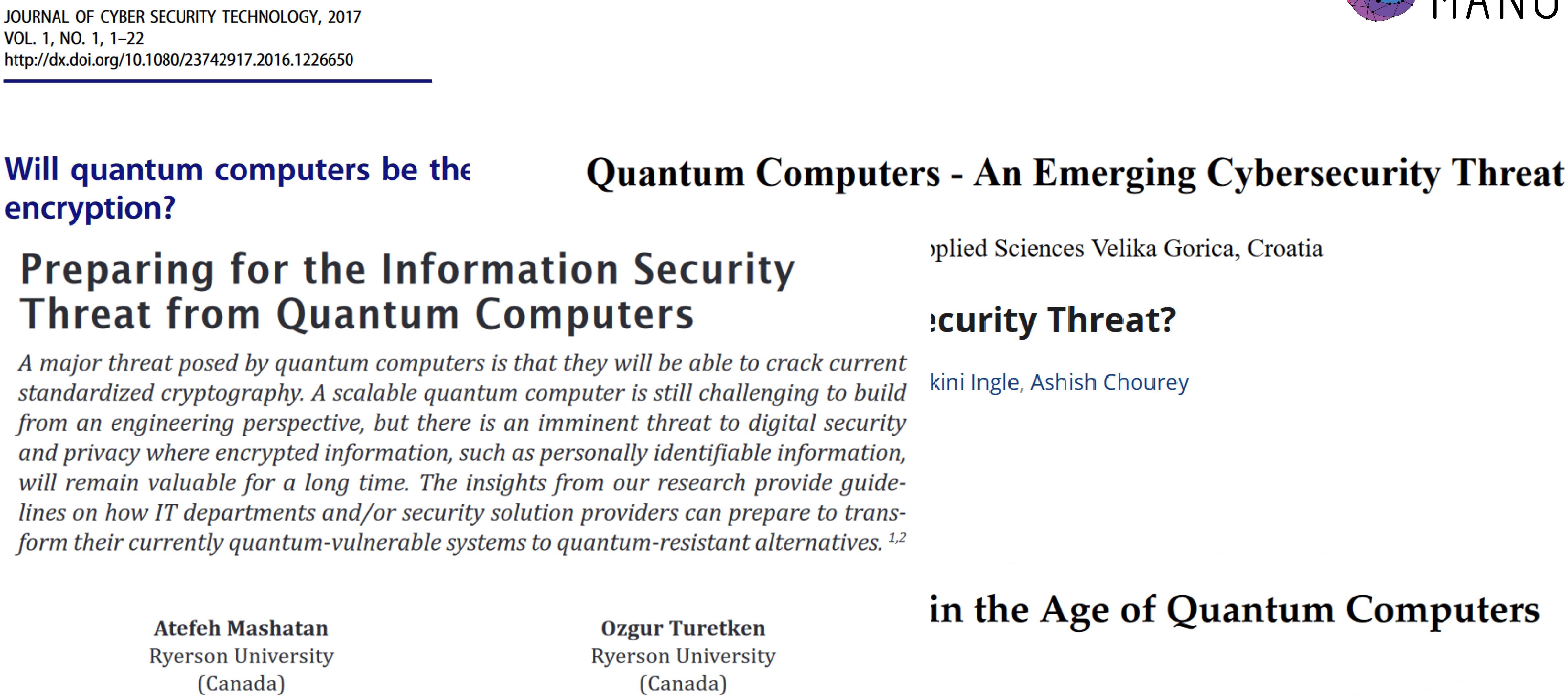


future internet

Brief Report

The Future of Cybersecurity in the Age of Quantum Computers

Fazal Raheman



JOURNAL OF CYBER SECURITY TECHNOLOGY, 2017
VOL. 1, NO. 1, 1–22
http://dx.doi.org/10.1080/23742917.2016.1226650

Will quantum computers be the encryption?

Quantum Computers - An Emerging Cybersecurity Threat

Preparing for the Information Security Threat from Quantum Computers

A major threat posed by quantum computers is that they will be able to crack current standardized cryptography. A scalable quantum computer is still challenging to build from an engineering perspective, but there is an imminent threat to digital security and privacy where encrypted information, such as personally identifiable information, will remain valuable for a long time. The insights from our research provide guidelines on how IT departments and/or security solution providers can prepare to transform their currently quantum-vulnerable systems to quantum-resistant alternatives. [1,2]

Atefeh Mashatan
Ryerson University
(Canada)

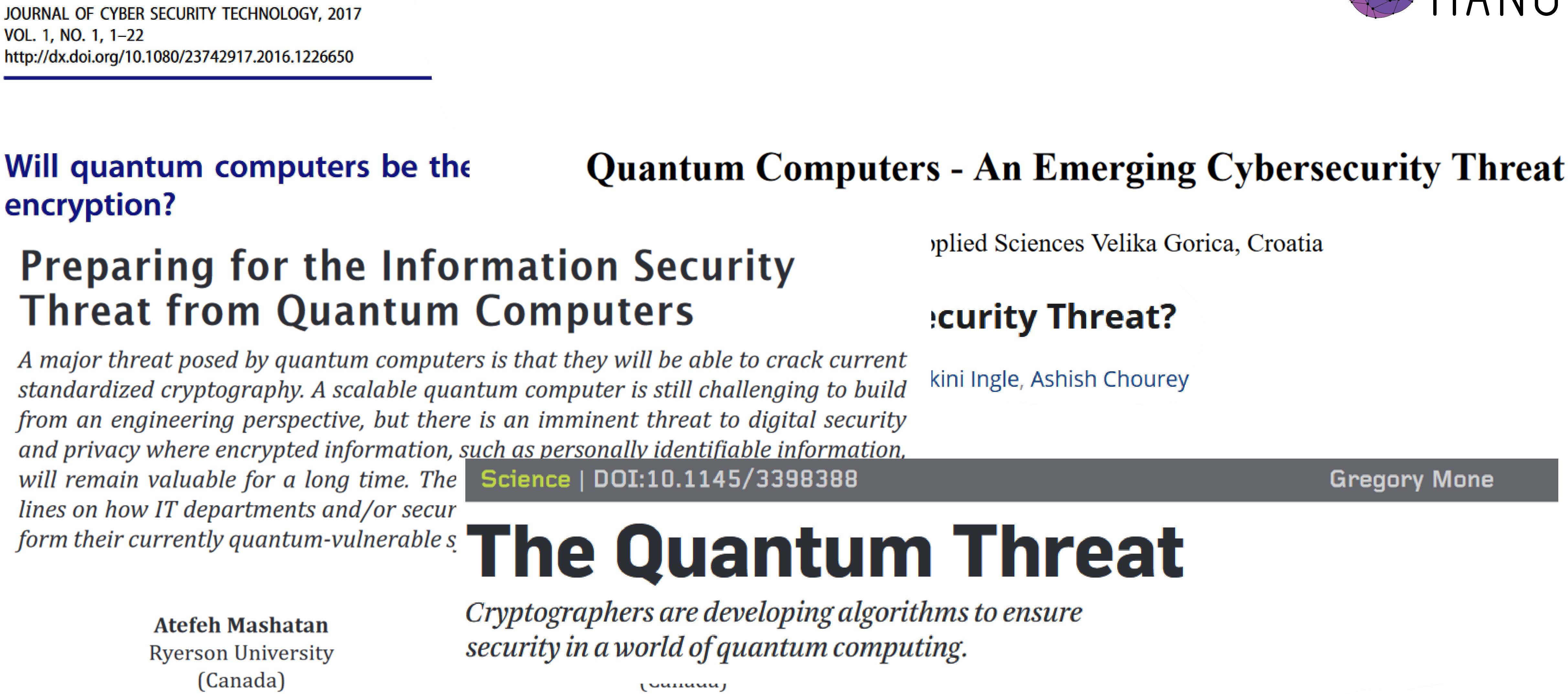
Ozgur Turetken
Ryerson University
(Canada)

plied Sciences Velika Gorica, Croatia

curity Threat?

kini Ingle, Ashish Chourey

in the Age of Quantum Computers



JOURNAL OF CYBER SECURITY TECHNOLOGY, 2017
VOL. 1, NO. 1, 1–22
http://dx.doi.org/10.1080/23742917.2016.1226650

Will quantum computers be the encryption?

Quantum Computers - An Emerging Cybersecurity Threat

ıplied Sciences Velika Gorica, Croatia

Preparing for the Information Security Threat from Quantum Computers

A major threat posed by quantum computers is that they will be able to crack current standardized cryptography. A scalable quantum computer is still challenging to build from an engineering perspective, but there is an imminent threat to digital security and privacy where encrypted information, such as personally identifiable information, will remain valuable for a long time. The lines on how IT departments and/or secur form their currently quantum-vulnerable s

:curity Threat?

kini Ingle, Ashish Chourey

Science | DOI:10.1145/3398388 Gregory Mone

The Quantum Threat

Cryptographers are developing algorithms to ensure security in a world of quantum computing.

Atefeh Mashatan
Ryerson University
(Canada)

JOURNAL OF CYBER SECURITY TECHNOLOGY, 2017
VOL. 1, NO. 1, 1–22
http://dx.doi.org/10.1080/23742917.2016.1226650

Will quantum computers be the

Quantum Computers - An Emerging Cybersecurity Threat

The New York Times

The Race to Save Our Secrets From the Computers of the Future

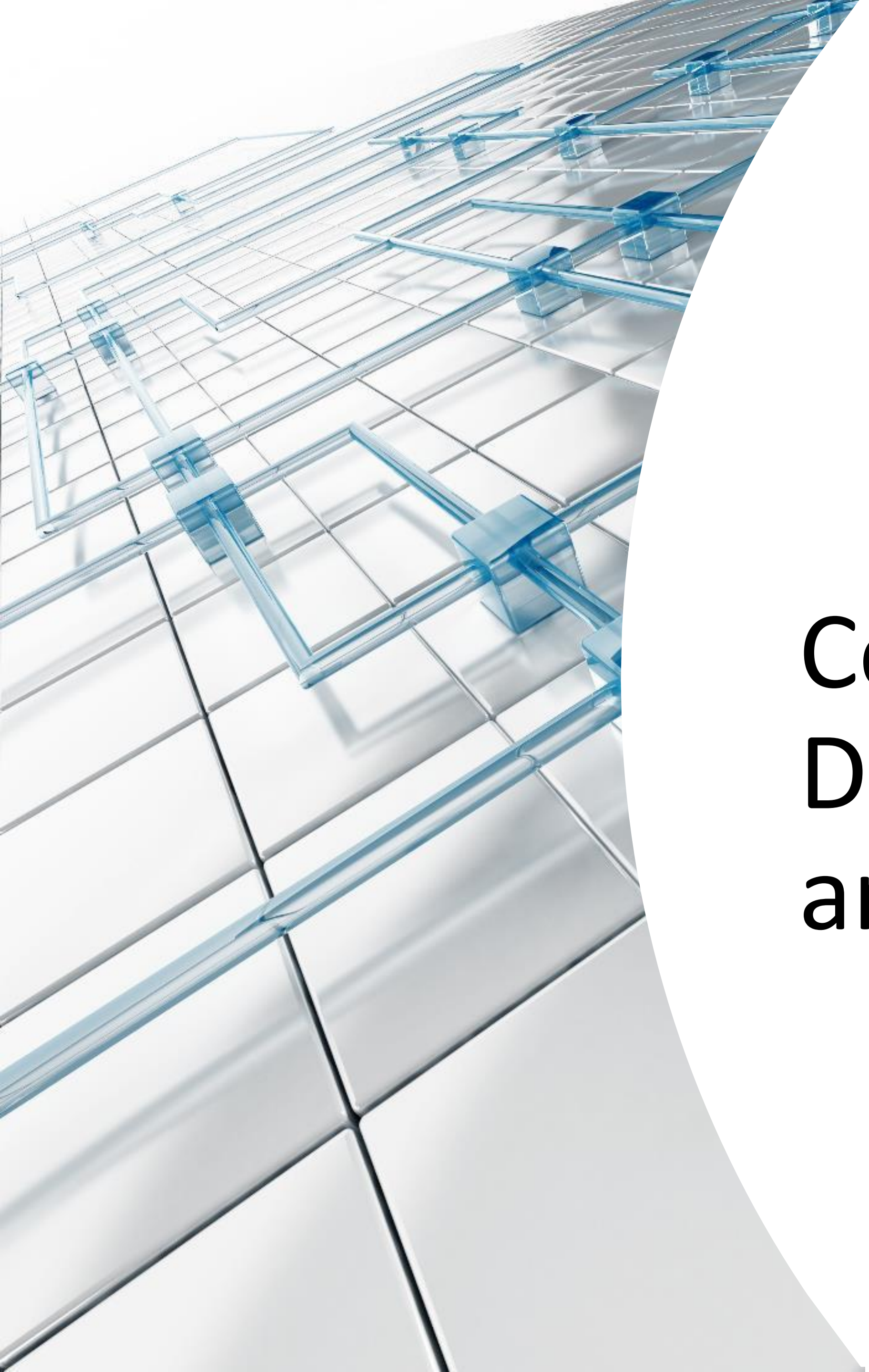
will remain valuable for a long time. The
lines on how IT departments and/or secur
form their currently quantum-vulnerable s

Atefeh Mashatan
Ryerson University
(Canada)

Gregory Mone

The Quantum Threat

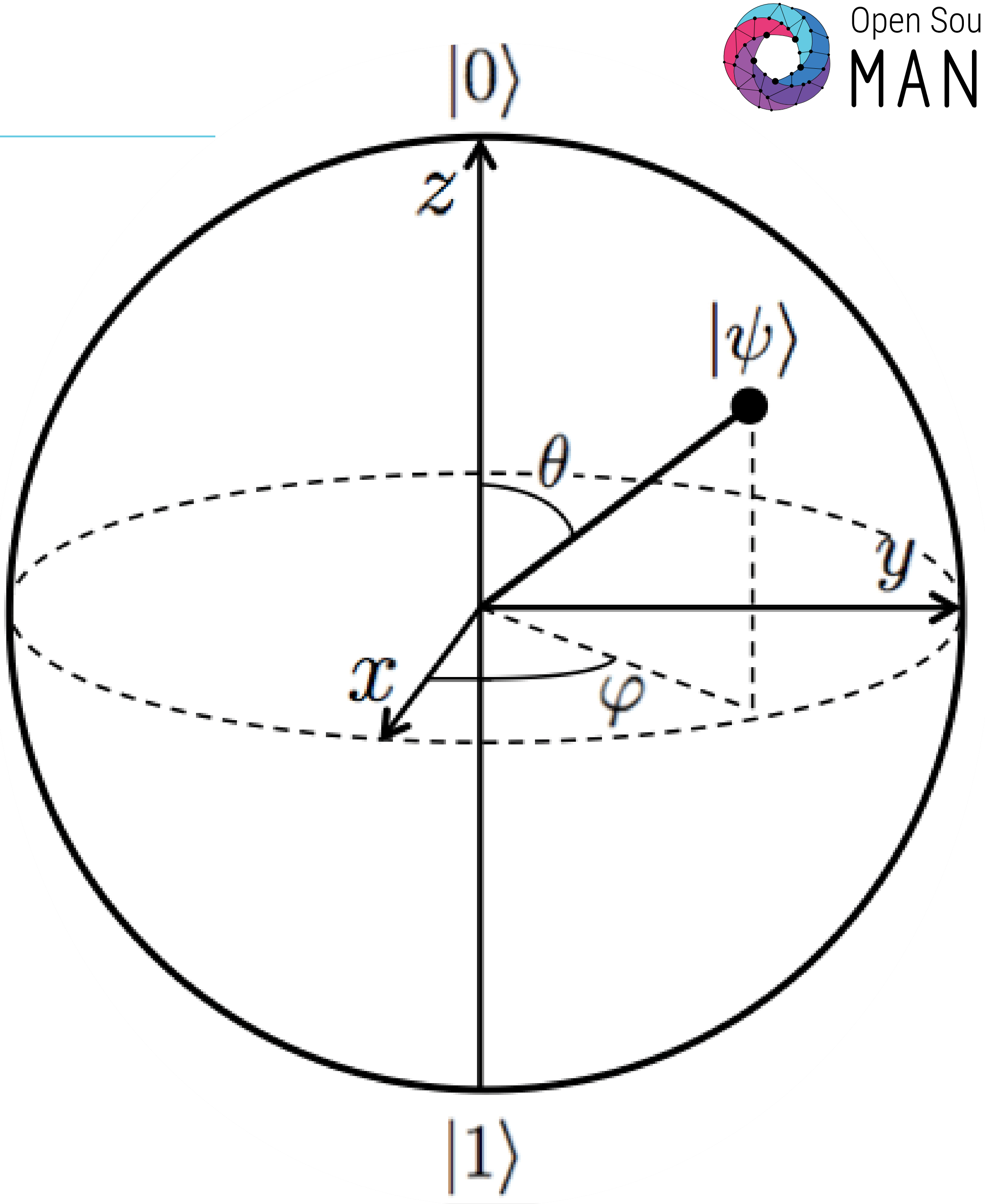
Cryptographers are developing algorithms to ensure security in a world of quantum computing.



Could Quantum Key Distribution (QKD) be the answer?

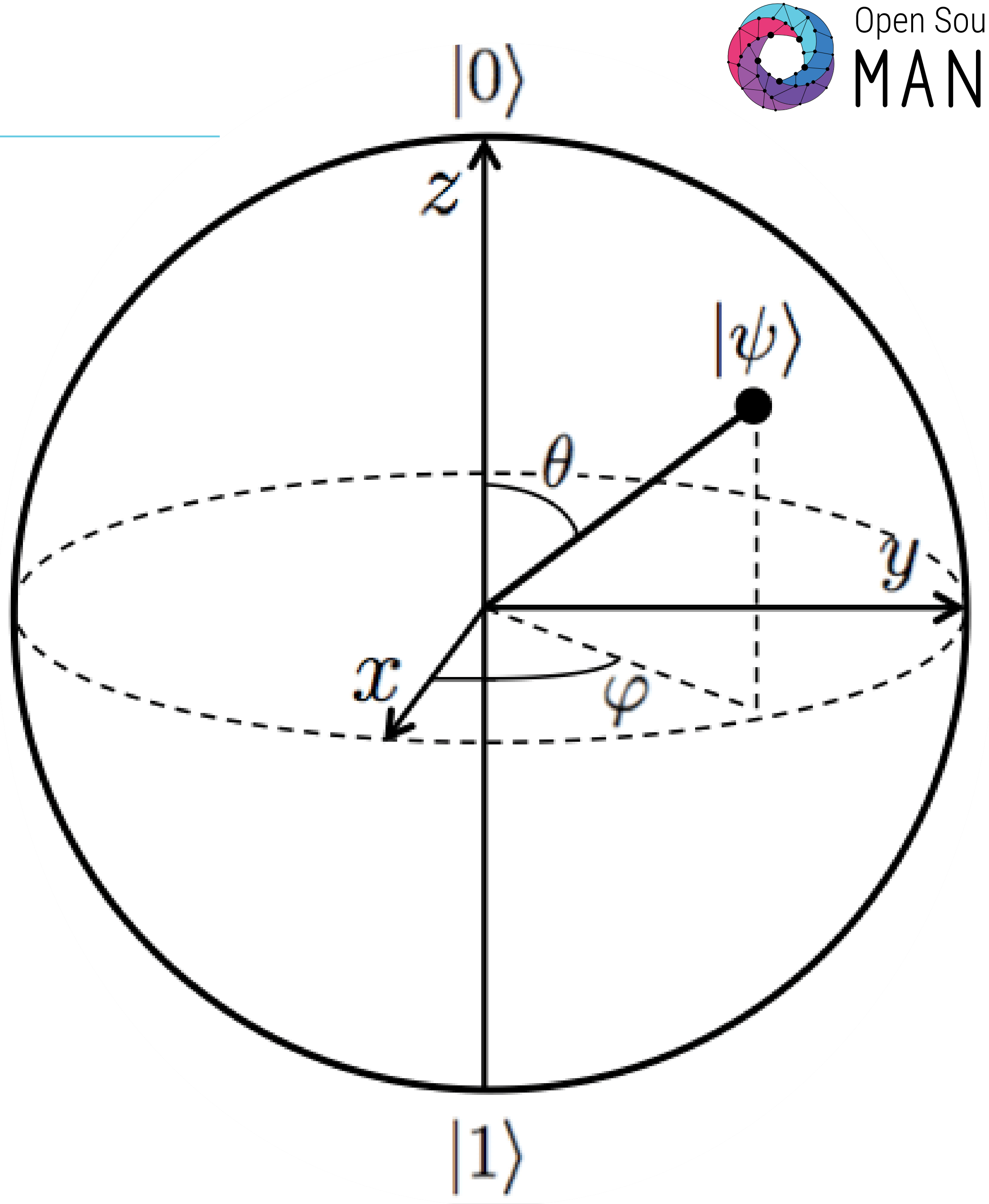
Bits vs Qubits

Bits	Qubits
States 0 or 1	Can present superposition
Can be cloned	Can **not** be cloned
----	Measurement destroys the original state
----	Can be entangled
Protocols security based in **computational assumptions**	Protocols security based in **Quantum Mechanics principles**

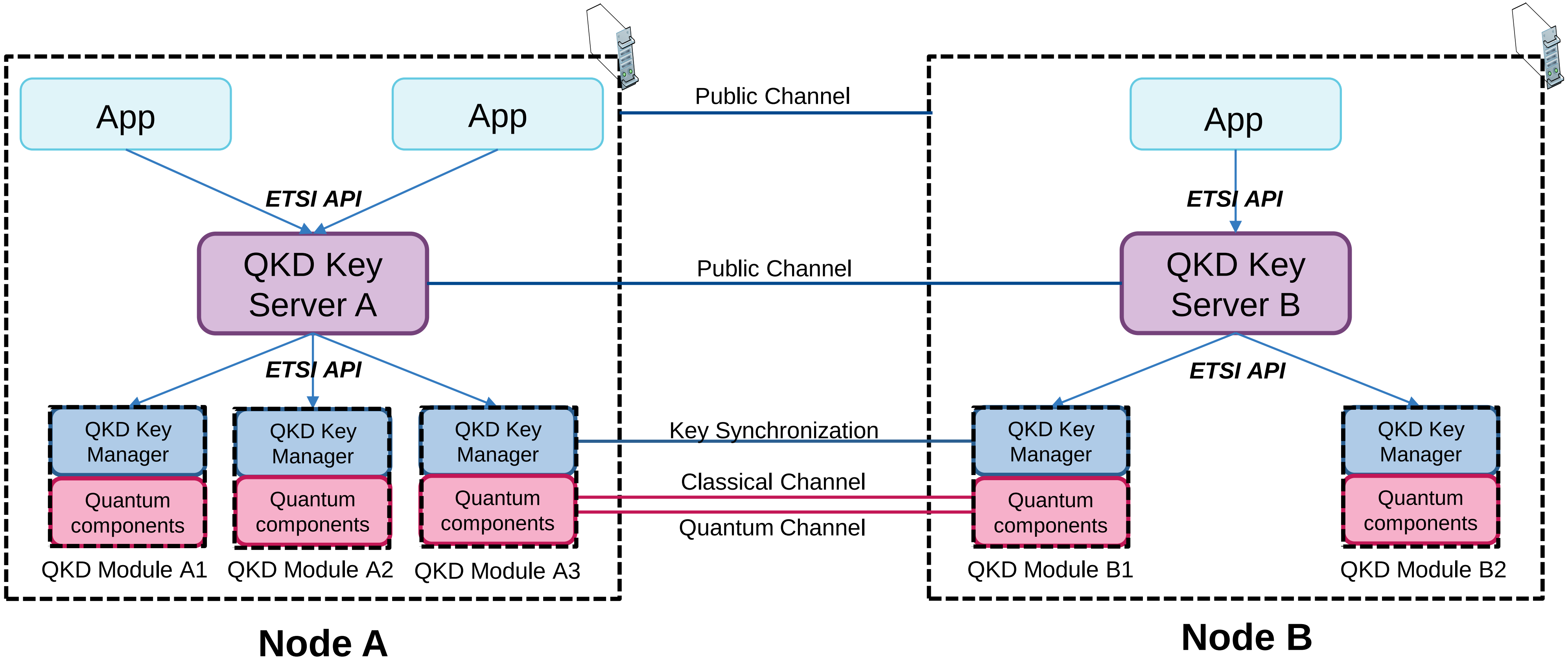


Bits vs Qubits

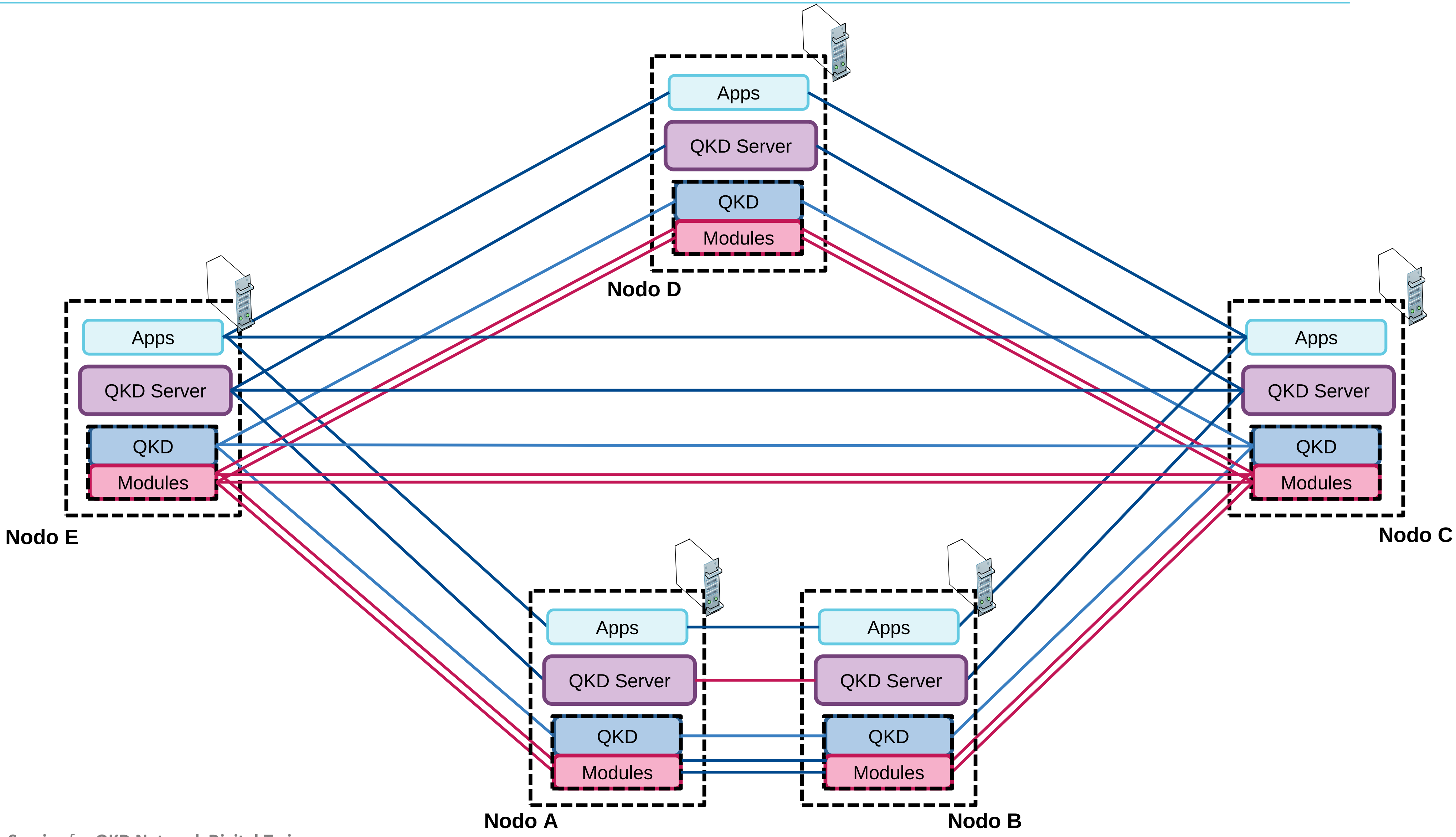
Bits	Qubits
States 0 or 1	Can present superposition
Can be cloned	Can **not** be cloned
----	Measurement destroys the original state
----	Can be entangled
Protocols security based in **computational assumptions**	Protocols security based in **Quantum Mechanics principles**
Easy to work with	**… not so easy**



QKD Networks (an example from ETSI GS QKD 004)



QKD Networks (an example from ETSI GS QKD 004)



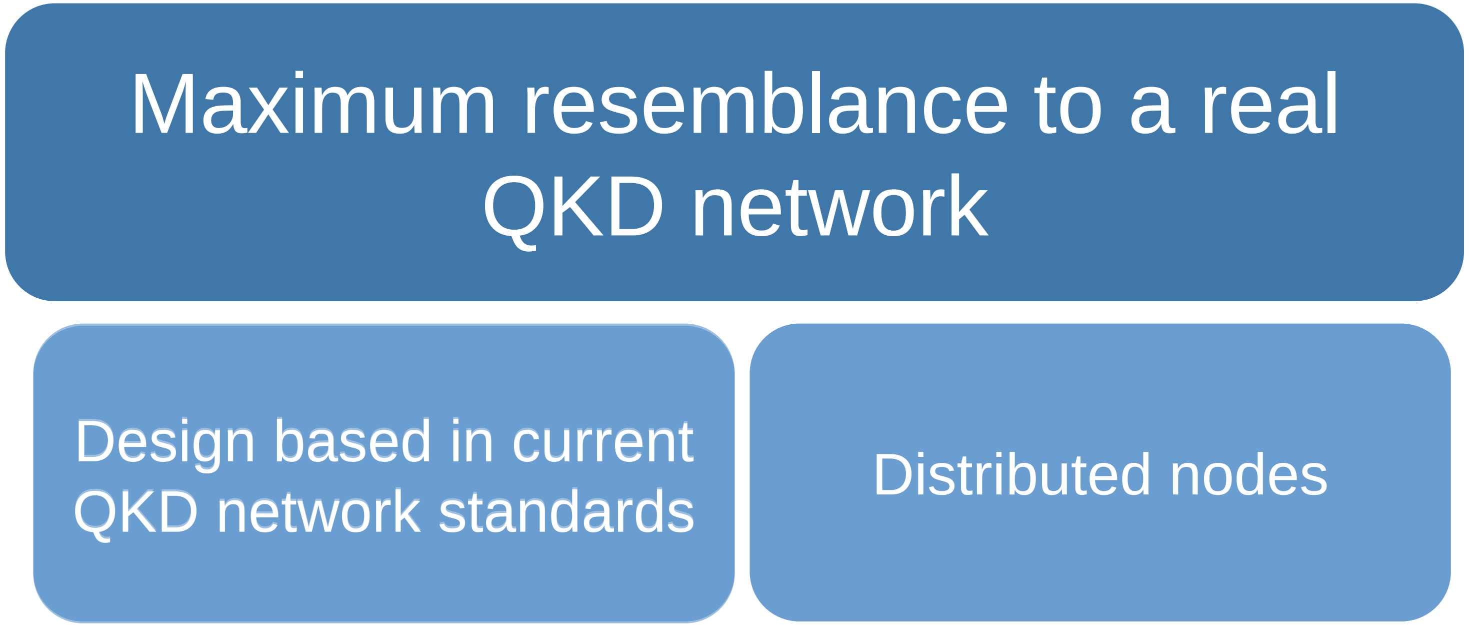
Open Source MANO

Building a Digital Twin to ease the QKD networks development

Features sought in our DT

Maximum resemblance to a real QKD network

Features sought in our DT

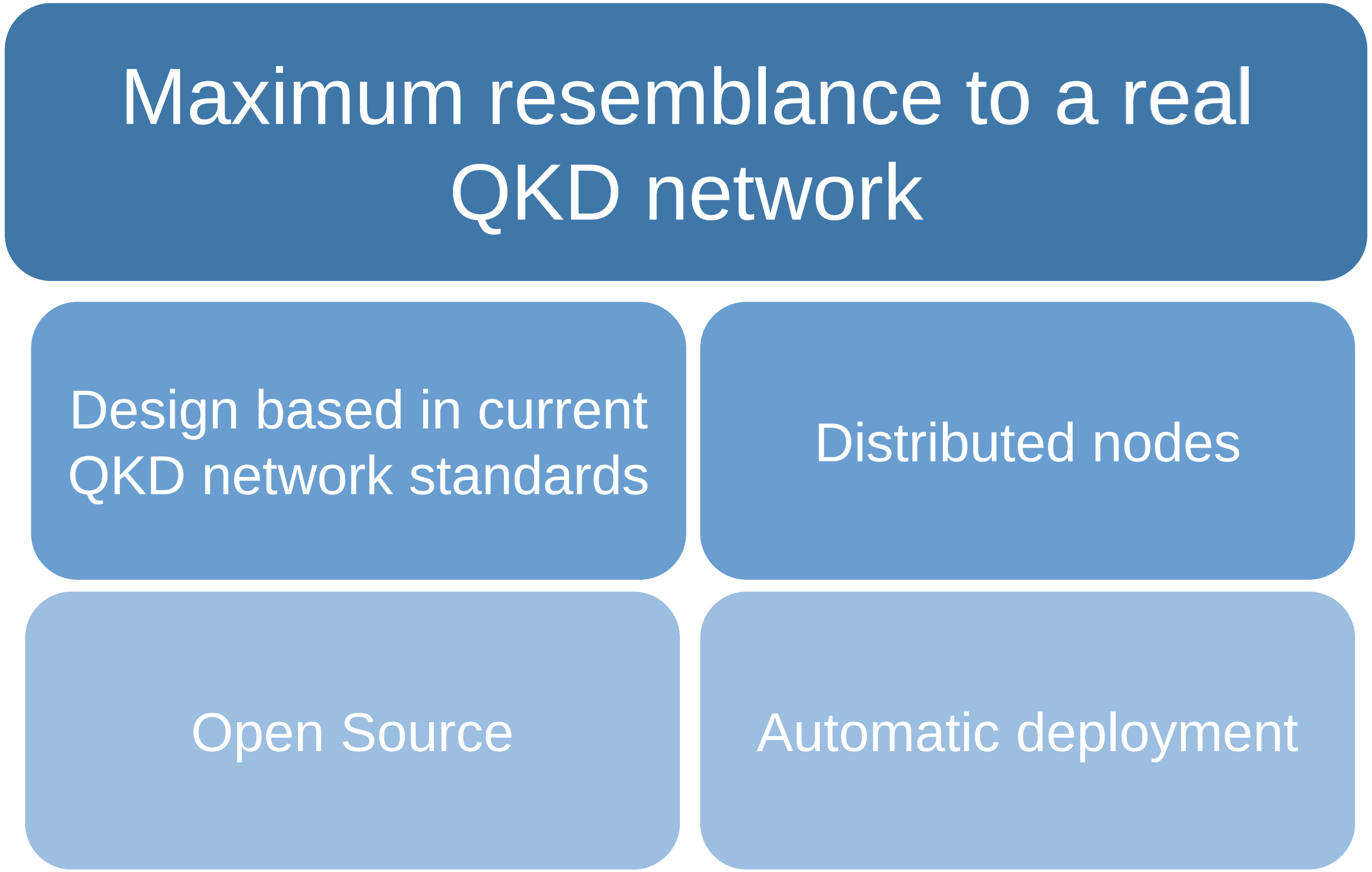


Maximum resemblance to a real QKD network

Design based in current QKD network standards

Distributed nodes

Features sought in our DT



Maximum resemblance to a real QKD network

Design based in current QKD network standards

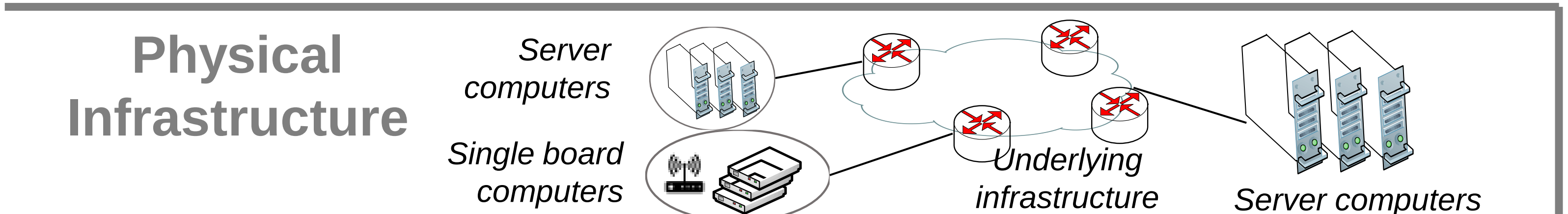
Distributed nodes

Open Source

Automatic deployment

Functioning

YAML description file



Physical Infrastructure

Server computers

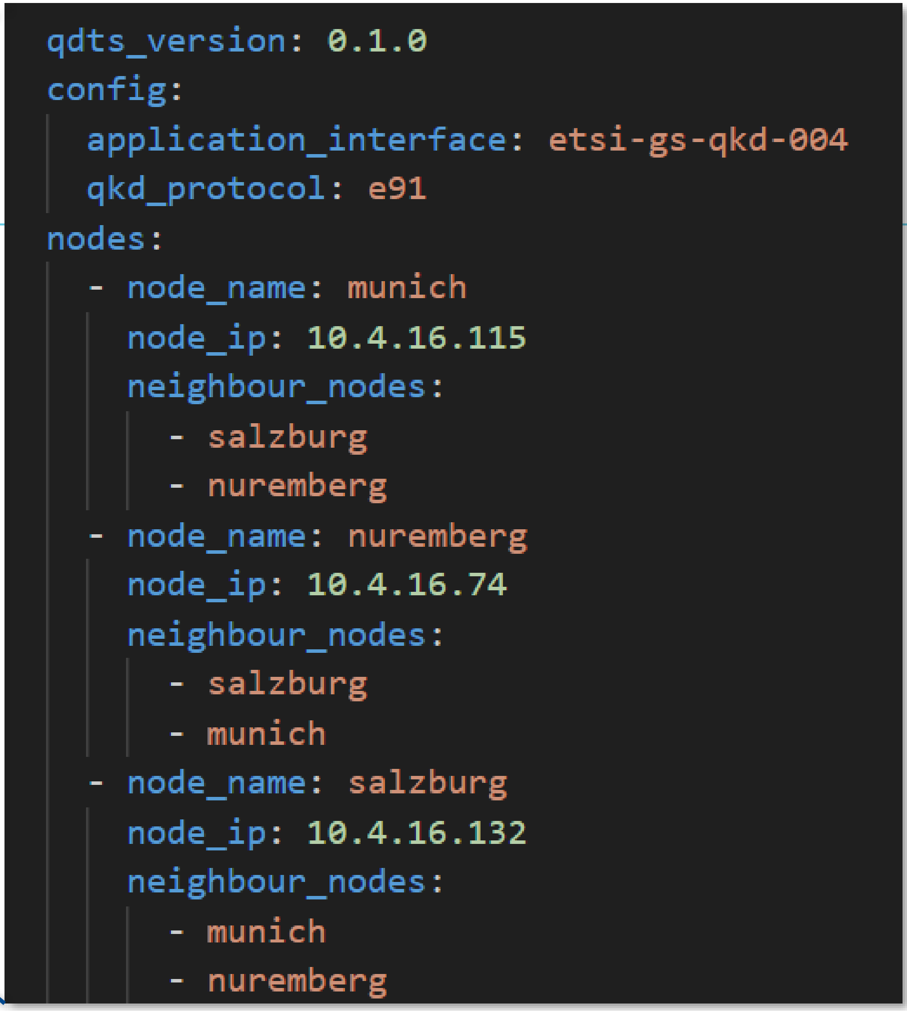
Single board computers

Underlying infrastructure

Server computers

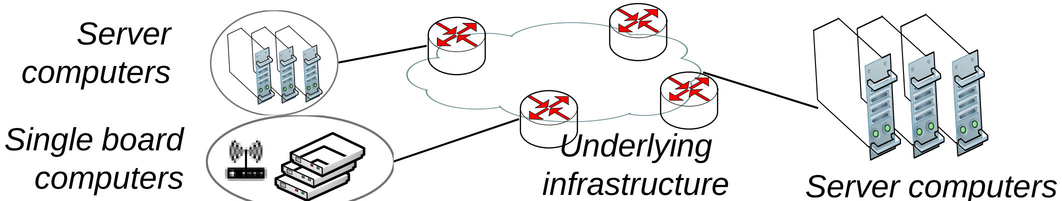
Functioning

YAML description file

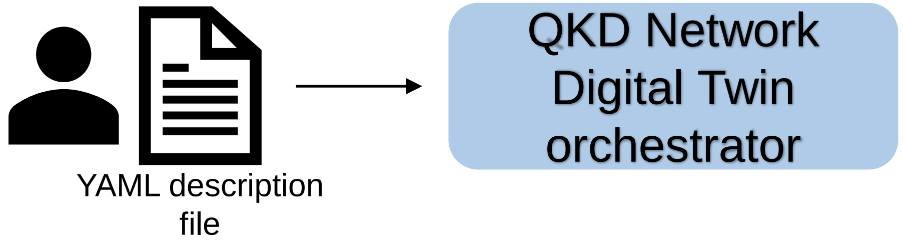


```
qdts_version: 0.1.0
config:
  application_interface: etsi-gs-qkd-004
  qkd_protocol: e91
nodes:
  - node_name: munich
    node_ip: 10.4.16.115
    neighbour_nodes:
      - salzburg
      - nuremberg
  - node_name: nuremberg
    node_ip: 10.4.16.74
    neighbour_nodes:
      - salzburg
      - munich
  - node_name: salzburg
    node_ip: 10.4.16.132
    neighbour_nodes:
      - munich
      - nuremberg
```

Physical Infrastructure

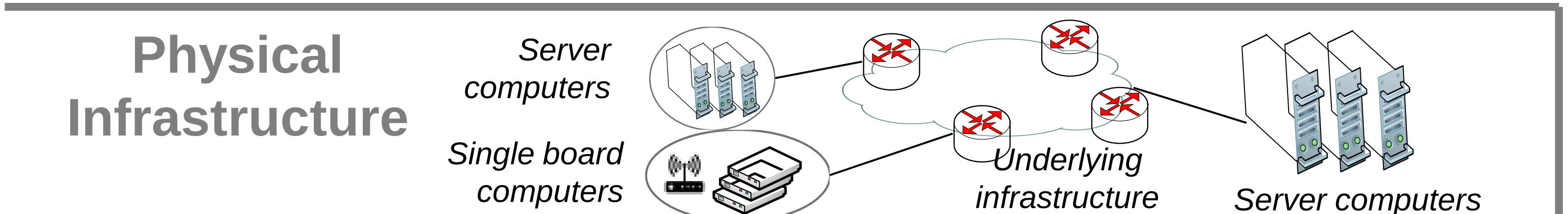


Functioning



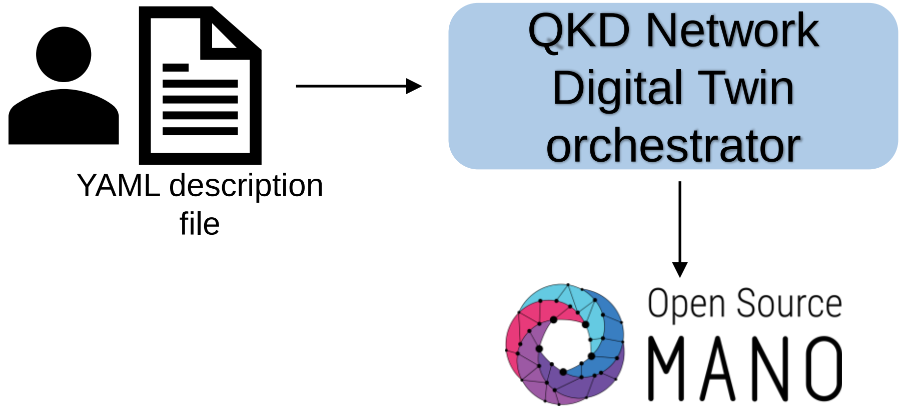
QKD Network Digital Twin orchestrator

YAML description file



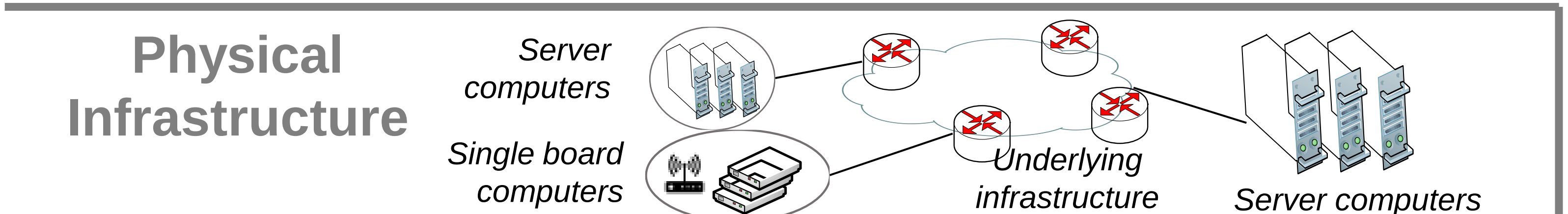
Physical Infrastructure

Functioning



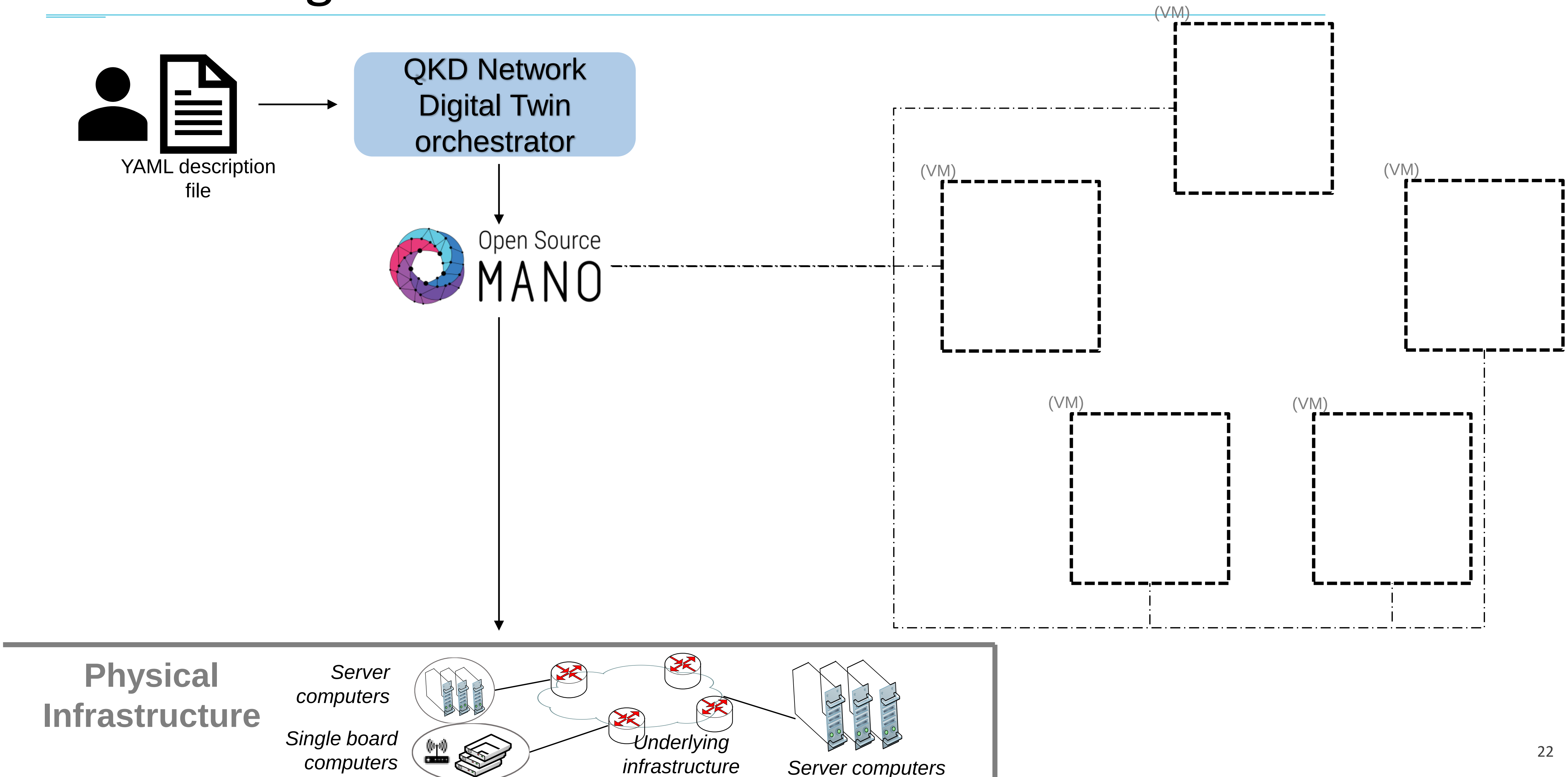
YAML description file

QKD Network Digital Twin orchestrator

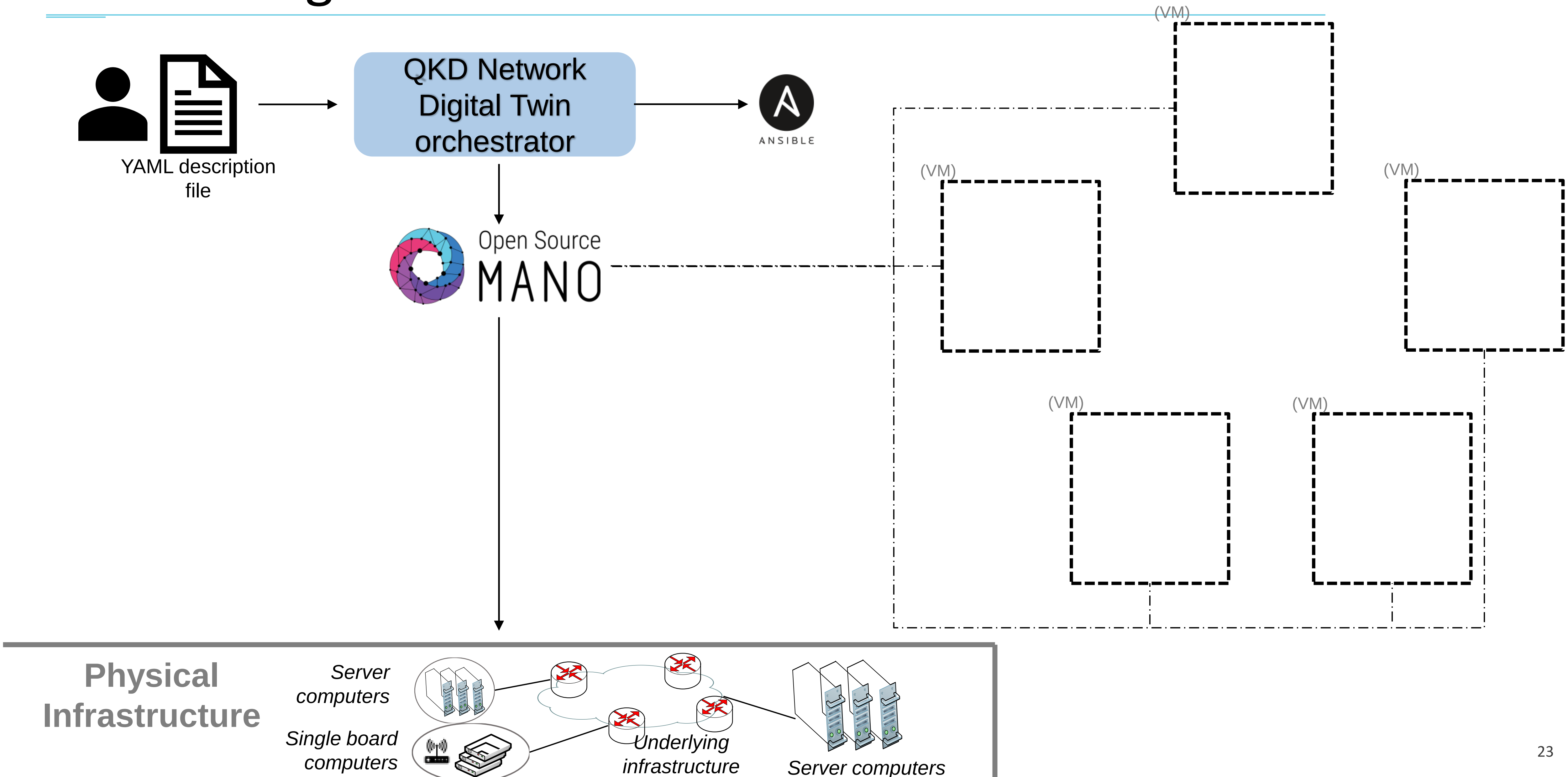


Physical Infrastructure

Functioning



Functioning



YAML description file

QKD Network Digital Twin orchestrator

ANSIBLE

Open Source MANO

(VM)

(VM)

(VM)

(VM)

(VM)

Physical Infrastructure

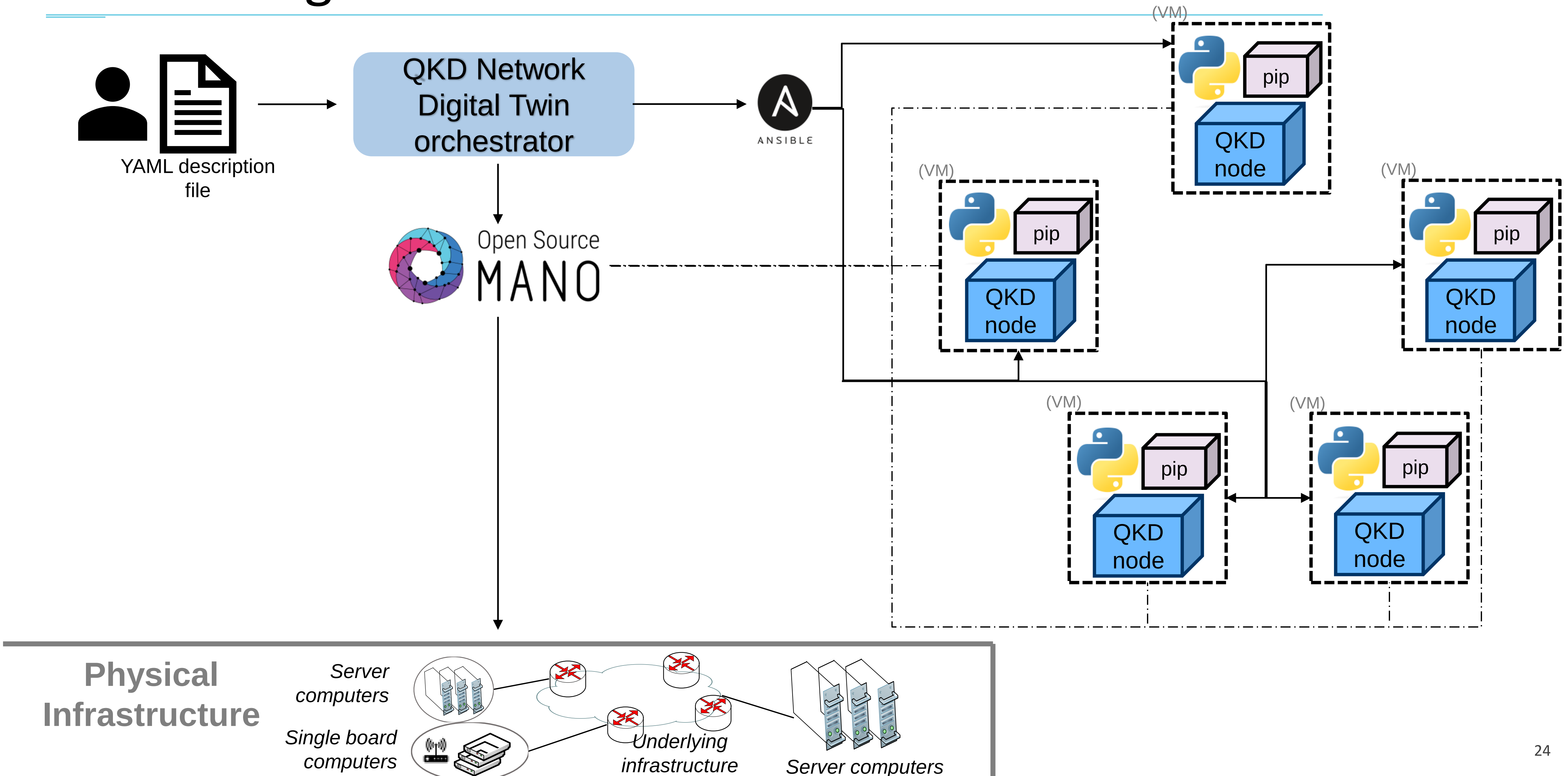
Server computers

Single board computers

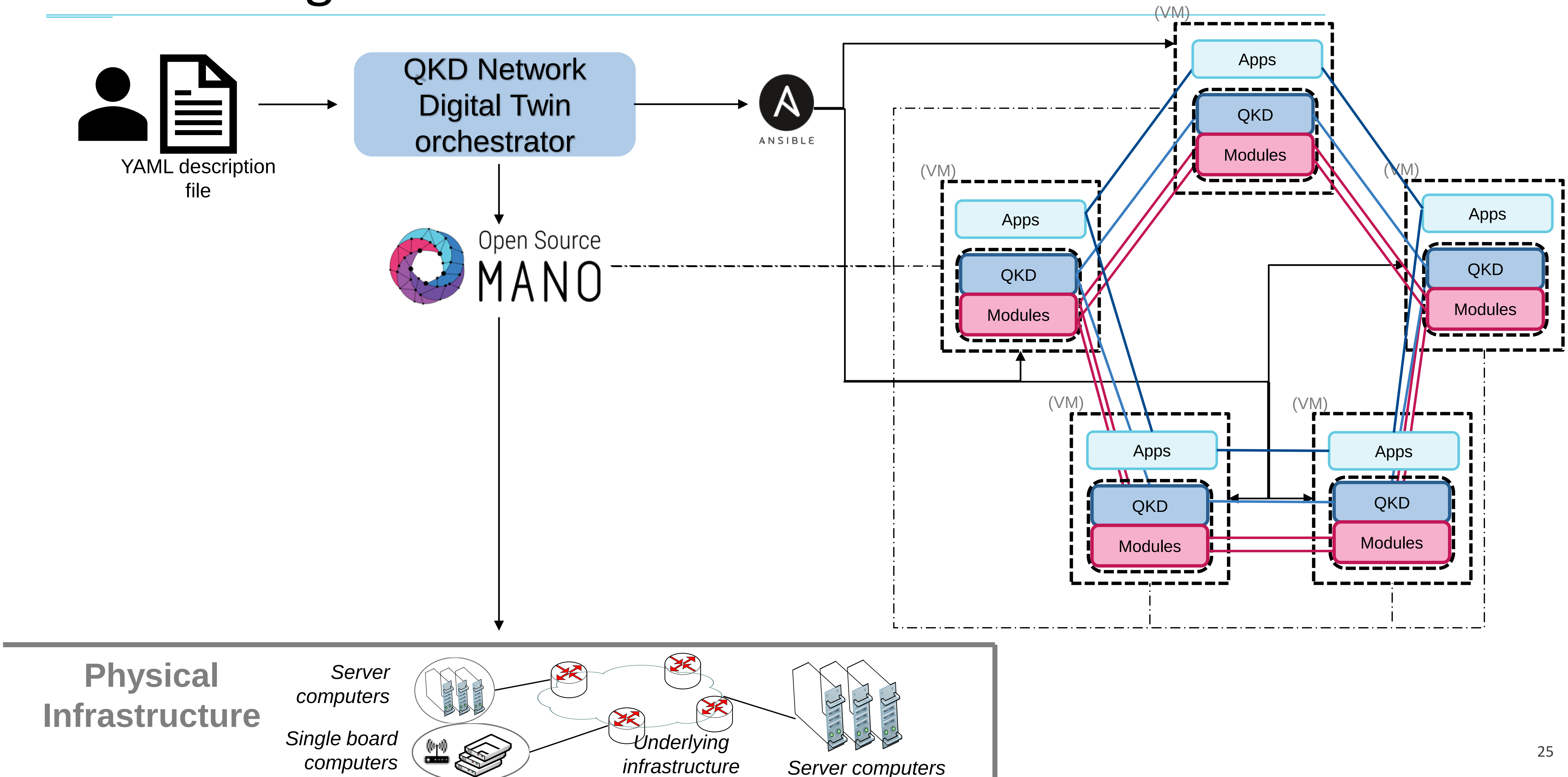
Underlying infrastructure

Server computers

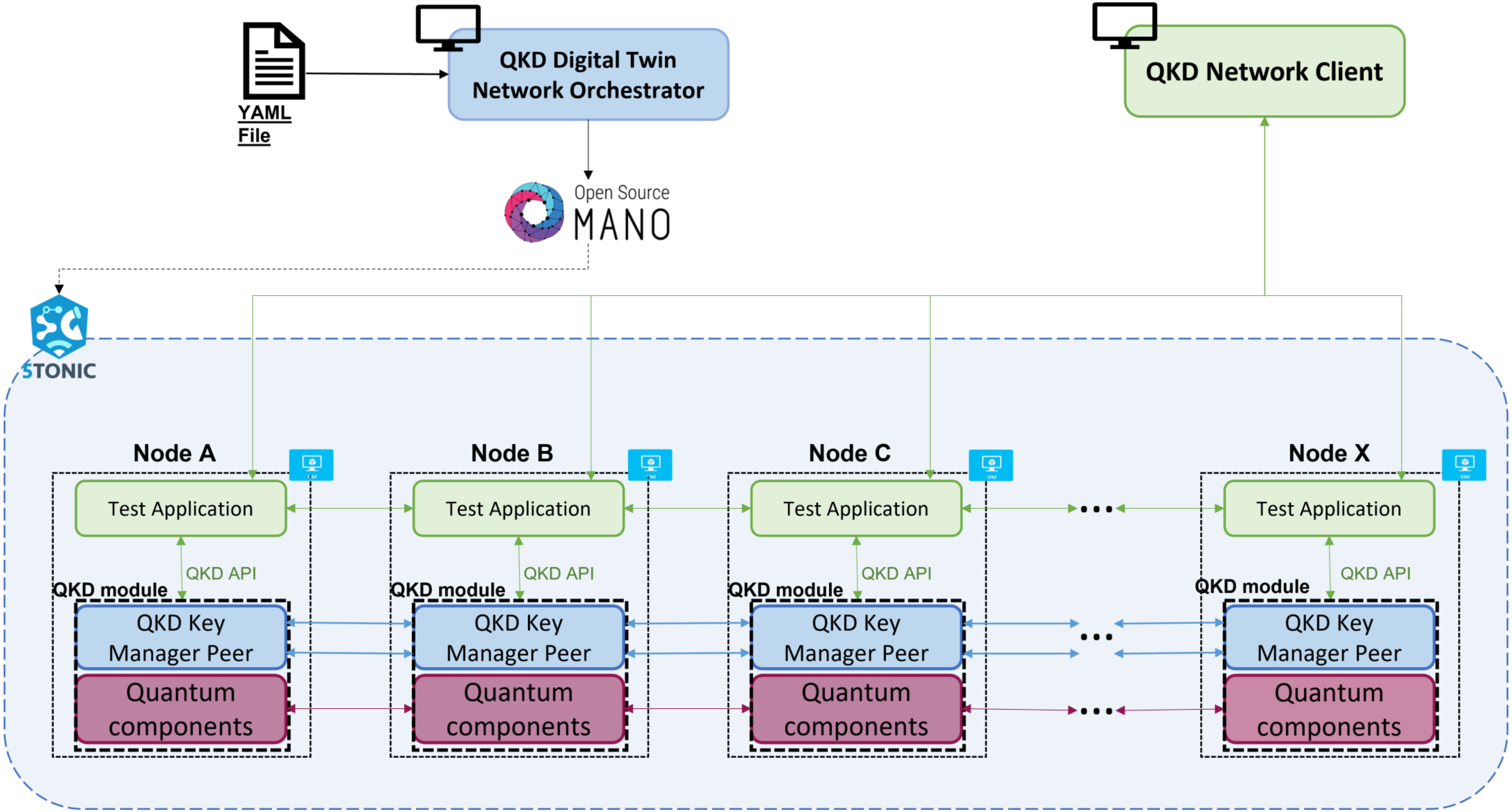
Functioning



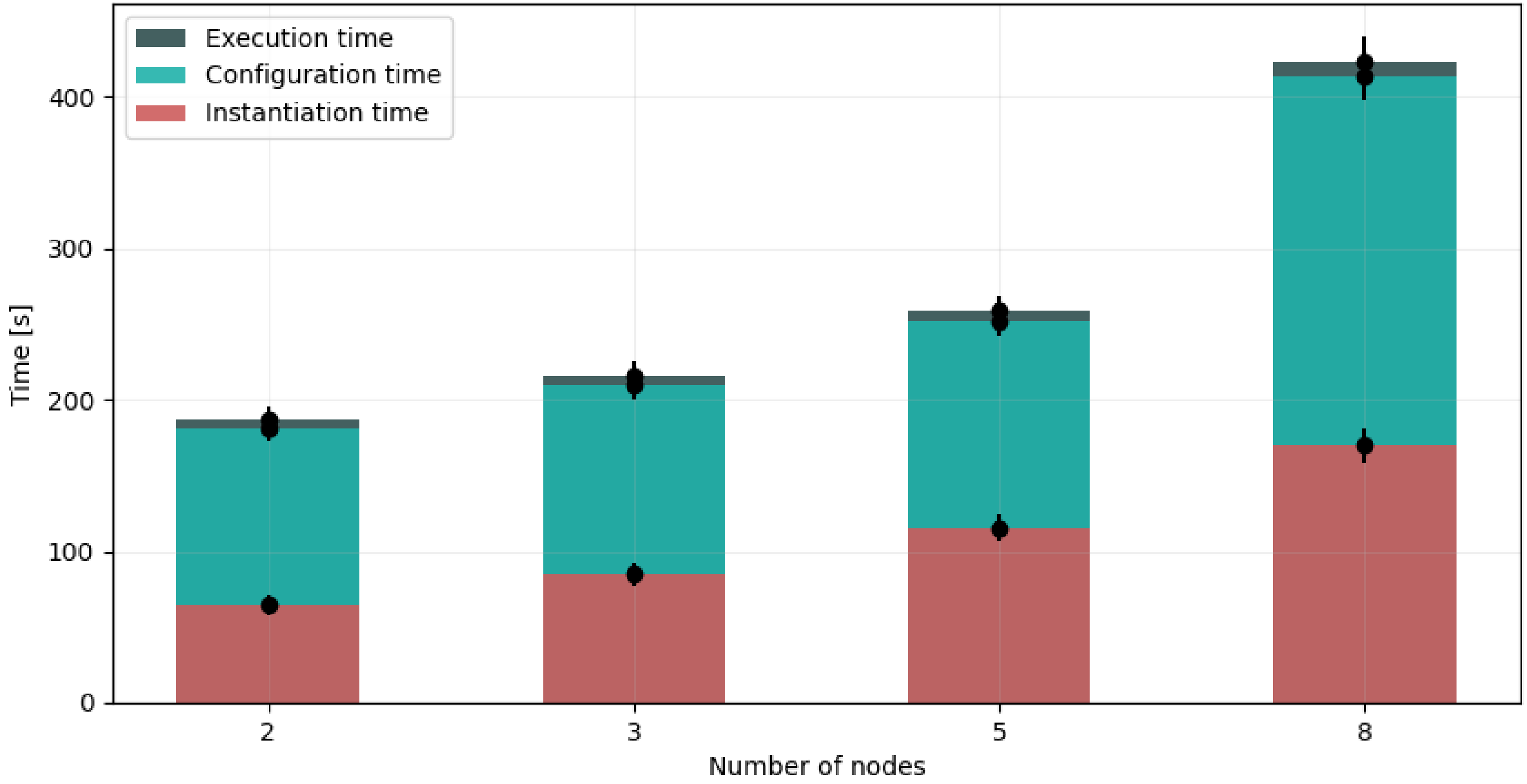
Functioning

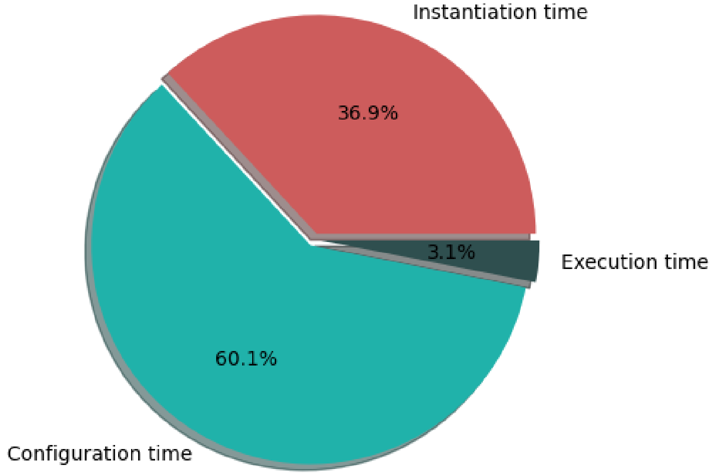


Tests and results



Tests and results





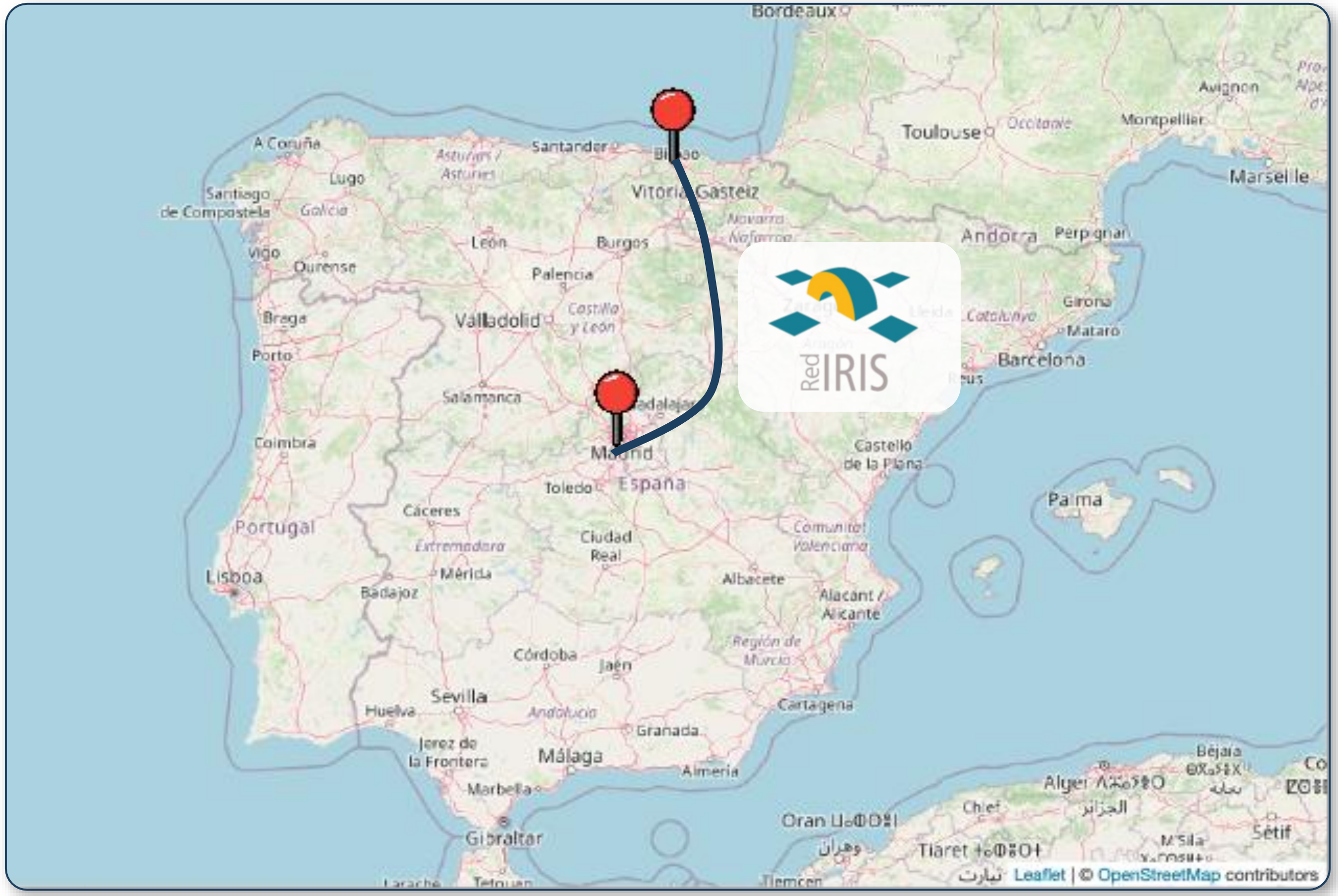
To sum up

- ✓ We now **have access to a digital twin** environment for the **development of QKD networking issues**.
- ✓ The service **can deploy, and start up, moderate sized networks** (6-10 nodes) **in 7 minutes** thanks to OSM.
- ✓ **Quantum applications can run** over the QKD network digital twin **using a standardized API**.

Next steps

- ❑ Support **hybrid deployments**.
- ❑ Add **quantum parameters**.
- ❑ Emulate **channel authentication**.
- ❑ Incoming field test!

Use case: Collaboration with EHU/UPV



Leaflet | © OpenStreetMap contributors

***Objective**: Deployment of a QKD network using the digital twin with network nodes in different locations (Madrid, Bilbao).*

- Collaboration in the context of the Spanish national project TRUE5G:
  - Universidad Carlos III de Madrid
  - Universidad del País Vasco
- Use the digital twin to emulate the automated deployment of a QKD network in which the nodes involved may span across multiple locations
- Dedicated layer-2 link: VLAN provided by RedIRIS at national scale, with a transmission rate of 10 Gbps

uc3m Universidad Carlos III de Madrid

eman ta zabal zazu Universidad del País Vasco Euskal Herriko Unibertsitatea

TRUE5G

Open Source MANO by ETSI

Thank You!

Francisco Valera
fvalera@it.uc3m.es

Iván Vidal
ividal@it.uc3m.es

Borja Nogales
bdorado@pa.uc3m.es

Blanca López
blanca.lopez@imdea.org

Raúl Martín

institute imdea networks

uc3m | Universidad Carlos III de Madrid