العطاء الرقمي
Attaa Digital

Women in Cyber Security Middle East
رابطة نساء الشرق الأوسط للأمن السيبراني

تبسيط تقنية البلوكتشين

الثلاثاء | 1 سبتمبر

9-8 م

المحاور

حول تقنيةالبلوكتشين:
- تاريخها ووظائفها الأساسية
- أنواعها
- ميزاتهاوفوائدها

عرض حالة خاصة لتطبيق تقنية البلوكتشين في مجال الأمن السيبراني

أمثلة رائدة لتطبيق تقنية البلوكتشين بطرق مختلفة

دور تقنية البلوكتشين في أزمة COVID-19

للتسجيل https://attaa.live/view/181

أ. إيمان علي لياقت

- محللة أبحاث في DinarStandard
- تخصص دقيق في مجالات التقنيات الصناعية الرابعة كتقنية البلوكتشين وإنترنت الأشياء
- مؤلفة فصل من كتاب: الذكاء الاصطناعي (تحفيز التكنولوجيا في الشؤون الإنسانية)

Women in Cyber Security Middle East (WiCSME)

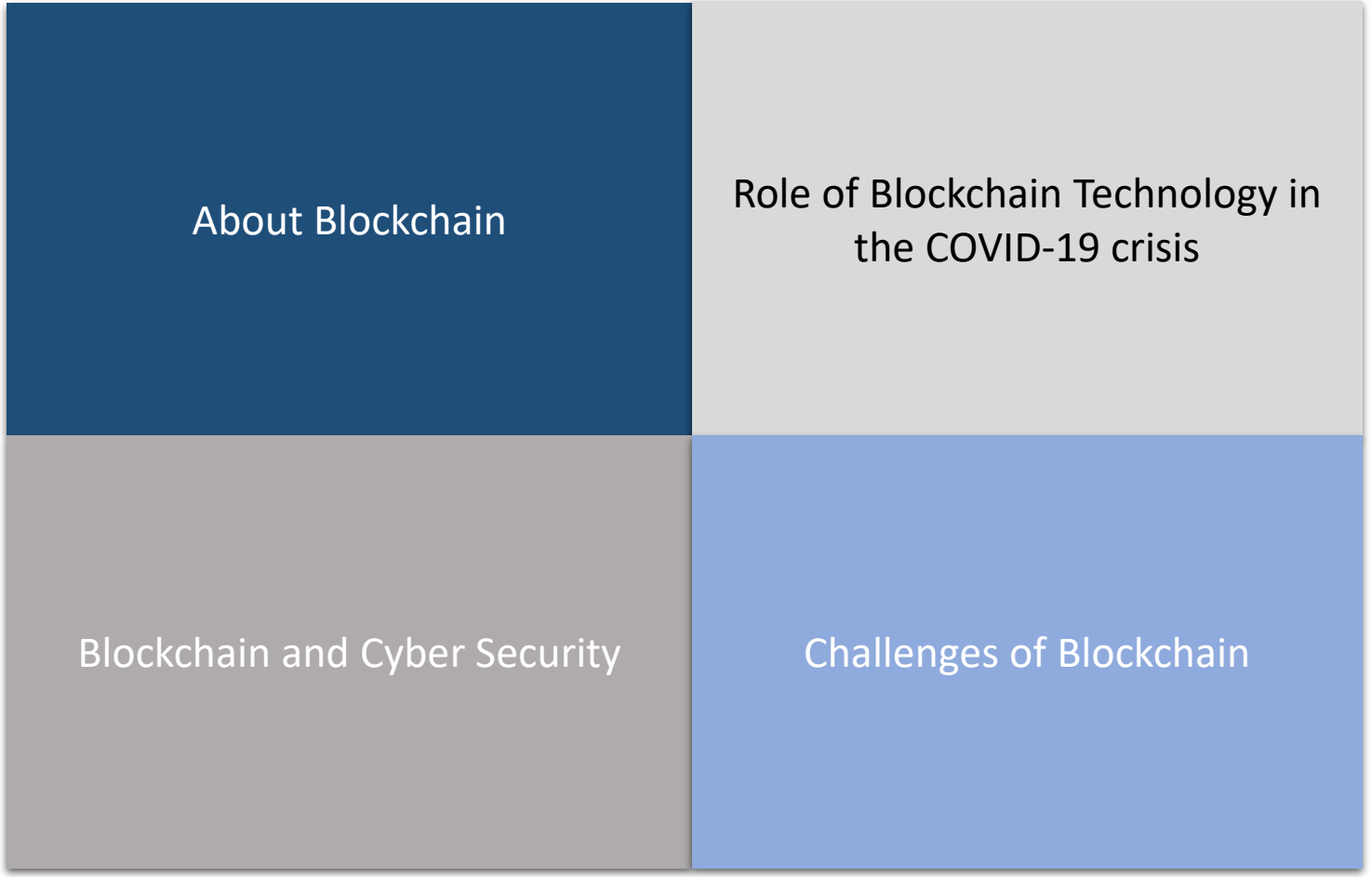
Iman Ali Liaqat
Advocate and Member of WiCSME Group
Research Analyst at DinarStandard

1st September 2020;
Saudi BootCamp

Women in Cyber Security Middle East
رابطة نساء الشرق الاوسط للأمن السيبراني

DEMYSTIFYING THE BLOCKCHAIN TECHNOLOGY
تبسيط تقنية البلوكتشين

Women in Cyber Security Middle East
رابطة نساء الشرق الاوسط للأمن السيبراني



DEMYSTIFYING THE BLOCKCHAIN TECHNOLOGY
تبسيط تقنية البلوكتشين

Women in Cyber Security Middle East
رابطة نساء الشرق الاوسط للأمن السيبراني

About Blockchain	Role of Blockchain Technology in the COVID-19 crisis
Blockchain and Cyber Security	Challenges of Blockchain

Blockchain

/ˈblɒktʃeɪn/

noun

1. Blockchain is a Distributed Ledger Technology that provides a single, immutable ledger of transactions across the network which are time-stamped and stored in “blocks”

```
GLOBAL STATE OF BLOCKCHAIN
{
“Worldwide spending on blockchain solutions 2020”:
“US$ 4.3 billion”

“Popular use cases:”
“Digital Currency”
“Data Sharing”
“Payments”
“Track-and-trace”
“...”
}
```

Source: Statista, Deloitte

Women in Cyber Security Middle East
رابطة نساء الشرق الاوسط للأمن السيبراني

Blockchain

/ˈblɒktʃeɪn/

noun

1. Blockchain is a Distributed Ledger Technology that provides a single, immutable ledger of transactions across the network which are time-stamped and stored in "blocks"

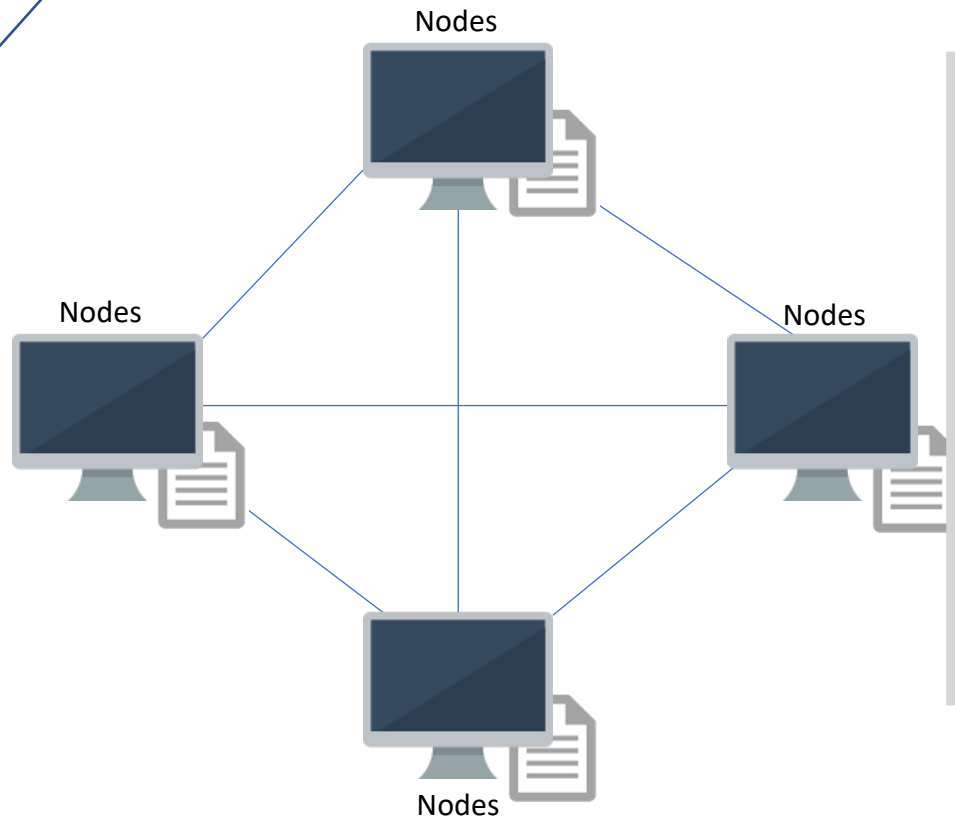
- *Public Key Infrastructure (PKI)*
- *Only those **authorized** to.*
- *"50% rule"*

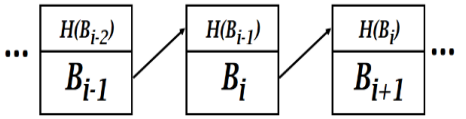
WHAT?

system 1. Decentralized & distributed ledger
nodes 2. Consensus mechanism
data 3. Immutable/ unchangeable

HOW?

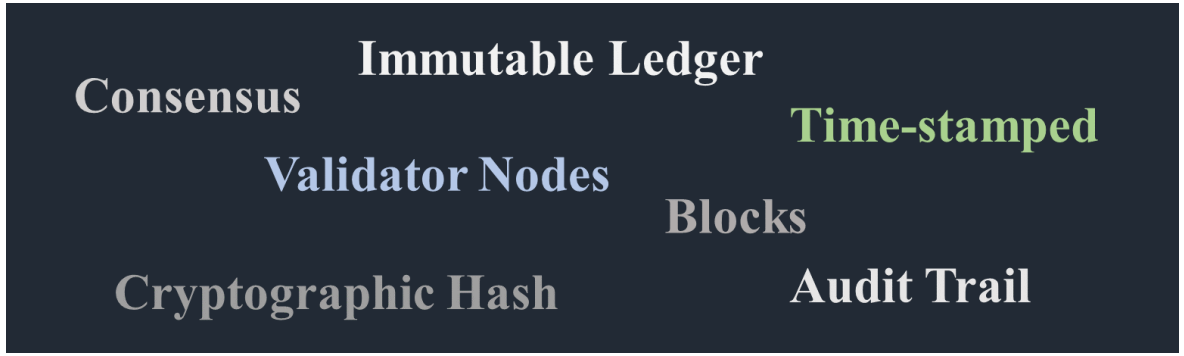
Public Key Infrastructure (PKI)
Cryptographic hash algorithms





Each block contains its own hash and is linked with the hash of the preceding block

Key Features



Public Blockchain

Permissionless, completely decentralized ledger technology.

Cryptocurrencies
Bitcoin

Private Blockchain

Permissioned, centralized ledger confined to an organization, where high privacy needed

Ripple (XRP), Hyperledger

Consortium Blockchain

Permissioned, decentralized ledger, connecting several organizations on one platform

Supply chain management, eGovernment

Provenance

Select Case Studies

Industry	Project	Application
Financial Services	EY - Nightfall	**Privacy:** Enable enterprise users to transact securely and privately on the public blockchains using *Zero Knowledge Proof (ZKP),* which allows users to prove certain items are true without revealing the underlying information. **Cuts the cost per transaction to around US$0.05.**
Cryptocurrency	Bitcoins	**Decentralize:** Launched in 2009, first to use blockchain and is the world's largest cryptocurrency by market cap. From $0.0008 per bitcoin when first launched, now it is **valued at around $11,893.**
Regulations/ e-government	Aber digital currency	**Clearing & settlement:** In Jan 2019, the central banks of Saudi Arabia and the UAE jointly launched a digital currency trial, called "Aber," to facilitate blockchain-based financial settlements between the two countries. **The goal is to reduce remittance costs.**
Supply chain	Everledger	**Traceability:** By combining blockchain technology with AI, IoT, and nanotechnology, Everledger create a digital twin of every diamond, **enabling traceability in a secure, unalterable, and private platform.**

Women in Cyber Security Middle East
رابطة نساء الشرق الاوسط للأمن السيبراني

…Select Case Studies continued

Industry	Project	Application
Halal Industry	WhatsHalal	**Trust:** Seeking to **connect the entire supply chain from producers to consultants, auditors and certifying bodies**, working in Singapore and Indonesia. Successfully raise $4.5 million in seed investment.
Education	University of Bahrain	**Digital certificate:** One of the first universities globally to issue digital credentials anchored to the blockchain, using the *Blockcerts.* **Issued over 400 credentials to students** who recently graduated from the university's digital Academy.
Social Impact	Alipay	**Transparency:** "Charities on chain (CoC)" - Alipay has created a blockchain-based solution that **helps charitable organizations collaborate** more efficiently and transparently, and track donations. Aim to raise more than 200 million yuan ($28 million).

Source: The Gbbc 2020 Annual Report - Chain Reaction: Blockchain Enters The Mainstream

DEMYSTIFYING THE BLOCKCHAIN TECHNOLOGY
تبسيط تقنية البلوكتشين

Women in Cyber Security Middle East
رابطة نساء الشرق الاوسط للأمن السيبراني

About Blockchain	Role of Blockchain Technology in the COVID-19 crisis
Blockchain and Cyber Security	Challenges of Blockchain

Role of Blockchain in COVID-19 recovery

Source: DinarStandard Insights Brief - 15 Signals of a Post-COVID-19 'New Normal' for Government policy & function

Supply chain disruption

Impact: The COVID-19 crisis has caused major disruptions across global supply chains: (1) closure of **factories and transport**, (2) unprecedented **demand** for certain goods, like medical supplies and healthy food.

How Blockchain can help?

By providing: Trust, real-time data sharing, security, improve efficiency & accountability .

SME's in crisis

Impact: SME's account for 99% of all businesses and generate 60% of employment[1].
Due to **inefficiencies in traditional banking system** and a US$ 1.5 trillion global trade finance gap, SME's are further hit by the crisis[2], greatly impacting employment as well.

How Blockchain can help?

By providing new SME trading opportunities, ensure transparency, speed settlement, reduce risk through better regulatory compliance, and reduce costs through eliminating intermediaries

Sources: 1. OEDCiLibrary, 2. Asian Development Bank

Women in Cyber Security Middle East
رابطة نساء الشرق الاوسط للأمن السيبراني

Blockchain can help governments accelerate opportunities for "New Normal"

15 Signals of a Post-COVID-19 "New Normal" for Governments

The 15 signals presented here are based on our analysis of population, industry, and government function trends in the wake of Covid-19, that will together create the post-Covid-19 "new normal." These are categorized by six government function divisions using the Classification of the Functions of Government (COFOG) developed by the OECD.

Health

1. Stress-tested future crisis/ pandemic response

Education

2. Institutionalized flex education

Social protection

3. Mass scale mental health support
4. Heightened attention to at-risk population segments
5. Universal basic income and talent pool alignment

Economic affairs

6. Trade policy realignments
7. Response preparedness for chronic industry segments
8. Accelerating economies digital transformation
9. Engaging and regulating non-gov mass tech platform players
10. Enabling new working lifestyles

General public services

11. Active/ proactive investment role in economy
12. Accelerated automation of government services
13. Heightened trust building measures with communities
14. Stronger international coordination

Environmental protection

15. Strengthened green standards/ climate impact goals

Source: DinarStandard

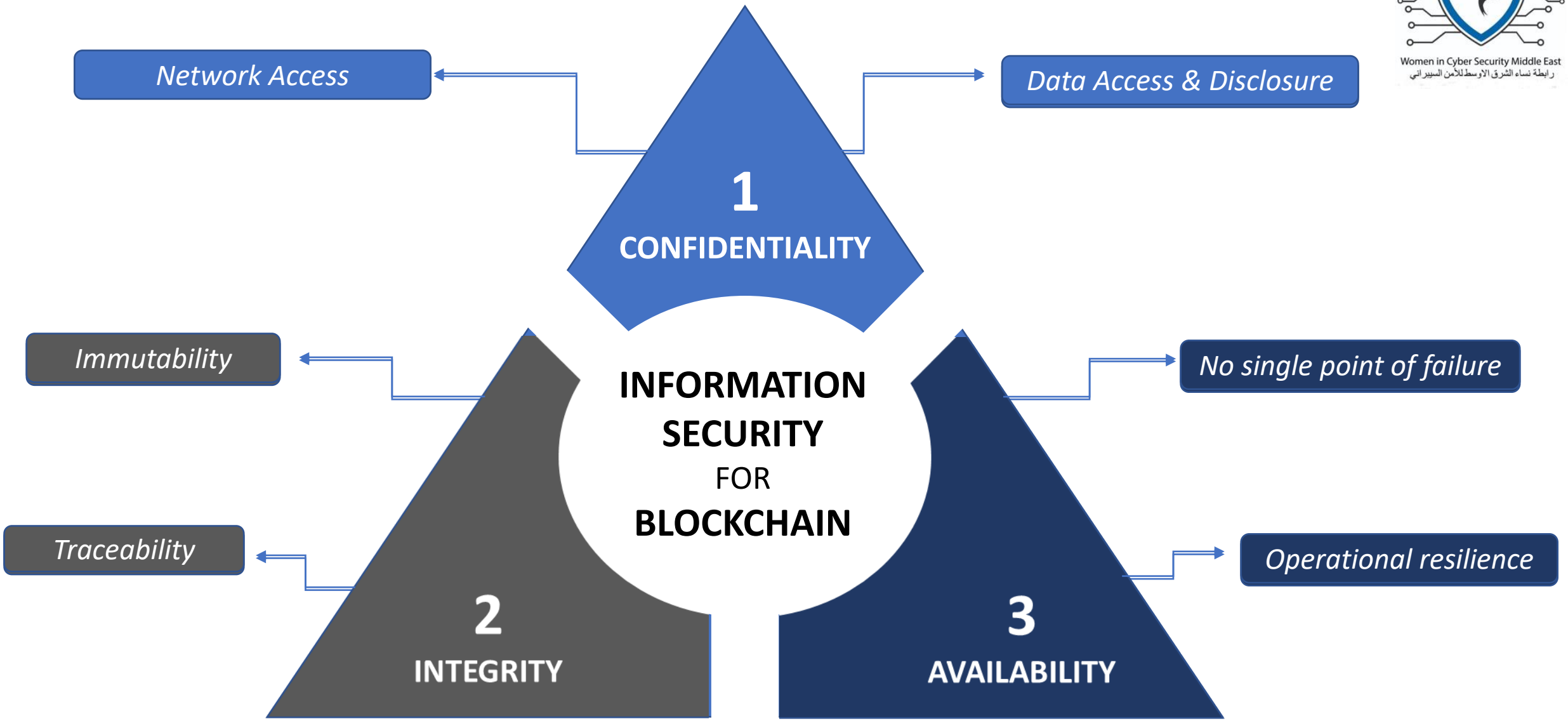
15 Signals of a Post-COVID-19 New Normal: Government Policy & Function © DinarStandard June 2020 8

Source: DinarStandard Insights Brief - 15 Signals of a Post-COVID-19 'New Normal' for Government policy & function https://dinarstandard.com/

DEMYSTIFYING THE BLOCKCHAIN TECHNOLOGY
تبسيط تقنية البلوكتشين

Women in Cyber Security Middle East
رابطة نساء الشرق الاوسط للأمن السيبراني

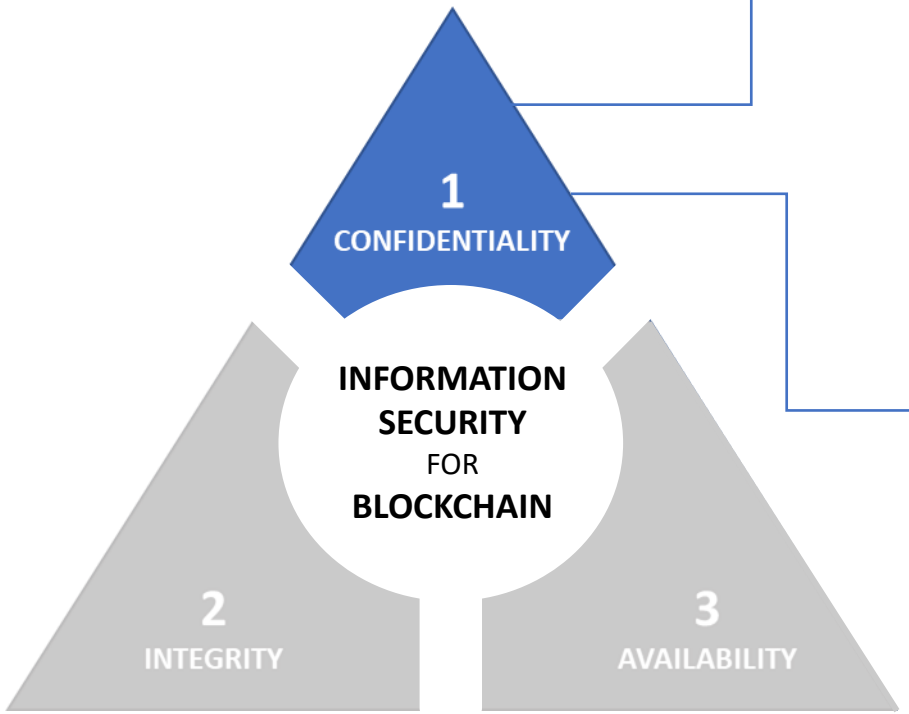
About Blockchain	Role of Blockchain Technology in the COVID-19 crisis
Blockchain and Cyber Security	Challenges of Blockchain


Network Access
Data Access & Disclosure
1
CONFIDENTIALITY
Immutability
INFORMATION SECURITY
FOR
BLOCKCHAIN
No single point of failure
Traceability
2
INTEGRITY
3
AVAILABILITY
Operational resilience

Women in Cyber Security Middle East
رابطة نساء الشرق الاوسط للأمن السيبراني

```
Confidentiality

C:\National Institute of Standards and Technology (NIST)\> the property that sensitive
information is not disclosed to unauthorized individuals, entities, or processes.
```



Network Access

Public key infrastructure (PKI) to authenticate and authorize parties

Data Access & Disclosure

End to end encryption - where only those who have authorization to access the encrypted data can access it

Risk: theft of private keys

Future: Quantum computing

Women in Cyber Security Middle East
رابطة نساء الشرق الاوسط للأمن السيبراني

```
Integrity

C:\NIST\> guarding against improper information modification or destruction and includes
ensuring information non-repudiation and authenticity.
```

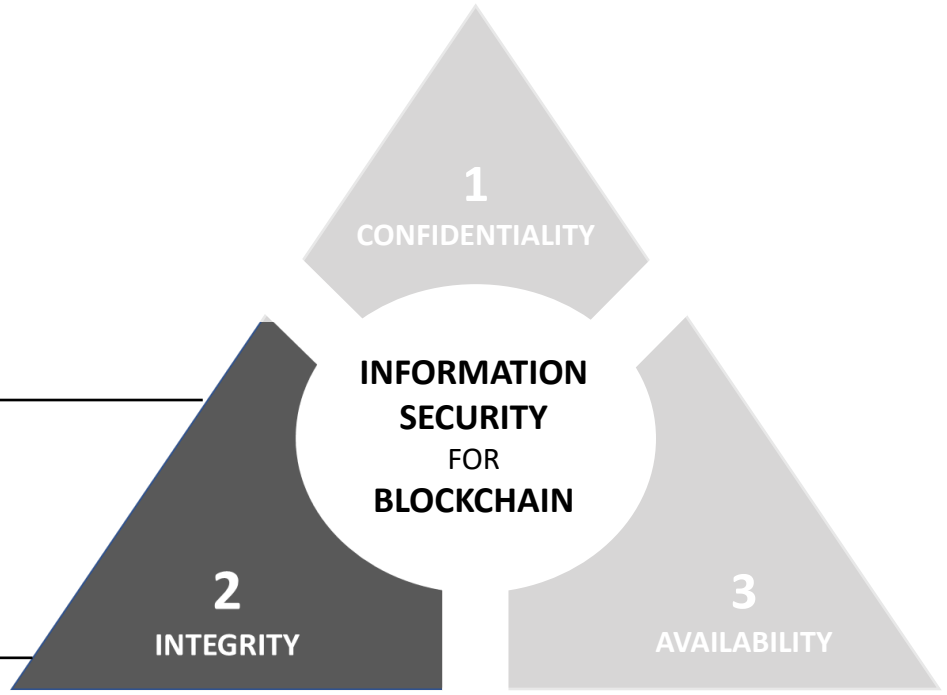
Immutability

combination of sequential **hashing and cryptography, decentralized structure and consensus model protocols** present organizations with a further level of assurance over the security of the data

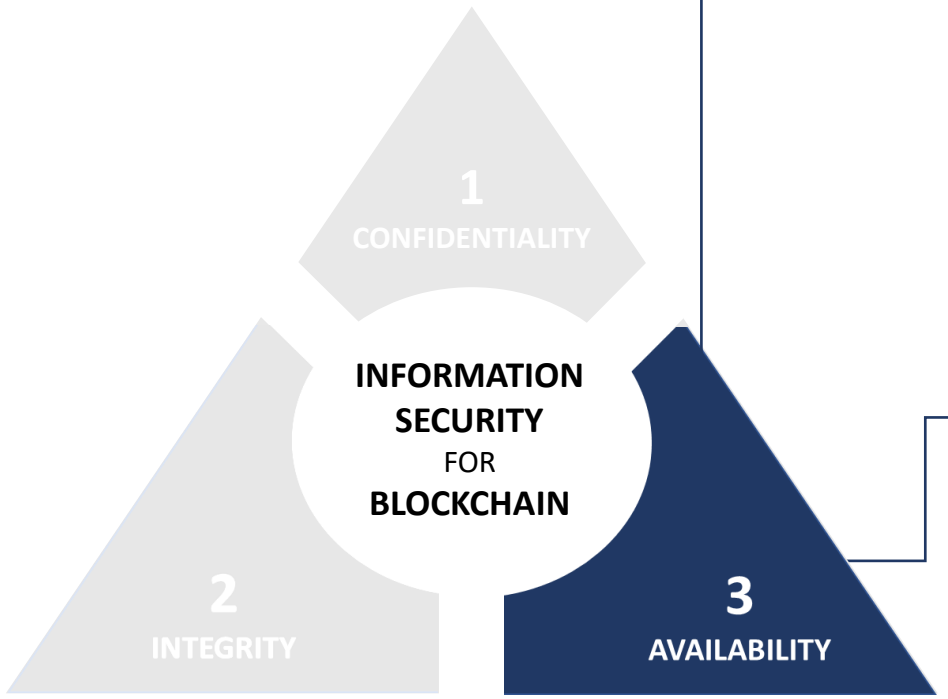
Risk: right to be forgotten

Traceability

Non repudiation - Every transaction added to a public or private blockchain is digitally signed and timestamped



```
Availability
C:\NIST\> ensuring timely and reliable access to and use of information.
```



No single point of failure

Distributed/ peer-to-peer ledger nature of the technology solves the Byzantine General's problem of false consensus.

Operational resilience

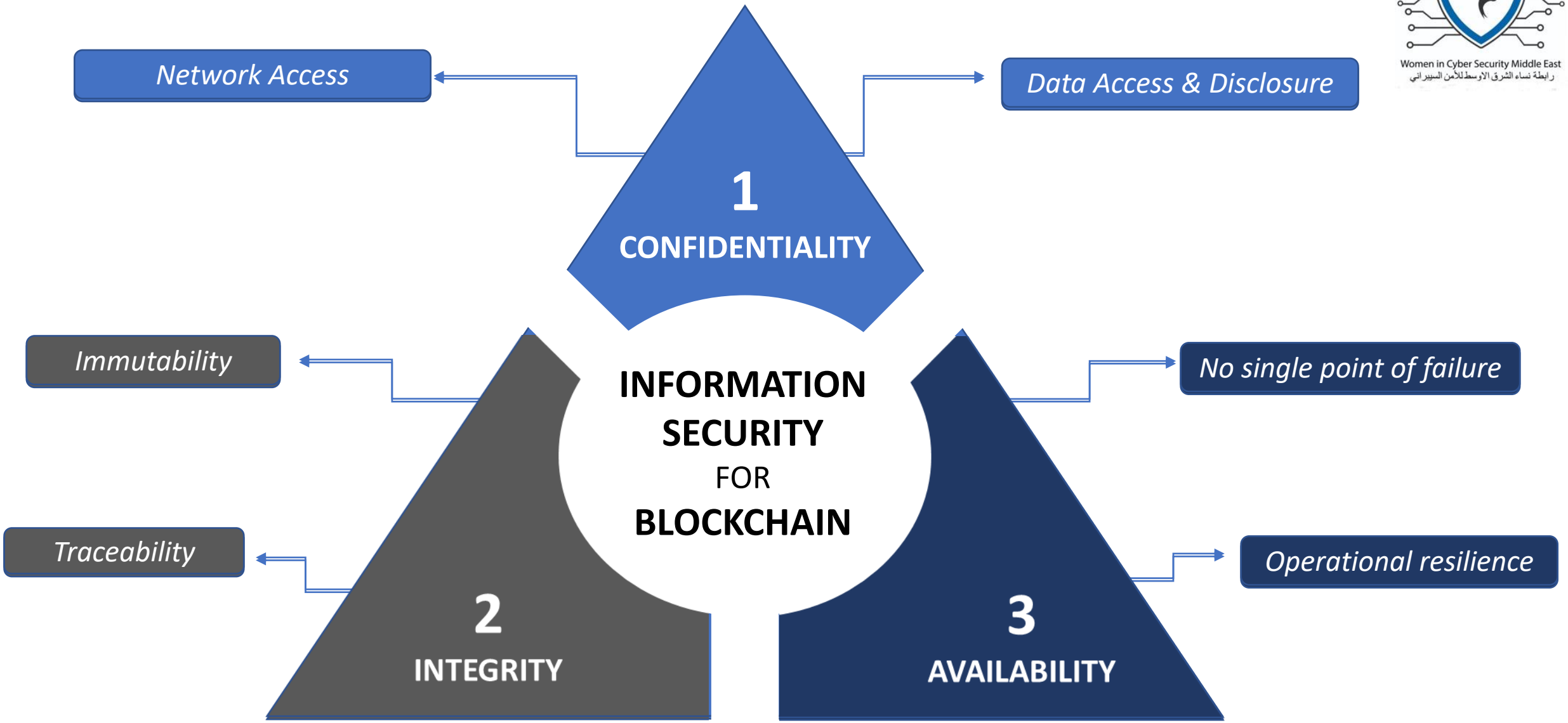
Combination of the peer-to-peer nature and sufficient nodes within the network make the platform operationally resilient

Risk: not completely "bullet-proof", several attacks in past since inception in 2008. Solved through a *hardfork*.

Risk:

#1 Public blockchain: external events outside of their control. For example, a global internet outage.

#2 Private blockchain: need for sufficient nodes.


Network Access
Data Access & Disclosure
1
CONFIDENTIALITY
Immutability
No single point of failure
INFORMATION SECURITY
FOR
BLOCKCHAIN
Traceability
Operational resilience
2
INTEGRITY
3
AVAILABILITY

DEMYSTIFYING THE BLOCKCHAIN TECHNOLOGY
تبسيط تقنية البلوكتشين

Women in Cyber Security Middle East
رابطة نساء الشرق الاوسط للأمن السيبراني

About Blockchain	Role of Blockchain Technology in the COVID-19 crisis
Blockchain and Cyber Security	Challenges of Blockchain

Women in Cyber Security Middle East
رابطة نساء الشرق الاوسط للأمن السيبراني

CHALLENGES WITH BLOCKCHAIN

```
Data Quality
Smart Contracts
Data Governance
Cyber Security
```

Data Quality: Blockchain technology **does not guarantee or improve data quality**. It can only take responsibility for the accuracy and quality of the information once added to the blockchain.

Solution: consider using multiple oracles to increase the trust in the integrity of the data entering the blockchain from the oracle.

Smart Contracts: Self-executing contracts, that may be **vulnerable to programming error or legal issues** (to account for implied expectations or unforeseen circumstances)

Solution: the adoption of smart contracts demand for legal advisors who can "code" in smart contract programming languages and ensure these computable contracts accurately reflect the underlying business deal.

CHALLENGES WITH BLOCKCHAIN

```
Data Quality
Smart Contracts
Data Governance
Cyber Security
```

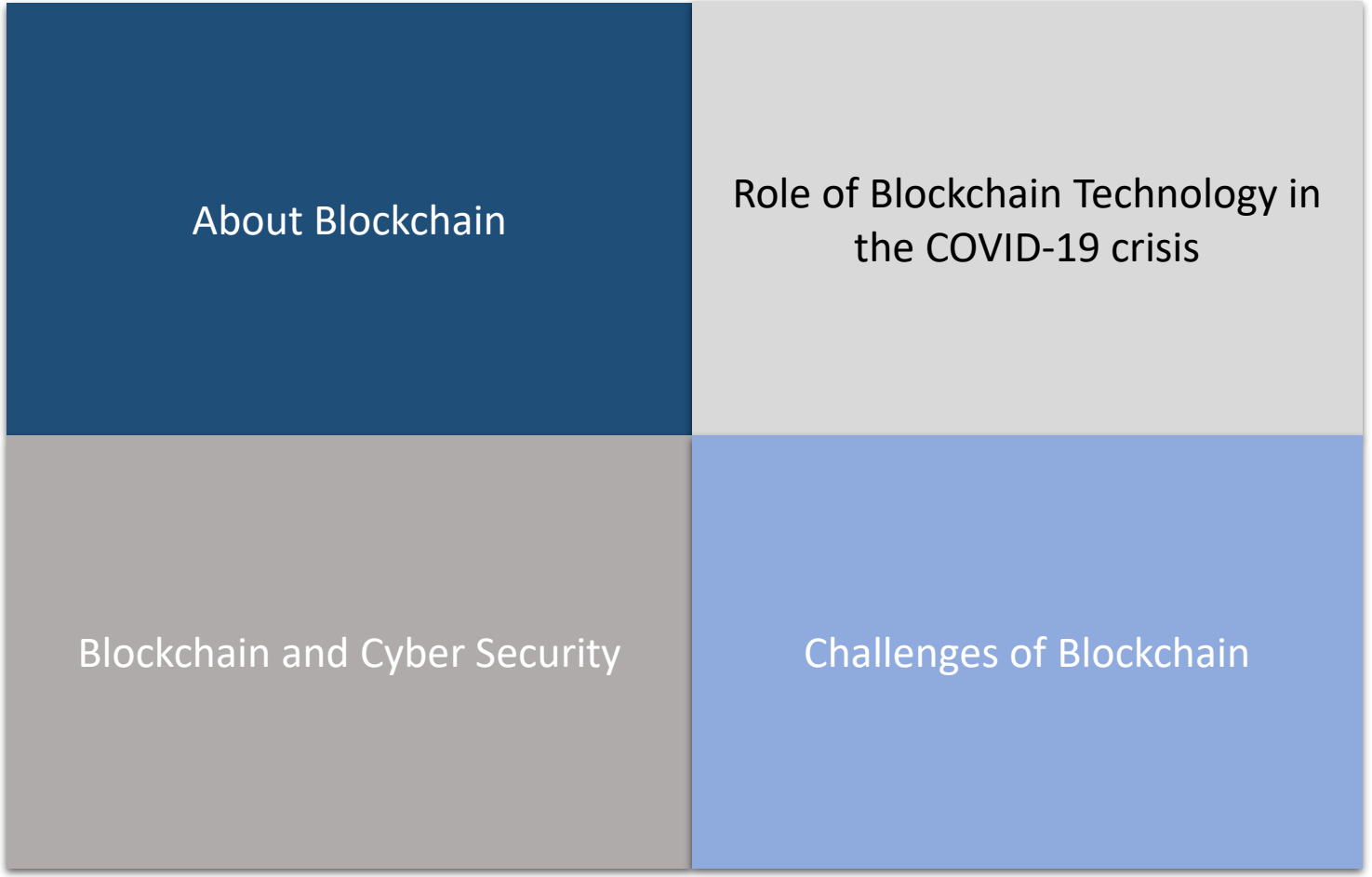
Data Governance: Laws and policies surrounding the data management – what is done with the data collected, how it is protected and so on. Eg: *GDPR – Right to be Forgotten*

Solution: A zero-knowledge protocol is a method wherein one party (the prover) can prove to another party (the verifier) that something is true, without revealing any further details with the verifier on the information proven truth.

Cyber Security: Software vulnerability, key management, integration risk (oracle authenticity management), cyber attacks like sybil attack - node that owns and runs a number of other nodes attempting to disrupt the network.

Solution: Robust White-Box Security Testing, use of secure wallets (cold or hot), a federation of off-chain external systems (oracles) from trusted sources, strict and well-regulated mechanism for accepting only trusted nodes on Blockchain

DEMYSTIFYING THE BLOCKCHAIN TECHNOLOGY
تبسيط تقنية البلوكتشين



DEMYSTIFYING THE BLOCKCHAIN TECHNOLOGY

تبسيط تقنية البلوكتشين

C:\WiCSME_Iman\>

{

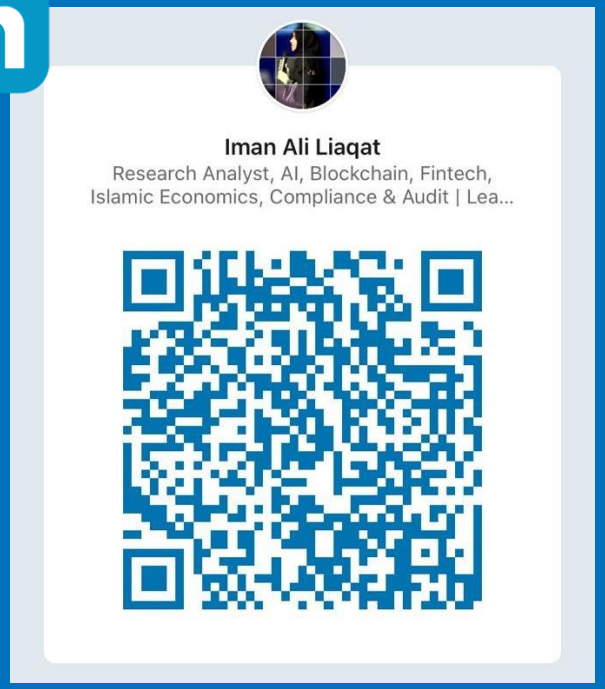
“Hope you had fun!”

“شكرا لك على المشاركة”

}

(◕‿◕)

CONTACT



@WiCSME

Women in Cyber Security Middle East
رابطة نساء الشرق الاوسط للأمن السيبراني

https://WomeninCyberSecurity.ME/

https://www.researchgate.net/profile/Iman_Ali8