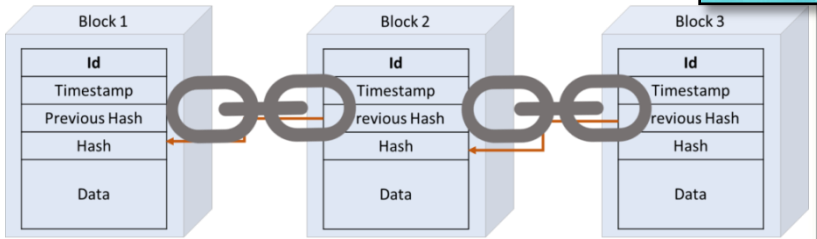
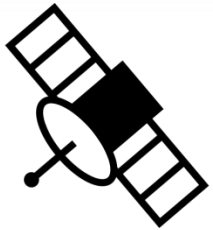
Exploring the INTERSECTION BLOCKCHAIN & SPACE THREATS





CYBER SECURITY

By: Lt Col Anupam Tiwari

NOTHING OFFICIAL

Views and opinions expressed in this talk and presentation are solely those of the presenter and do not necessarily reflect the views or opinions of the presenter's office or organization

BASED

OpenNews

Fast Paced

APPROX

Fast Paced

APPROX 15 min

About MISSING to read any slides. Just WATCH

PURPOSE OF MY SESSION

DISCUSS **SPACE THREATS** MUCH IN BRIEF

BLOCKCHAIN ASSOCIATION POSSIBLE AS SOLUTIONS TO EMERGING & EXISTING THREATS

- Current **Research works** ON & Challenges

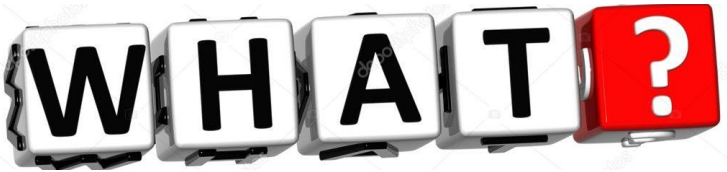
IMPORTANCE OF SATELLITE COMMUNICATION AND ITS ROLE IN OUR DAILY LIVES

IMPORTANCE OF SATELLITE COMMUNICATION AND ITS ROLE IN OUR DAILY LIVES

DO I NEED TO EVEN ASK THIS QUESTION ?

IMPORTANCE OF SATELLITE COMMUNICATION AND ITS ROLE IN OUR DAILY LIVES

DO I NEED TO EVEN ASK THIS QUESTION ?



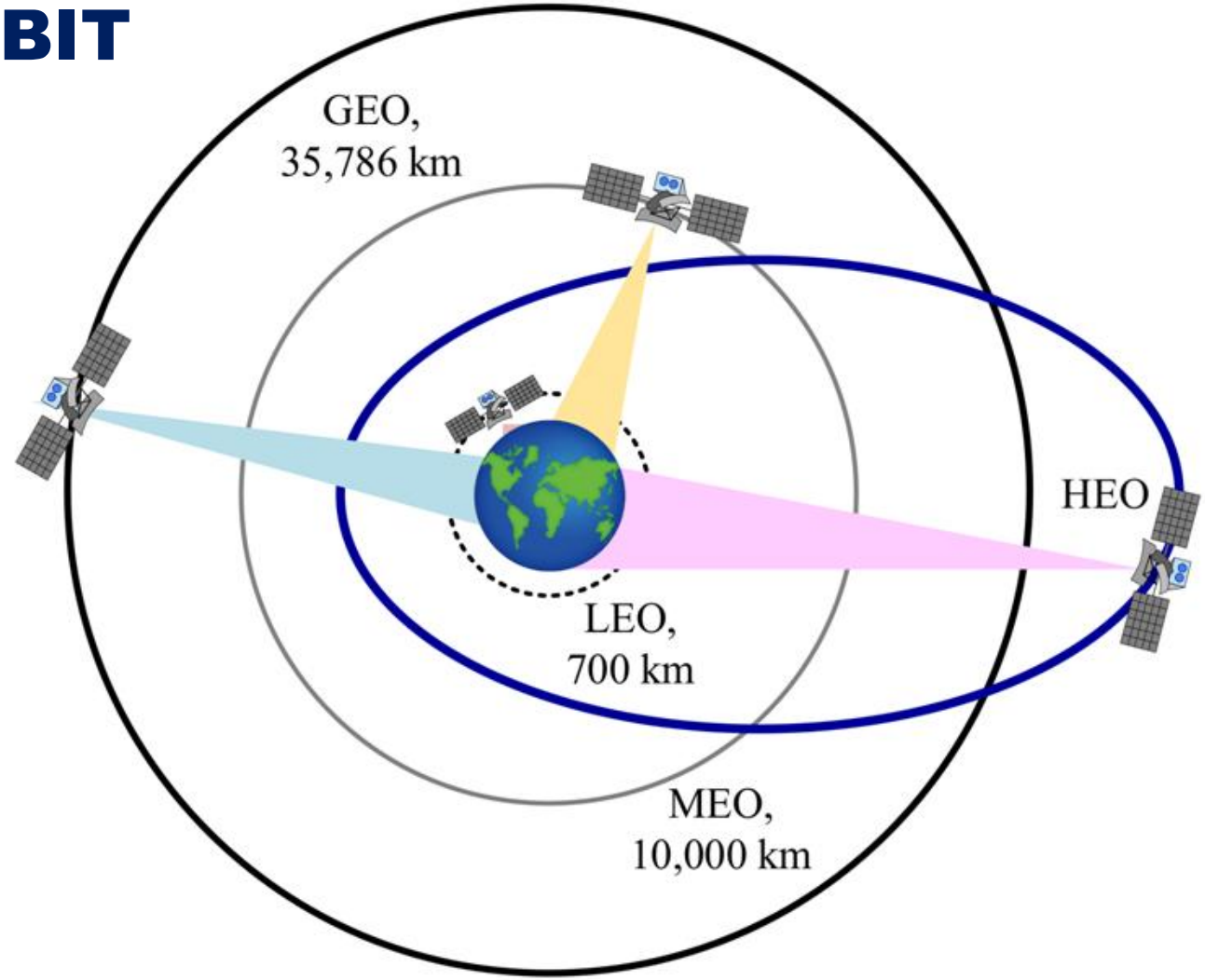
VULNERABILITY

SATELLITE COMMUNICATION WORKS?

A BIRD'S-EYE VIEW

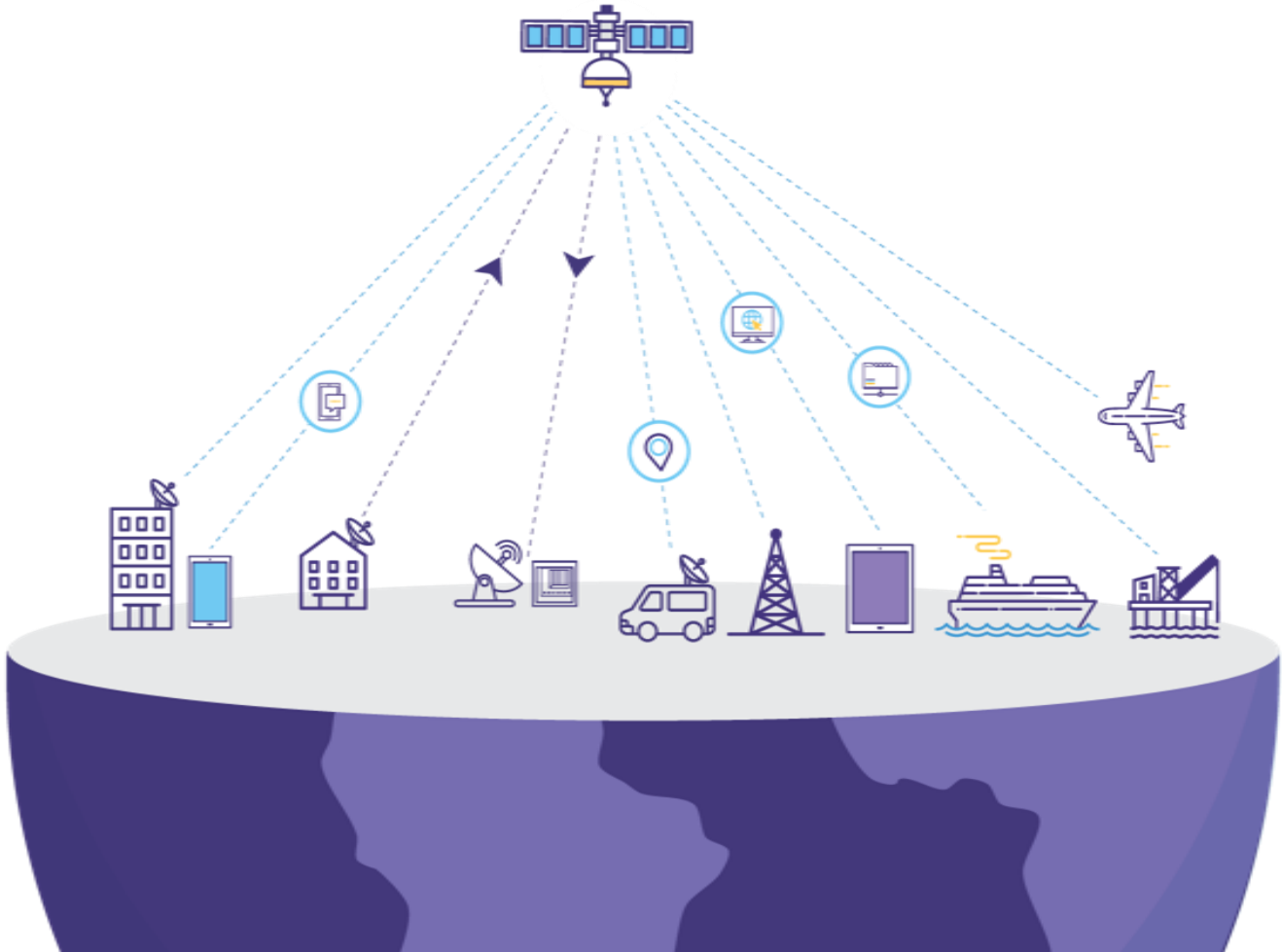
SATELLITE ORBIT

Is a **regular, repeating path** that one **object in space takes around another one** and an object in orbit is called a **SATELLITE**



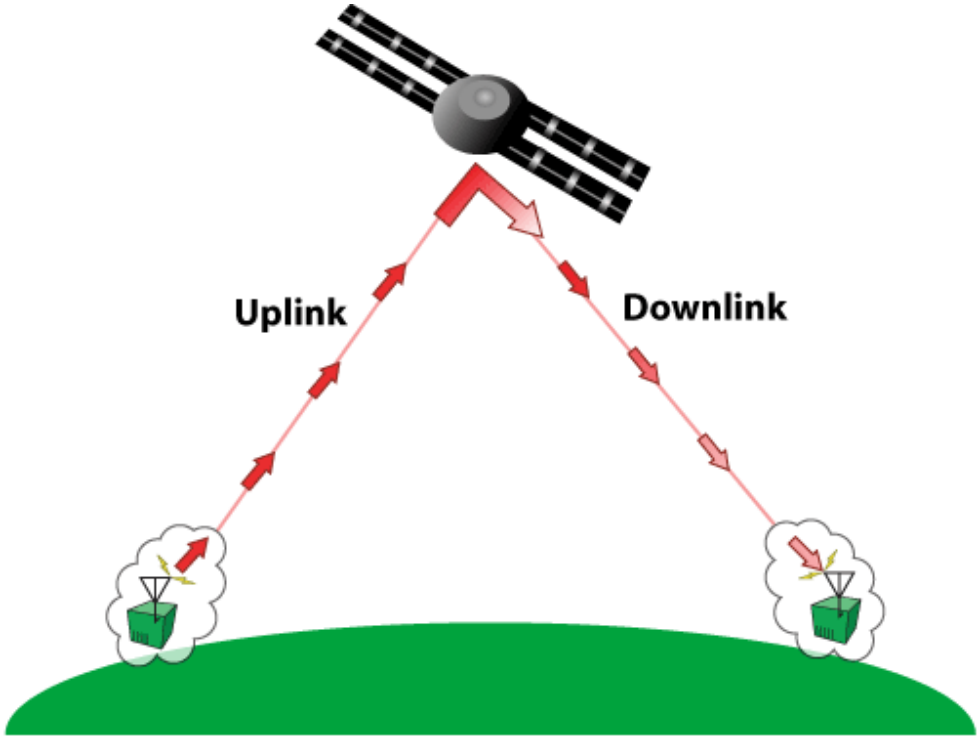
SATELLITE COMMUNICATION

Involves the **Transmission** and **Reception** of signals between **Earth-based stations** and **Satellites in orbit**



UPLINK-DOWNLINK

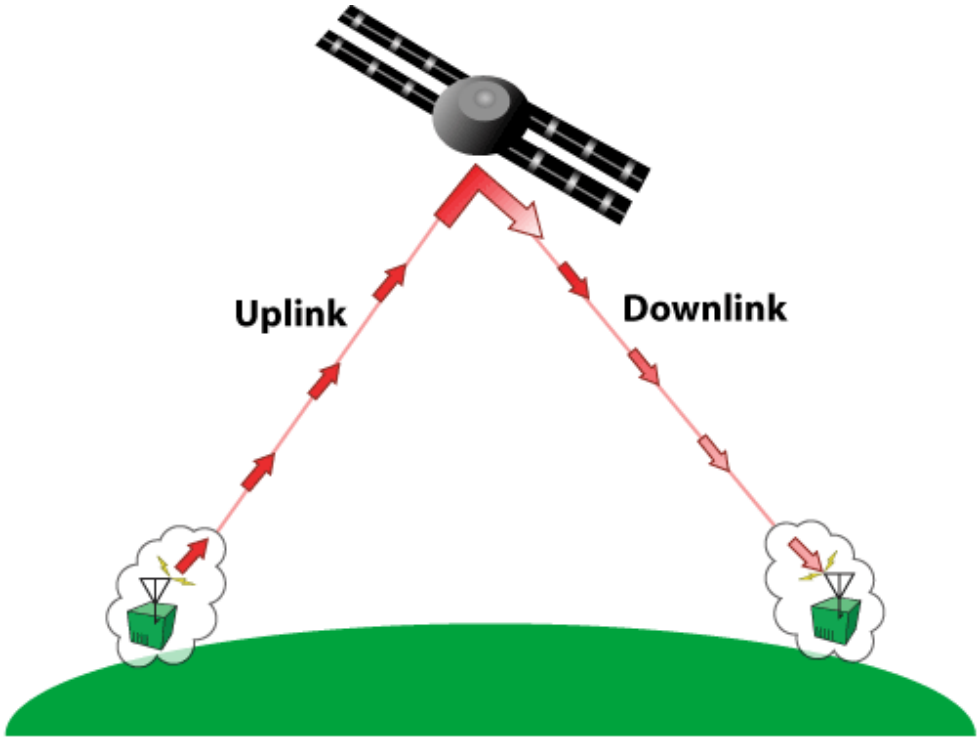
Two key components of Communication process



UPLINK-DOWNLINK

Two key components of Communication process

Uplink: Refers to the **transmission of signals from an Earth-based station** to a satellite and is responsible for **delivering information** or commands to the satellite.

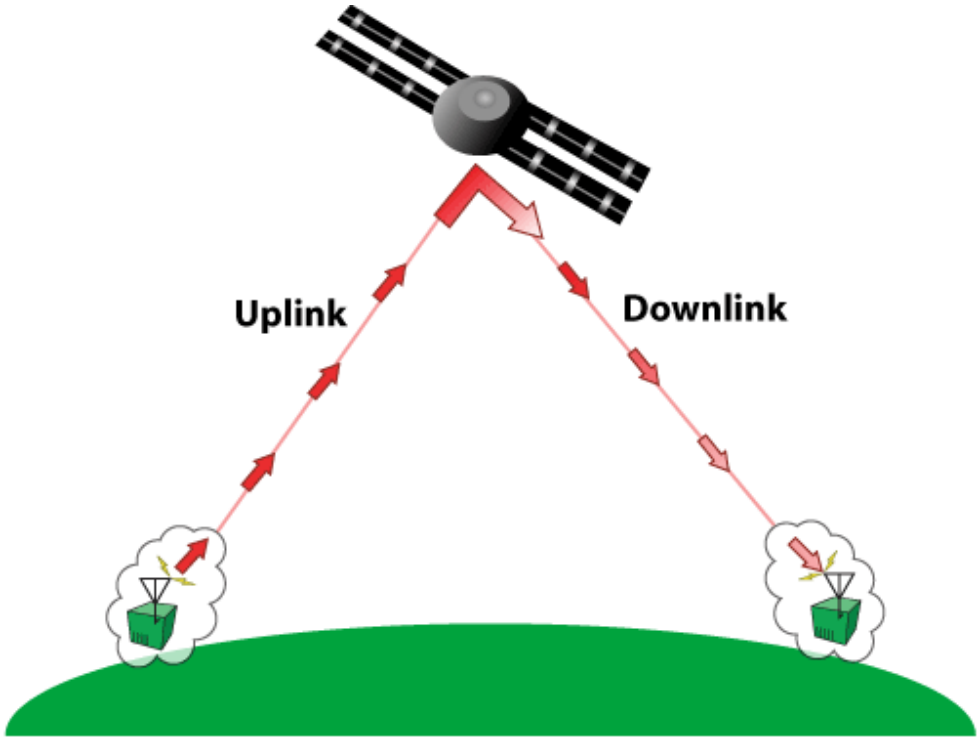


UPLINK-DOWNLINK

Two key components of Communication process

Uplink: Refers to the **transmission of signals from an Earth-based station** to a satellite and is responsible for **delivering information** or commands to the satellite.

Downlink: Refers to the **transmission of signals from a satellite back** to an Earth-based station and enables users on the ground to **receive the transmitted information from the satellite**.



GROUND SEGMENT

Consists of various Earth-based components, including Transmitting and Receiving antennas, Satellite control centers, and Communication networks

POTENTIAL VULNERABILITIES & SPACE THREATS FACED IN SPACE

JAMMING

JAMMING Types

JAMMING Types

Terrestrial' jamming : Signals can be jammed on the 'downlink' between satellites and receivers

JAMMING Types

Terrestrial' jamming : Signals can be jammed on the 'downlink' between satellites and receivers

Orbital' jamming : **on the 'uplink' between transmitting ground stations and satellites**

JAMMING Types

Terrestrial' jamming : Signals can be jammed on the 'downlink' between satellites and receivers

Orbital' jamming : on the 'uplink' between transmitting ground stations and satellites

Continuous Wave (CW) Jamming: CW jamming involves transmitting a constant, uninterrupted signal in the frequency band of the targeted satellite communication system, effectively overpowering the legitimate signals.

JAMMING Types

Terrestrial' jamming : Signals can be jammed on the 'downlink' between satellites and receivers

Orbital' jamming : on the 'uplink' between transmitting ground stations and satellites

Continuous Wave (CW) Jamming: CW jamming involves transmitting a constant, uninterrupted signal in the frequency band of the targeted satellite communication system, effectively overpowering the legitimate signals.

Partial-Band Jamming: **Partial-band jamming focuses on specific portions of the frequency band used by the satellite system. By selectively targeting certain frequencies, the jamming signal disrupts the reception of signals within that range.**

JAMMING Types

Terrestrial' jamming : Signals can be jammed on the 'downlink' between satellites and receivers

Orbital' jamming : on the 'uplink' between transmitting ground stations and satellites

Continuous Wave (CW) Jamming: CW jamming involves transmitting a constant, uninterrupted signal in the frequency band of the targeted satellite communication system, effectively overpowering the legitimate signals.

Partial-Band Jamming: Partial-band jamming focuses on specific portions of the frequency band used by the satellite system. By selectively targeting certain frequencies, the jamming signal disrupts the reception of signals within that range.

Barrage Jamming: Barrage jamming floods the entire frequency band with a wide range of random signals, making it difficult for legitimate signals to be discerned.

JAMMING Types

Terrestrial' jamming : Signals can be jammed on the 'downlink' between satellites and receivers

Orbital' jamming : on the 'uplink' between transmitting ground stations and satellites

Continuous Wave (CW) Jamming: CW jamming involves transmitting a constant, uninterrupted signal in the frequency band of the targeted satellite communication system, effectively overpowering the legitimate signals.

Partial-Band Jamming: Partial-band jamming focuses on specific portions of the frequency band used by the satellite system. By selectively targeting certain frequencies, the jamming signal disrupts the reception of signals within that range.

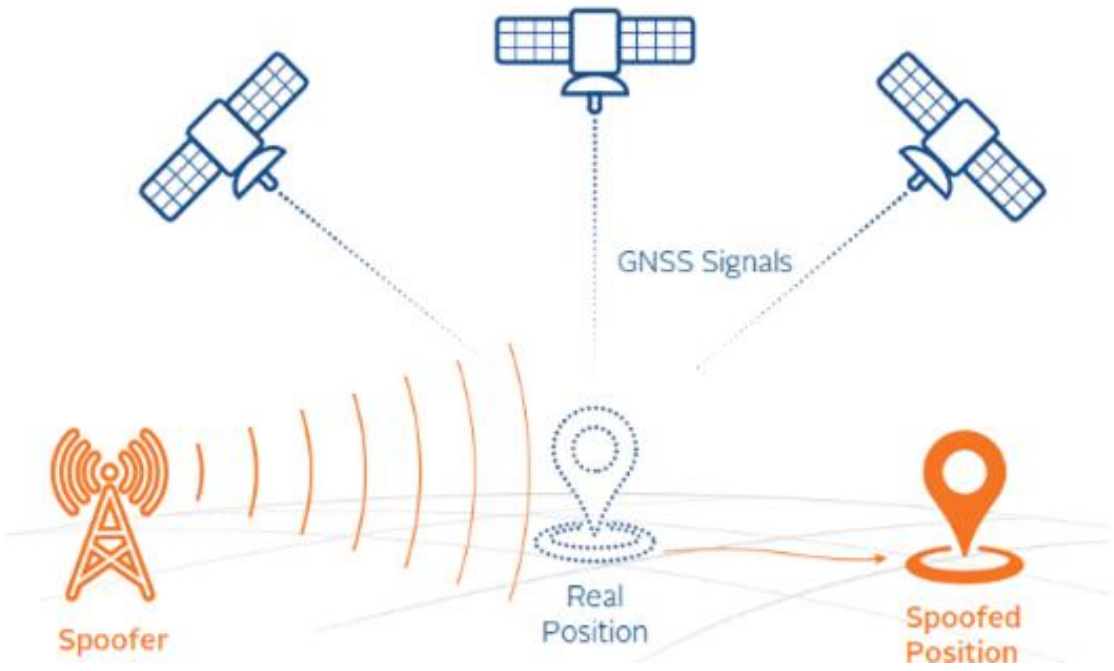
Barrage Jamming: Barrage jamming floods the entire frequency band with a wide range of random signals, making it difficult for legitimate signals to be discerned.

Spot or Narrow Beam Jamming: **Spot jamming involves focusing a high-power jamming signal on a specific spot**

JAMMING Counter MEASURE

- Frequency Hopping
- Spread Spectrum Modulation
- Adaptive Power Control
- Directional Antennas and Beamforming
- Advanced Signal Processing
- Redundancy and Diversity
- Monitoring and Detection
- International Regulations and Coordination
- Secure Satellite Communication Protocols
- Education and Awareness

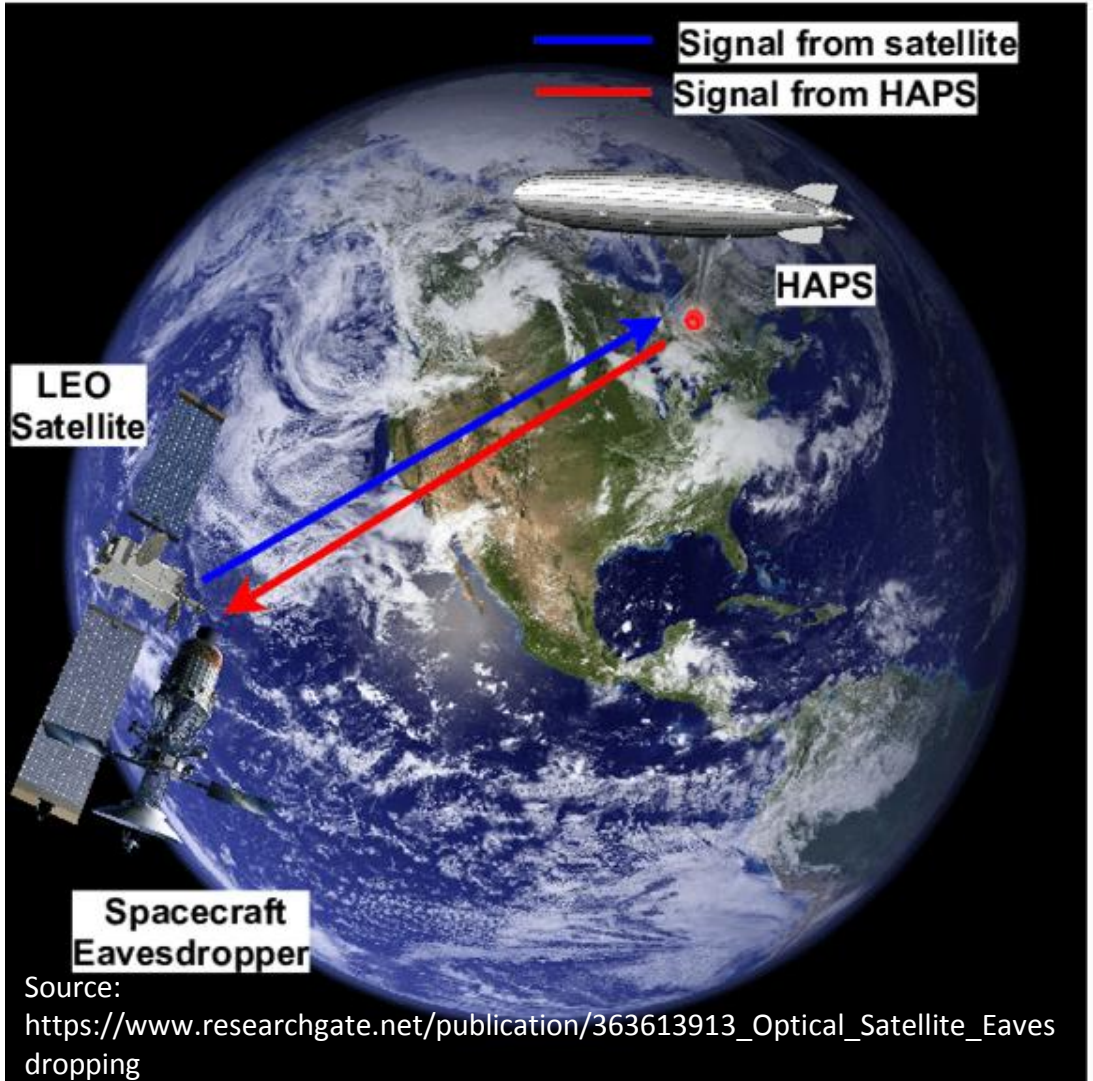
SPOOFING



When an unauthorized entity impersonates a legitimate satellite or ground station by broadcasting false signals & deceives receivers and manipulate or intercept the transmitted data.

EAVESDROPPING

Involves unauthorized parties intercepting and decoding the satellite signals which allows attackers to access sensitive information being transmitted, compromising confidentiality



Source: https://www.researchgate.net/publication/363613913_Optical_Satellite_Eavesdropping

PHYSICAL ATTACKS

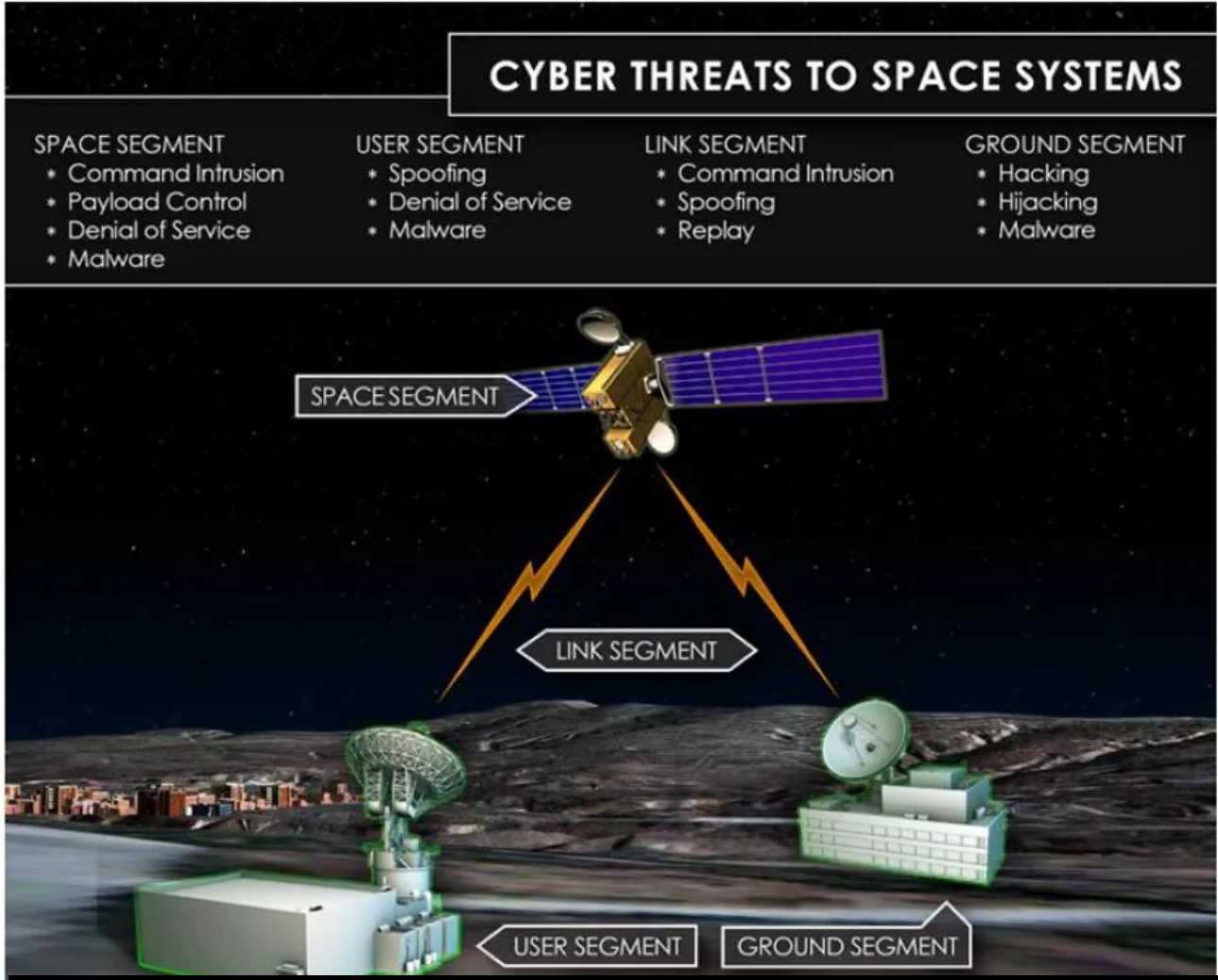
Target satellite ground stations or the satellite itself.

CYBER ATTACKS

Cyber attacks targeting ground-based systems,can compromise the security and integrity of the entire system.

MALICIOUS SOFTWARE

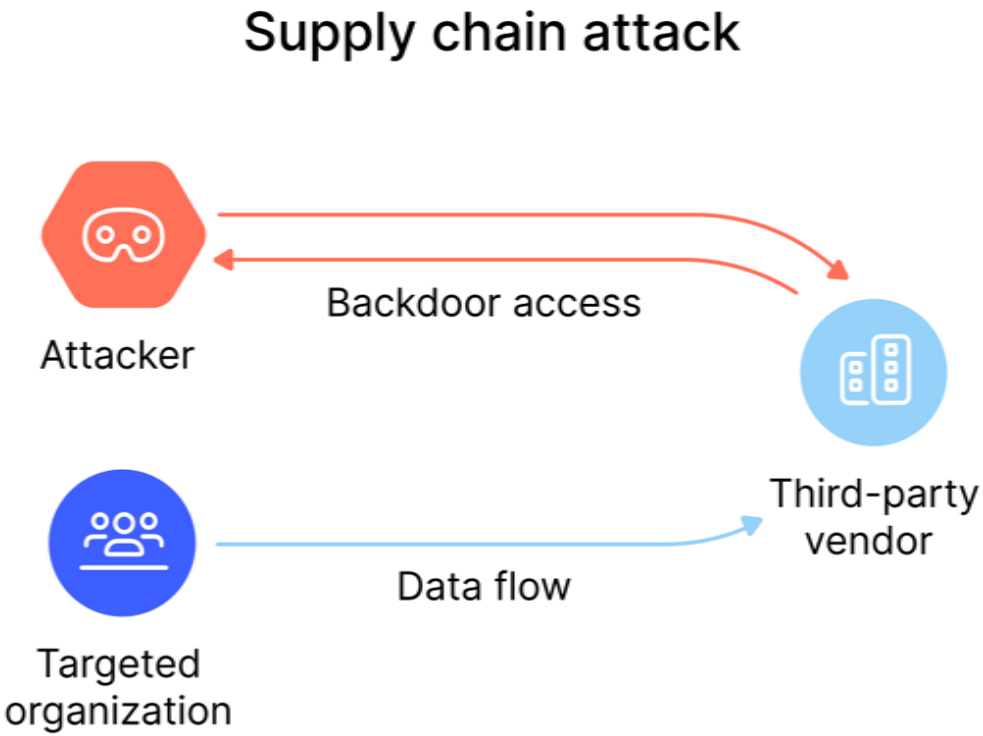
Can infect computers and networks involved in satellite communication systems.



Source: https://medium.com/the-aerospace-corporation/protecting-space-systems-from-cyber-attack-3db773aff368

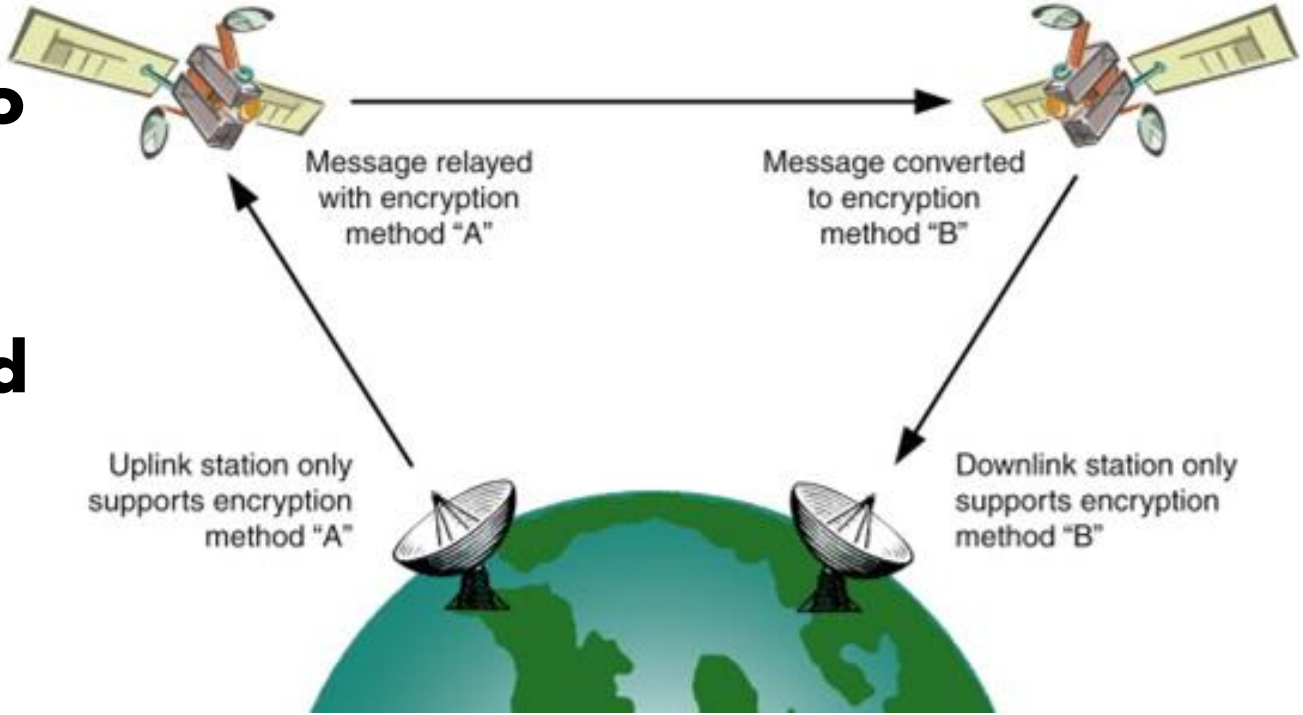
SUPPLY CHAIN ATTACKS

May introduce backdoors during the manufacturing or distribution process



LACK OF ENCRYPTION

Can leave satellite commn systems vulnerable to interception and unauthorized access



INSIDER THREATS

Refer to individuals with auth access to SATCOM systems who intentionally or unintentionally compromise system security.

Lack of Security Updates

Failure to regularly update and patch software and firmware in satellite communication systems can leave them vulnerable to known security vulnerabilities.

SOLAR RADIATION & GRILLING

- Satellites **exposed to intense solar radiation**.
- Can cause a phenomenon known as **"GRILLING"**
- When a satellite is positioned in a way that all its solar panels are simultaneously exposed to direct sunlight, **the sudden surge in power generation can lead to overloading** of the energy system.
- Can **potentially damage or disable the satellite's power supply** or other critical components.

SPACE DEBRIS & COLLISIONS

- **Increasing amount of space debris poses a significant threat to satellites.**

- **Space debris includes defunct satellites, spent rocket stages, and fragments from previous space missions.**

- **Collisions with space debris can cause catastrophic damage to satellites, leading to the loss of functionality or complete mission failure.**

SPACE WEATHER

- Refers to the conditions and disturbances in the space environment caused by solar activity
- Can disrupt satellite communication, interfere with signal transmission, and even damage onboard electronics
- Ground operators would not even know the attributable reason to blame it on for space weather or otherwise

SINGLE POINT FAILURES

- Satellites are complex systems with numerous components and subsystems

- Single point failures occur when a critical component or subsystem malfunctions or fails, leading to the satellite's complete or partial loss of functionality

- Caused by manufacturing defects, design flaws, or even natural degradation over time

DEEPFAKE GEOGRAPHY

A growing problem of 'deepfake geography': How AI falsifies satellite images

Deepfake Satellite Images Pose Risk to Global Politics and Military: Report

Deepfake tech takes on satellite maps

Devin Coldewey @techcrunch / 2:16 AM GMT+5:30 • April 23, 2021

INTELLIGENCE, NETWORKS / CYBER

NGA working with NRO to target satellite imagery 'deep fakes'

NGA's Chief Information Office Mark Andress said he has an entire engineering team dedicated to certifying the accuracy and validity of imagery products and the metadata around them.

Cyber Attack | Cyber Security | Cyber Security News | Malware | Ransomware

Ransomware Groups Attacking Satellite and Space Industry

By **Balaji N** - April 3, 2023 0

Dish confirms ransomware attack allowed hackers to steal personal data

Carly Page @carlypage_ / 12:36 AM GMT+5:30 • March 1, 2023 Comment

Satellite TV company Dish confirms ransomware attack

By VARINDIA - 2023-05-24

Satellite television giant Dish has confirmed that personal information of 3,00,000 employees has been stolen in a **ransomware attack** in February.

AND

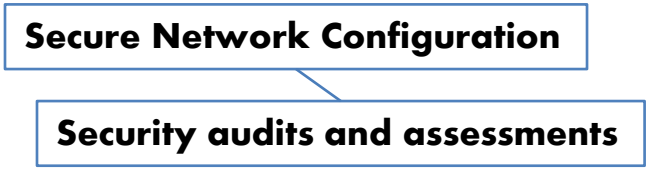
each

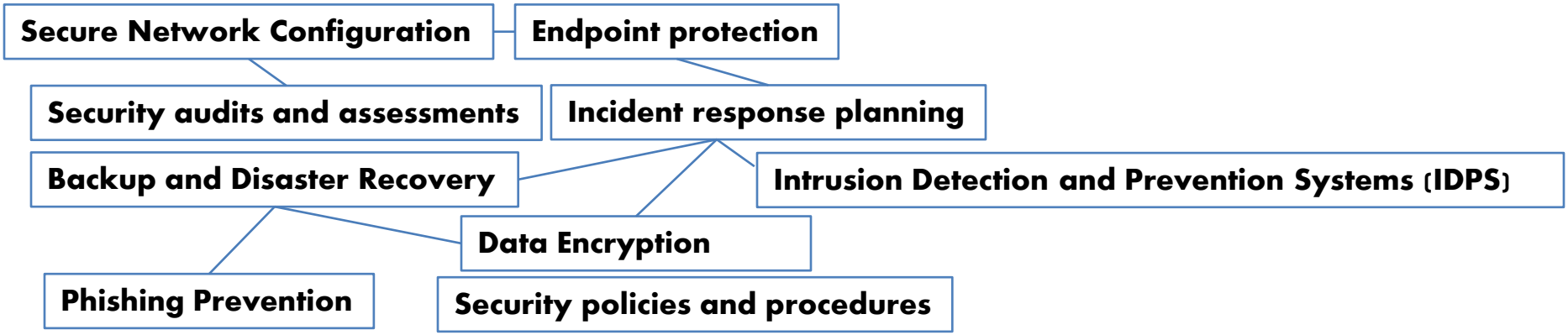
HAS

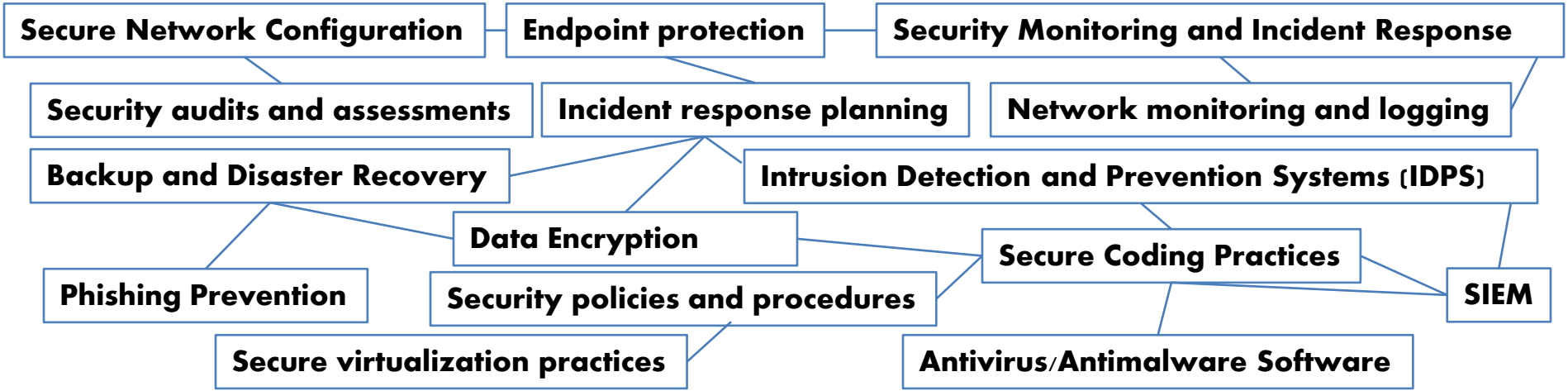
CyberWay

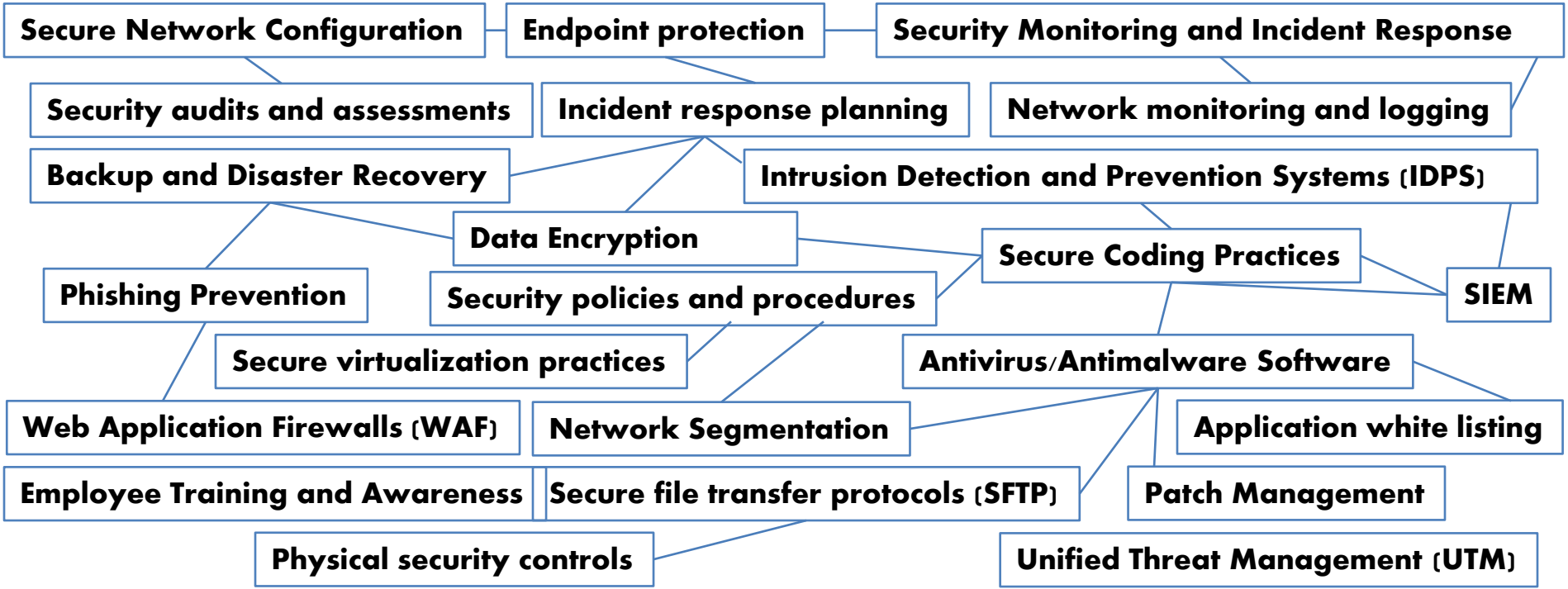

COMPLEX

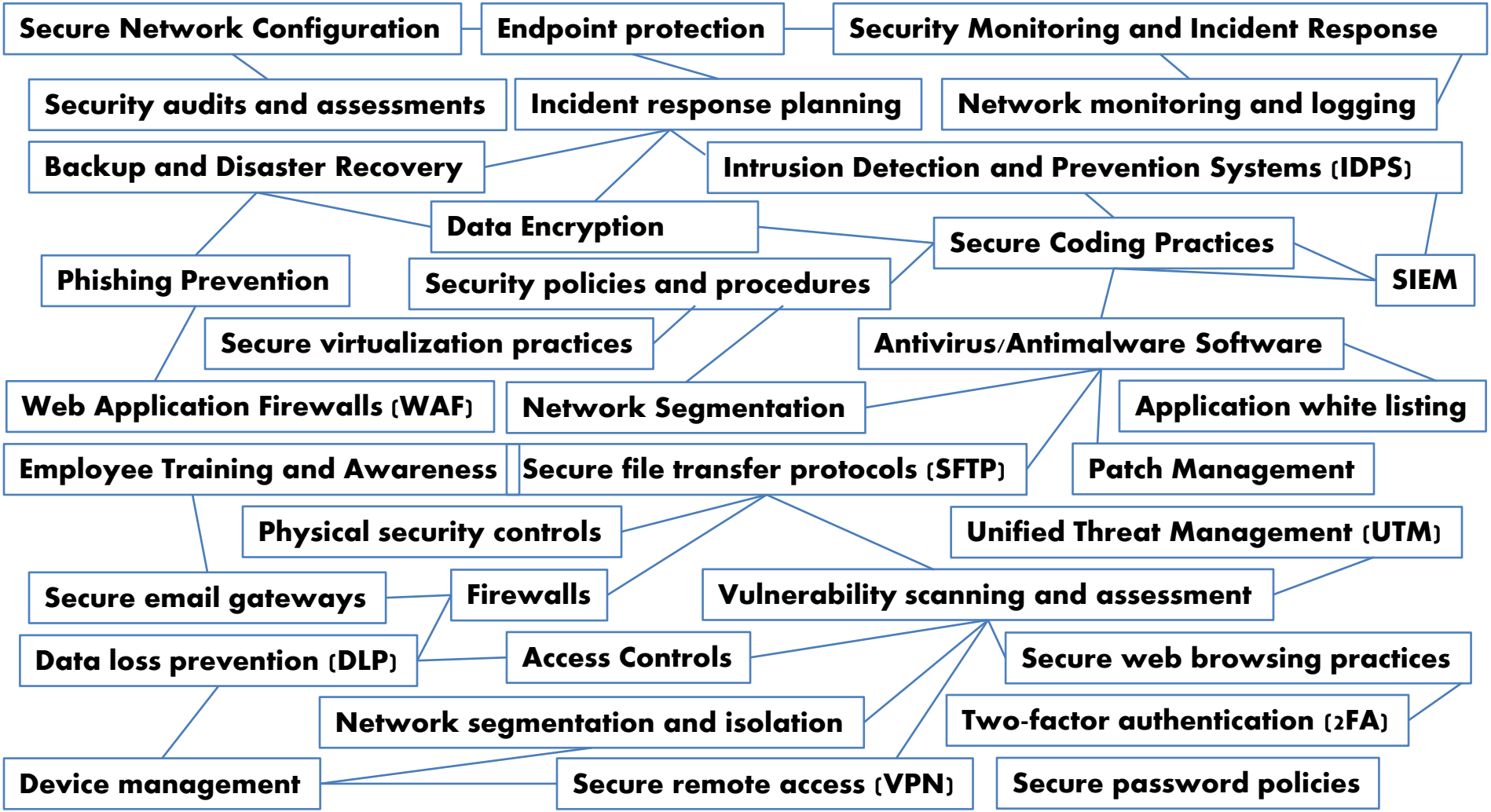

Solution


Secure Network Configuration
Security audits and assessments


Secure Network Configuration
Endpoint protection
Security audits and assessments
Incident response planning
Backup and Disaster Recovery
Intrusion Detection and Prevention Systems (IDPS)
Data Encryption
Phishing Prevention
Security policies and procedures


Secure Network Configuration
Endpoint protection
Security Monitoring and Incident Response
Security audits and assessments
Incident response planning
Network monitoring and logging
Backup and Disaster Recovery
Intrusion Detection and Prevention Systems (IDPS)
Data Encryption
Secure Coding Practices
Phishing Prevention
Security policies and procedures
SIEM
Secure virtualization practices
Antivirus/Antimalware Software


Secure Network Configuration
Endpoint protection
Security Monitoring and Incident Response
Security audits and assessments
Incident response planning
Network monitoring and logging
Backup and Disaster Recovery
Intrusion Detection and Prevention Systems (IDPS)
Data Encryption
Secure Coding Practices
Phishing Prevention
Security policies and procedures
SIEM
Secure virtualization practices
Antivirus/Antimalware Software
Web Application Firewalls (WAF)
Network Segmentation
Application white listing
Employee Training and Awareness
Secure file transfer protocols (SFTP)
Patch Management
Physical security controls
Unified Threat Management (UTM)


Secure Network Configuration
Endpoint protection
Security Monitoring and Incident Response
Security audits and assessments
Incident response planning
Network monitoring and logging
Backup and Disaster Recovery
Intrusion Detection and Prevention Systems (IDPS)
Data Encryption
Secure Coding Practices
Phishing Prevention
Security policies and procedures
SIEM
Secure virtualization practices
Antivirus/Antimalware Software
Web Application Firewalls (WAF)
Network Segmentation
Application white listing
Employee Training and Awareness
Secure file transfer protocols (SFTP)
Patch Management
Physical security controls
Unified Threat Management (UTM)
Secure email gateways
Firewalls
Vulnerability scanning and assessment
Data loss prevention (DLP)
Access Controls
Secure web browsing practices
Network segmentation and isolation
Two-factor authentication (2FA)
Device management
Secure remote access (VPN)
Secure password policies


Secure Network Configuration
Endpoint protection
Security Monitoring and Incident Response
Security audits and assessments
Incident response planning
Network monitoring and logging
Backup and Disaster Recovery
Intrusion Detection and Prevention Systems (IDPS)
Phishing Prevention
SIEM
Secure virtualization practices
Antivirus/Antimalware Software
Web Application Firewalls (WAF)
Application white listing
Employee Training and Awareness
Patch Management
Physical security
Unified Threat Management (UTM)
Secure email gateways
Firewalls
Vulnerability scanning and assessment
Data loss prevention (DLP)
Access Controls
Secure web browsing practices
Network segmentation and isolation
Two-factor authentication (2FA)
Device management
Secure remote access (VPN)
Secure password policies
no end

MULTIPLE Options

CYBER SECURITY

BUSINESS MODELSINC

After DOING All this

WE ARE

After DOING All this

WE ARE Only

RELATIVELY

SeCURE

be.cause We Know

ONE HUNDRED PERCENT PROTECTION DOES NOT EXIST

SeCURE

So what else ?


I WILL
DISCUSS
Solutions
UNDER
CONSTRUCTION
RESEARCH
WORKS
around
BLOCKCHAIN
TECHNOLOGY

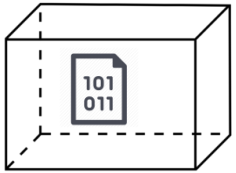
FOR THE

UNversed

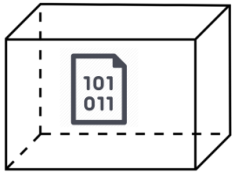
WHAT

Exactly. IS BLOCKCHAIN

An Overall View.....



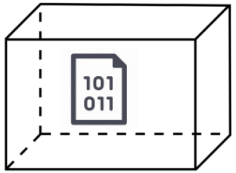
BLOCK with some DATA



BLOCK with some DATA

HASH

Cryptographic function, a mathematical algorithm that maps data of arbitrary size to a bit array of a fixed size



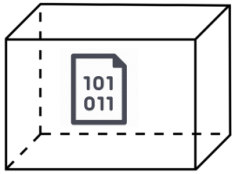
BLOCK with some DATA

HASH

Cryptographic function, a mathematical algorithm that maps data of arbitrary size to a bit array of a fixed size

INPUT

ANYTHING



BLOCK with some DATA

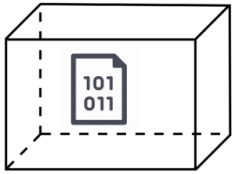
HASH

Cryptographic function, a mathematical algorithm that maps data of arbitrary size to a bit array of a fixed size

INPUT

ANYTHING

ANY Format



BLOCK with some DATA

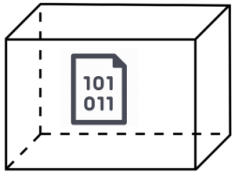
HASH

Cryptographic function, a mathematical algorithm that maps data of arbitrary size to a bit array of a fixed size

INPUT

ANYTHING

ANY Format



BLOCK with some DATA

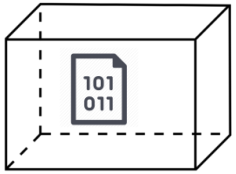
HASH

Cryptographic function, a mathematical algorithm that maps data of arbitrary size to a bit array of a fixed size

INPUT

ANYTHING

ANY Format



BLOCK with some DATA

HASH

Cryptographic function, a mathematical algorithm that maps data of arbitrary size to a bit array of a fixed size

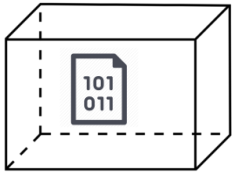
INPUT

ANYTHING

ANY Format

There are 100's of algorithms & this is one TYPE

SHA-256 (Hash algorithm)



BLOCK with some DATA

HASH

Cryptographic function, a **mathematical algorithm** that **maps data** of **arbitrary size** to a bit array of a fixed size

INPUT

ANYTHING

ANY Format

SHA-256 (Hash algorithm)

6bcec30f359e597986bcdc075eed3e339a3a1
8673ec4624425d75247eacce9f5

HASH

Text input : TALK ON 07 JUN 2023

HASH

Text input : TALK ON 07 JUN 2023

Let this be a sample **TEXT data** and be applied **HASH upon**

HASH

Text input : TALK ON 07 JUN 2023

58b162269025ef5388e111768847ef995e8831f
5d82a5d22076833ed25b29b95

HASH

Text input : TALK ON 07 JUN 2023

58b162269025ef5388e111768847ef995e8831f
5d82a5d22076833ed25b29b95

UNIQUE

HASH

WATCH HERE

Text input : TALK ON 07 JUN 2023

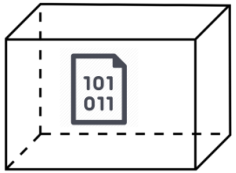
58b162269025ef5388e111768847ef995e8831f5d82a5d22076833ed25b29b95

HASH

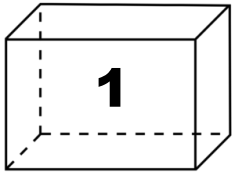
WATCH HERE

Text input : TALK ON 07 JUn 2023

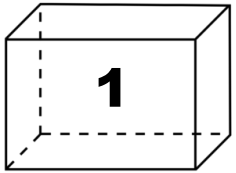
eb23df9940ebe8ad1ad9ef271e7de5923e7b45
93199ce699f82c9e4986df737b

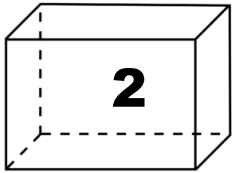


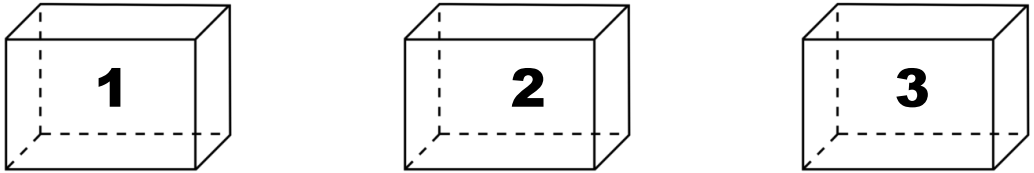
BLOCK with some DATA

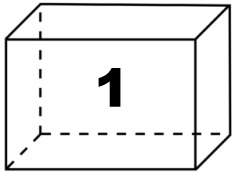


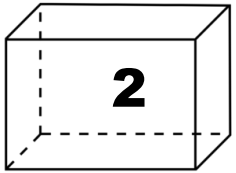
BLOCK with some DATA

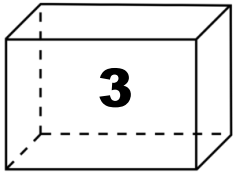

1

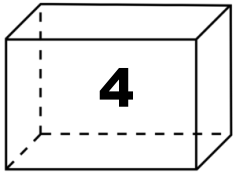

2

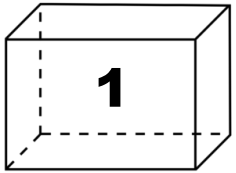

1
2
3

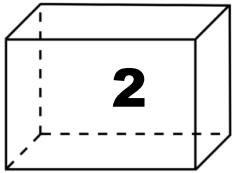

1

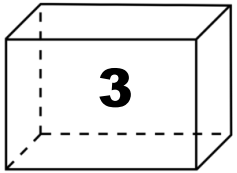

2

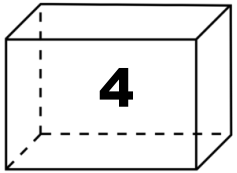

3

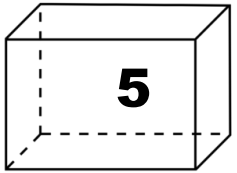

4

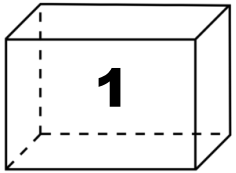

1

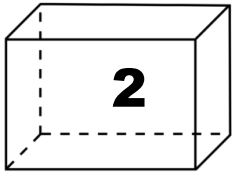

2

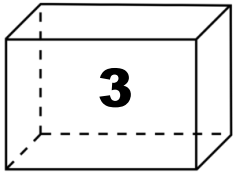

3

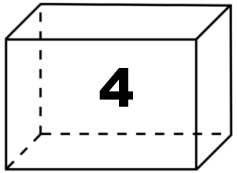

4

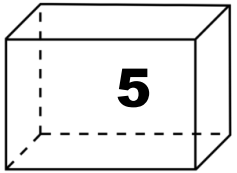

5

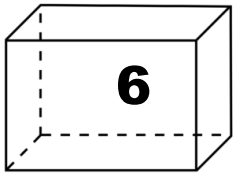

1

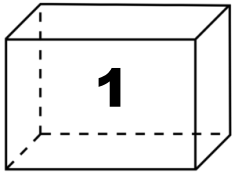

2

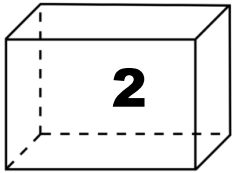

3

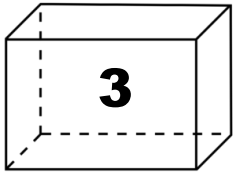

4

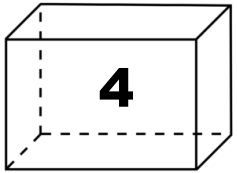

5

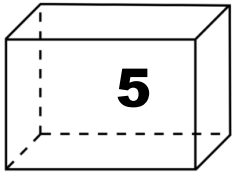

6

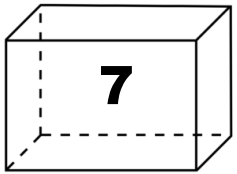

1

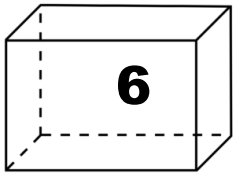

2

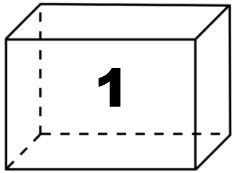

3

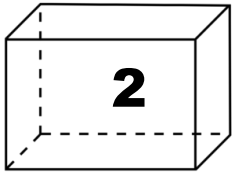

4

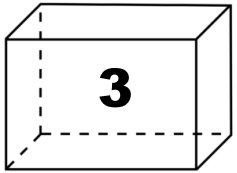

5

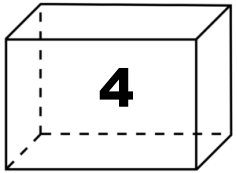

7

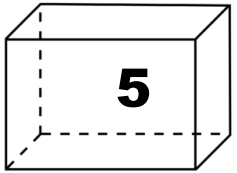

6

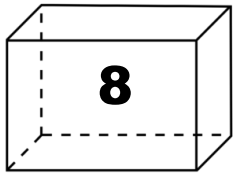

1

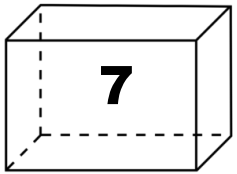

2

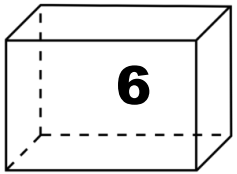

3

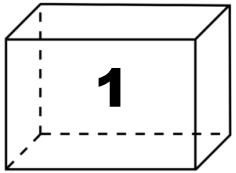

4

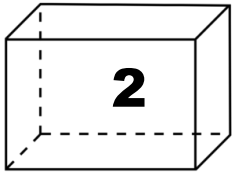

5

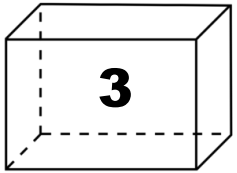

8

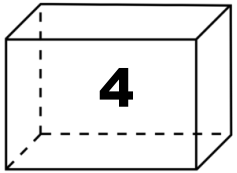

7

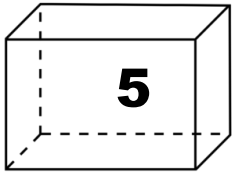

6

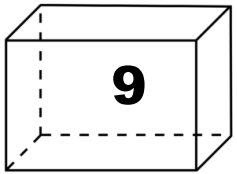

1

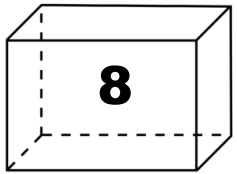

2

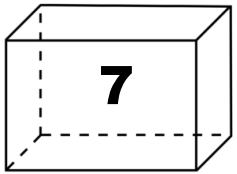

3

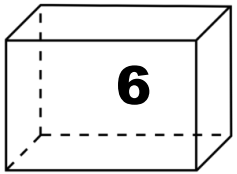

4

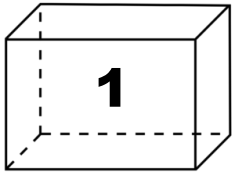

5

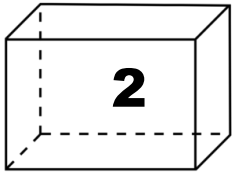

9

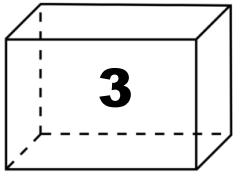

8

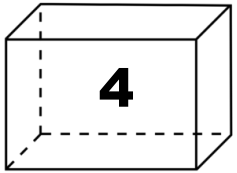

7

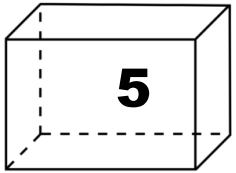

6

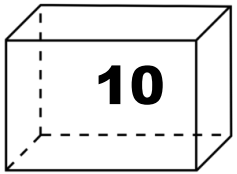

1

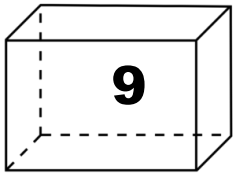

2

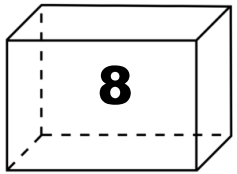

3

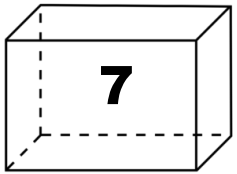

4

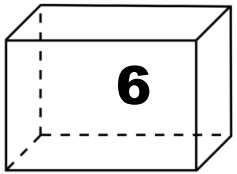

5

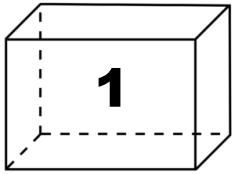

10

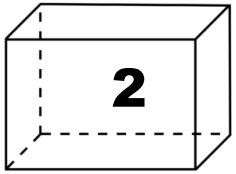

9

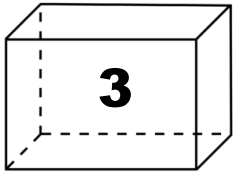

8

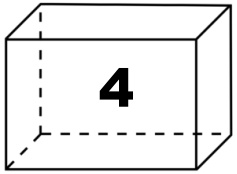

7

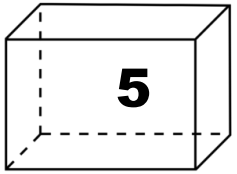

6

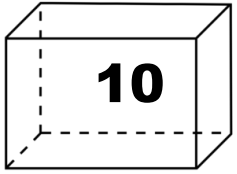

1

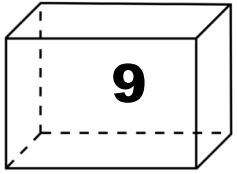

2

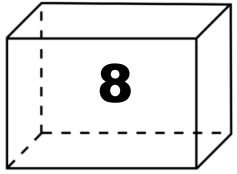

3

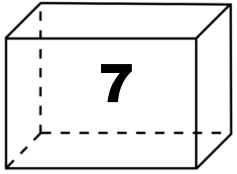

4

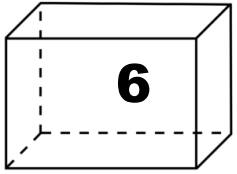

5

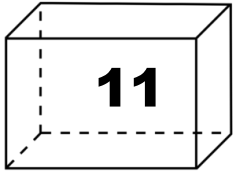

10

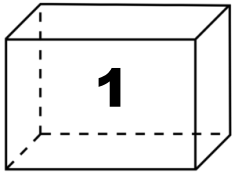

9

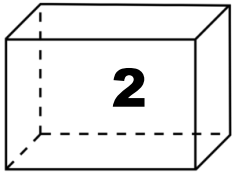

8

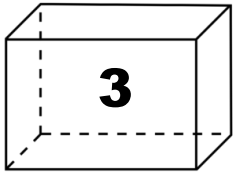

7

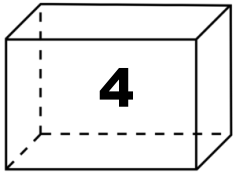

6

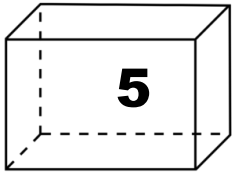

11

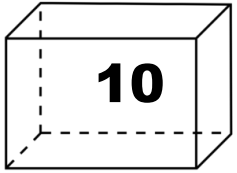

1

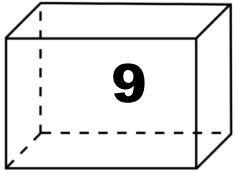

2

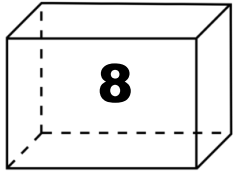

3

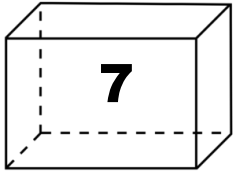

4

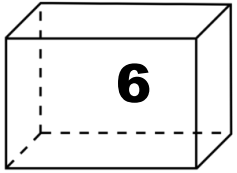

5

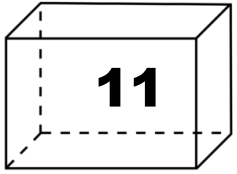

10

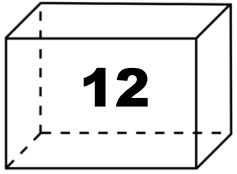

9

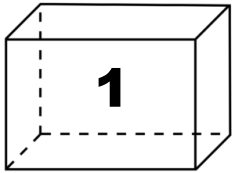

8

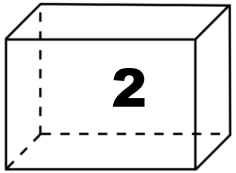

7

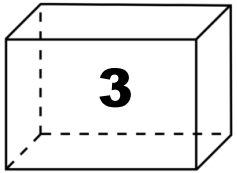

6

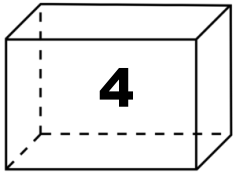

11

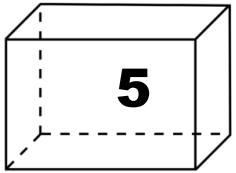

12

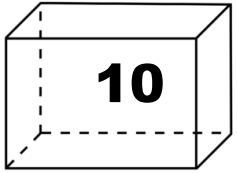

1

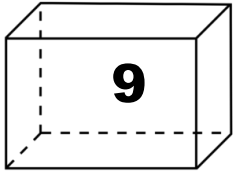

2

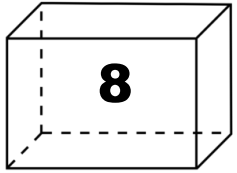

3

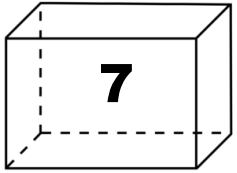

4

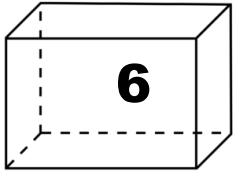

5

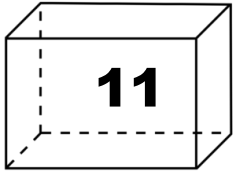

10

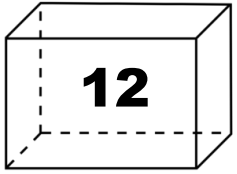

9

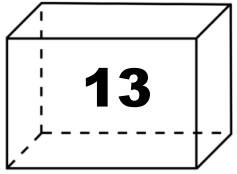

8

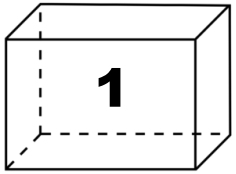

7

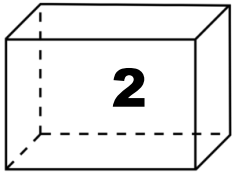

6

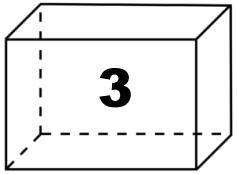

11

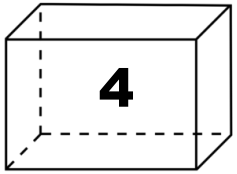

12

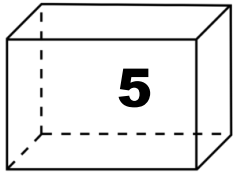

13

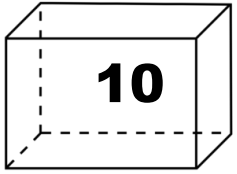

1

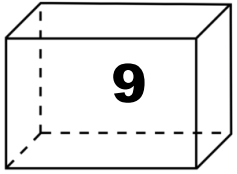

2

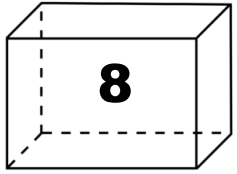

3

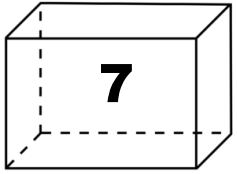

4

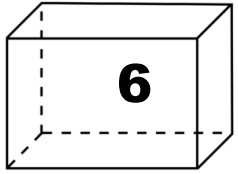

5

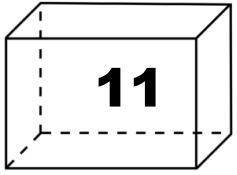

10

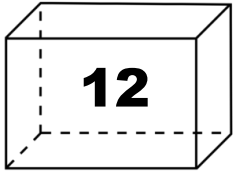

9

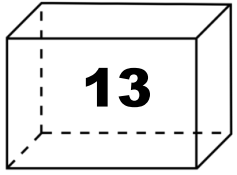

8

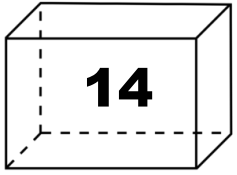

7

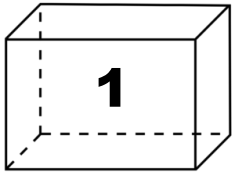

6

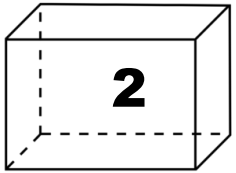

11

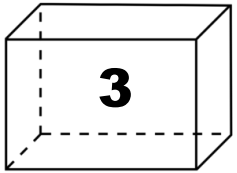

12

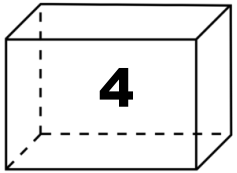

13

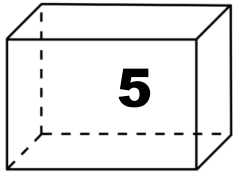

14

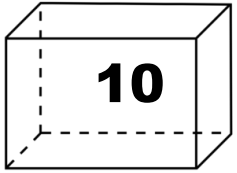

1

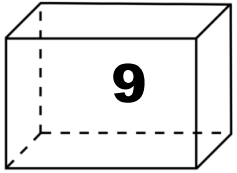

2

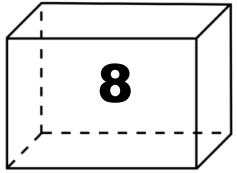

3

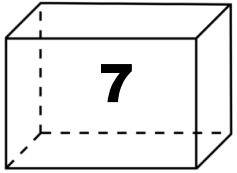

4

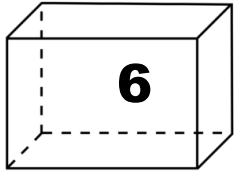

5

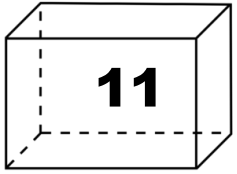

10

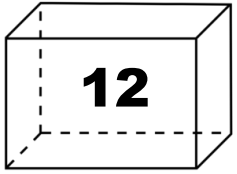

9

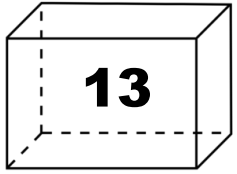

8

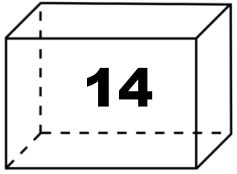

7

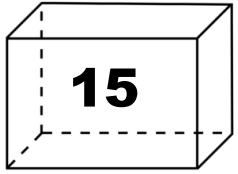

6

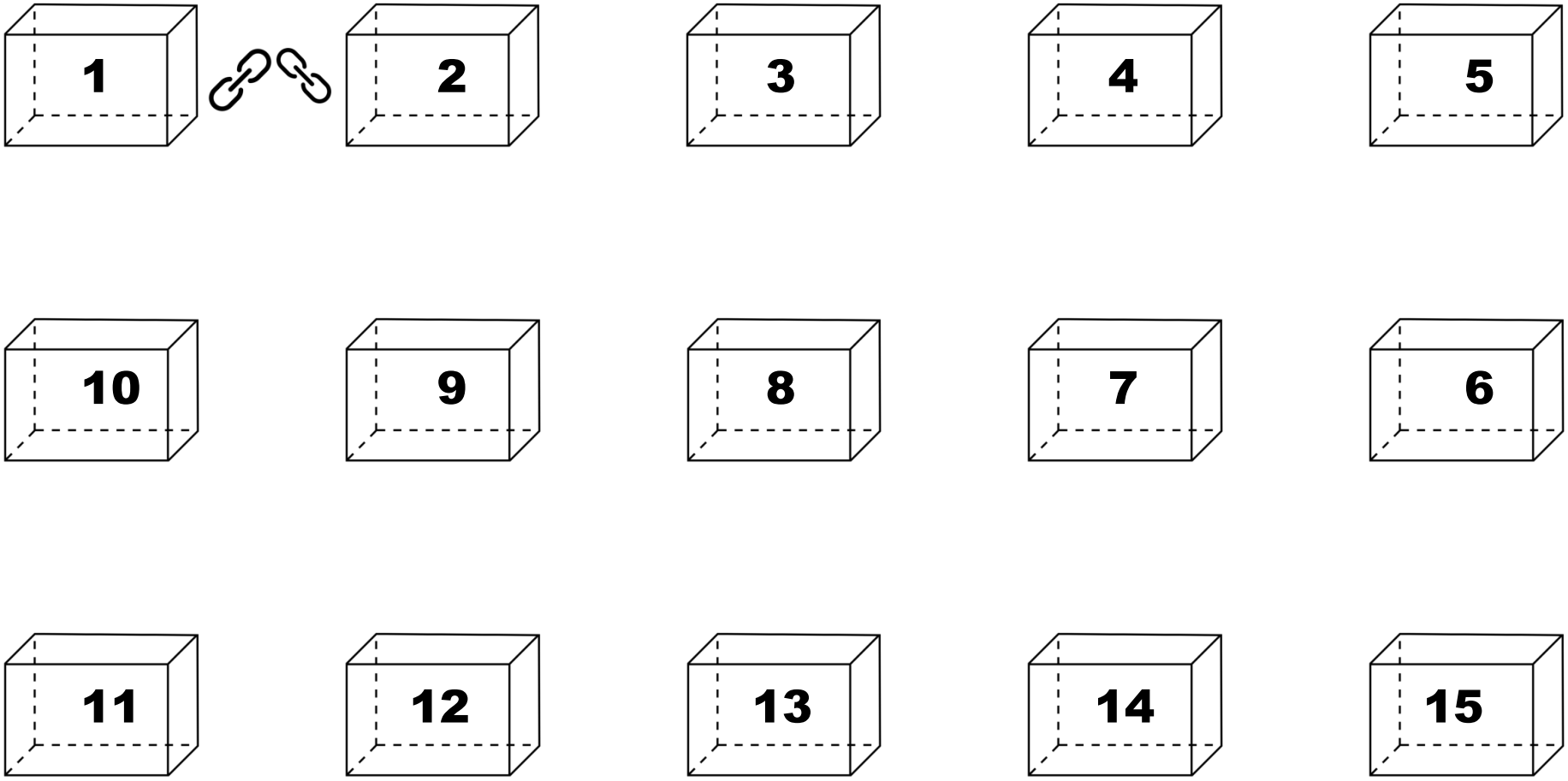

11

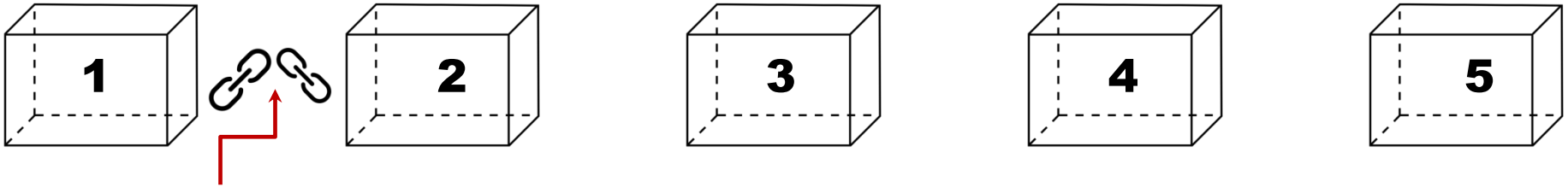

12


13

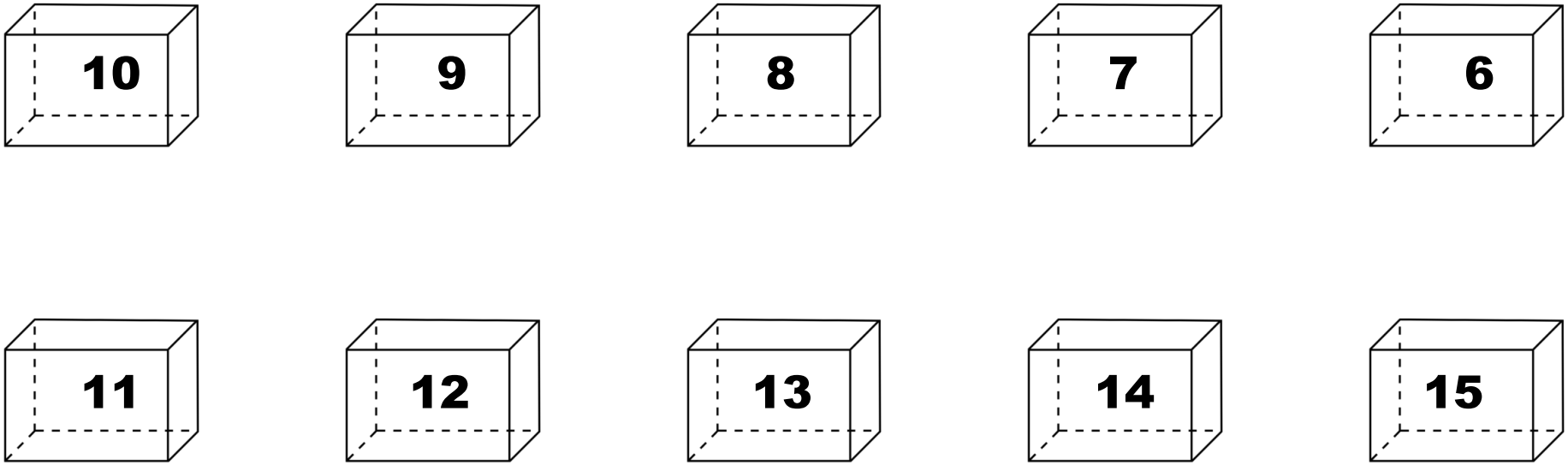

14

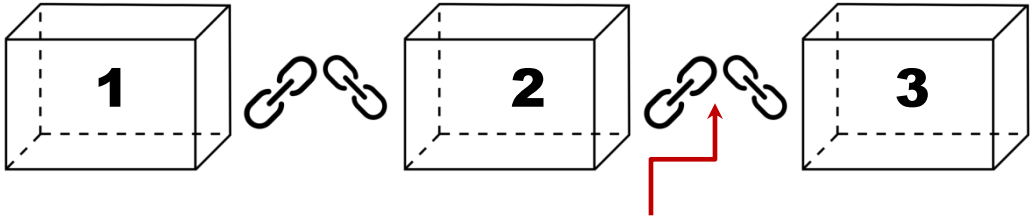

15


1
2
3
4
5
10
9
8
7
6
11
12
13
14
15

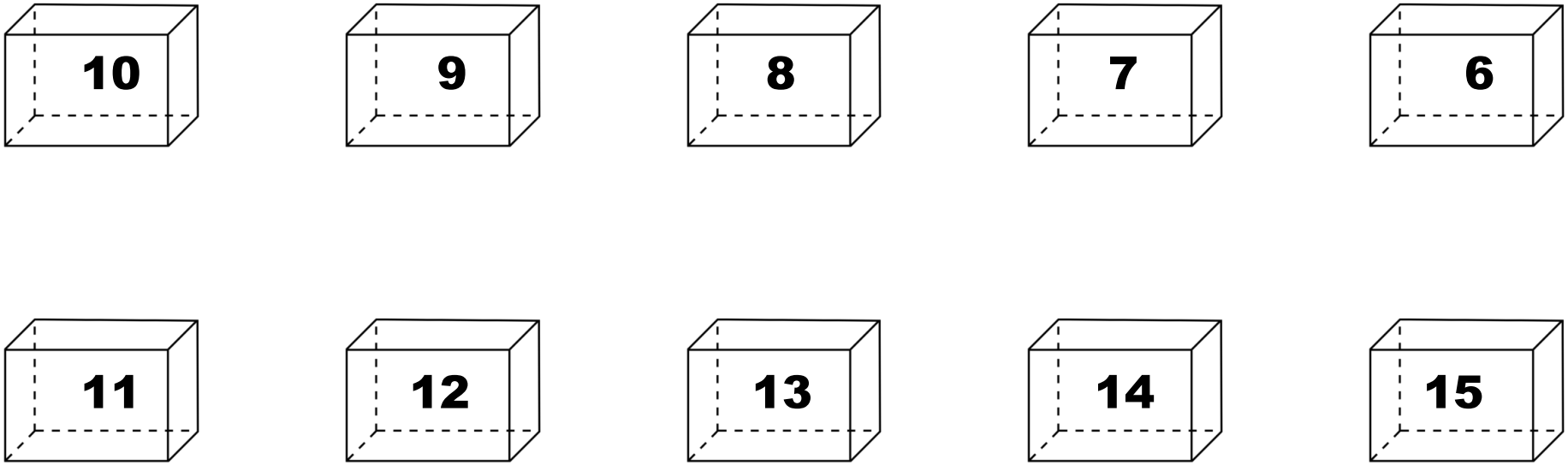


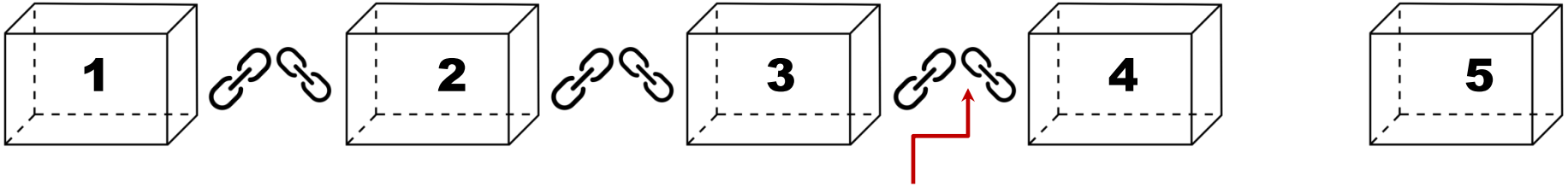
Mathematically connected Hash of **Block 1** embedded in **Block 2**



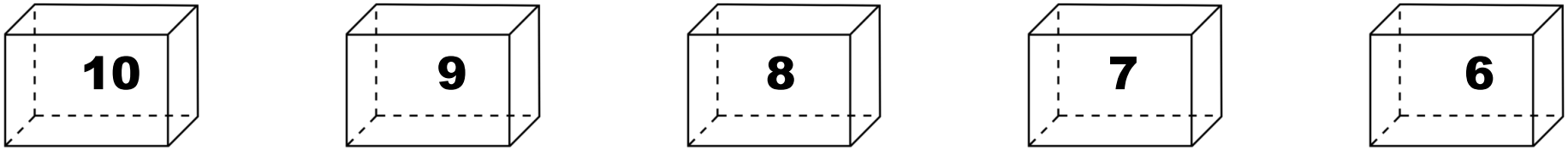


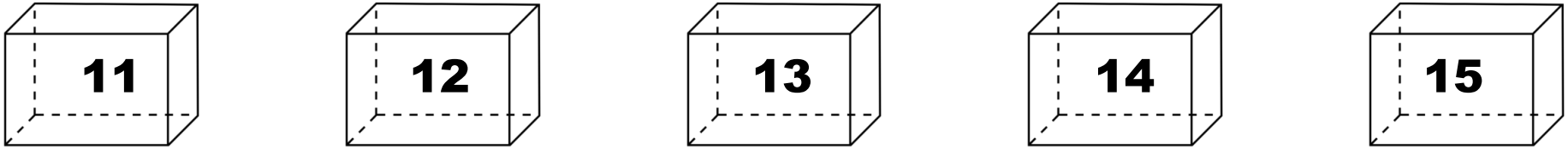
Mathematically connected Hash of **Block 2** embedded in **Block 3**

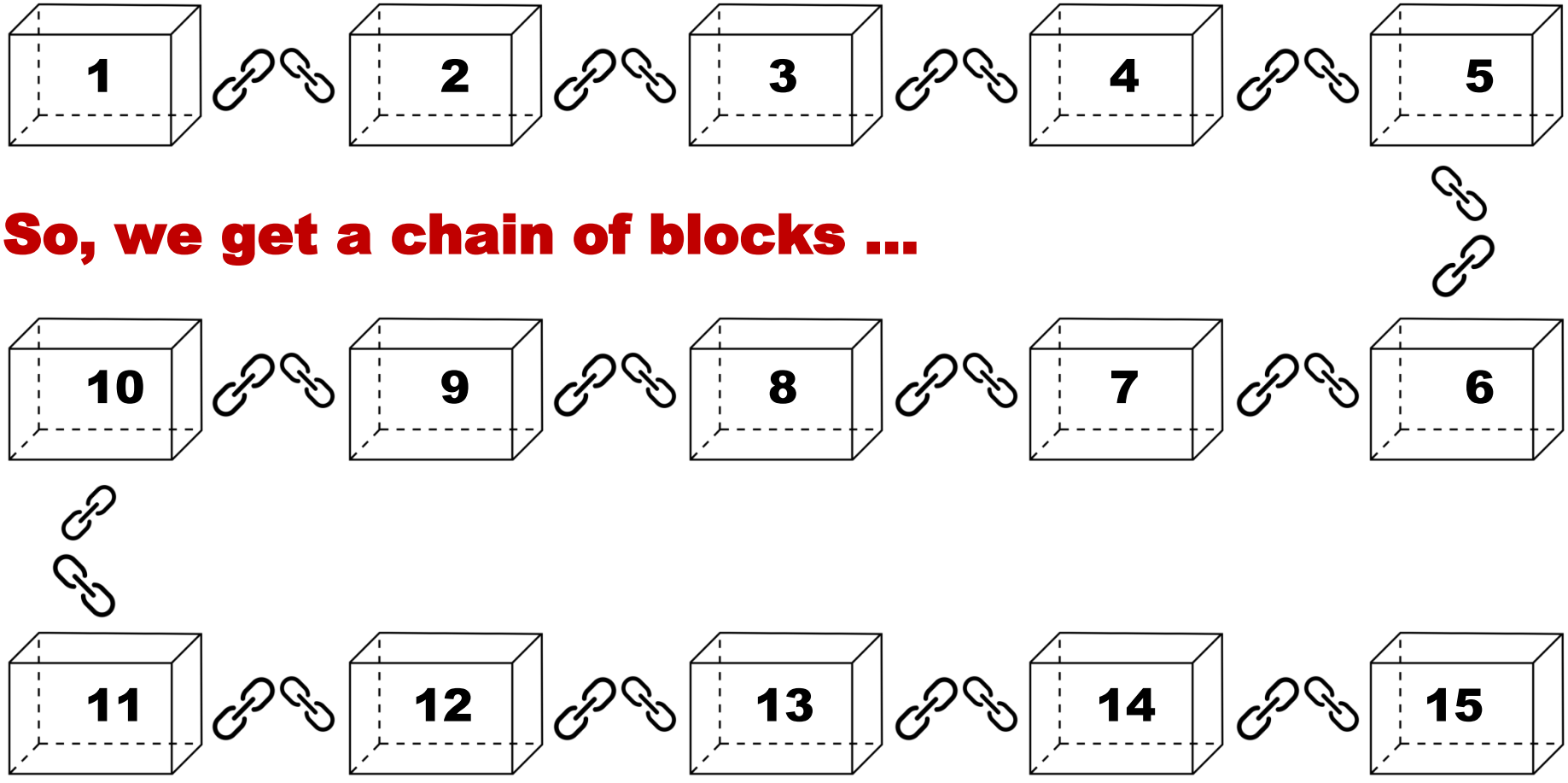


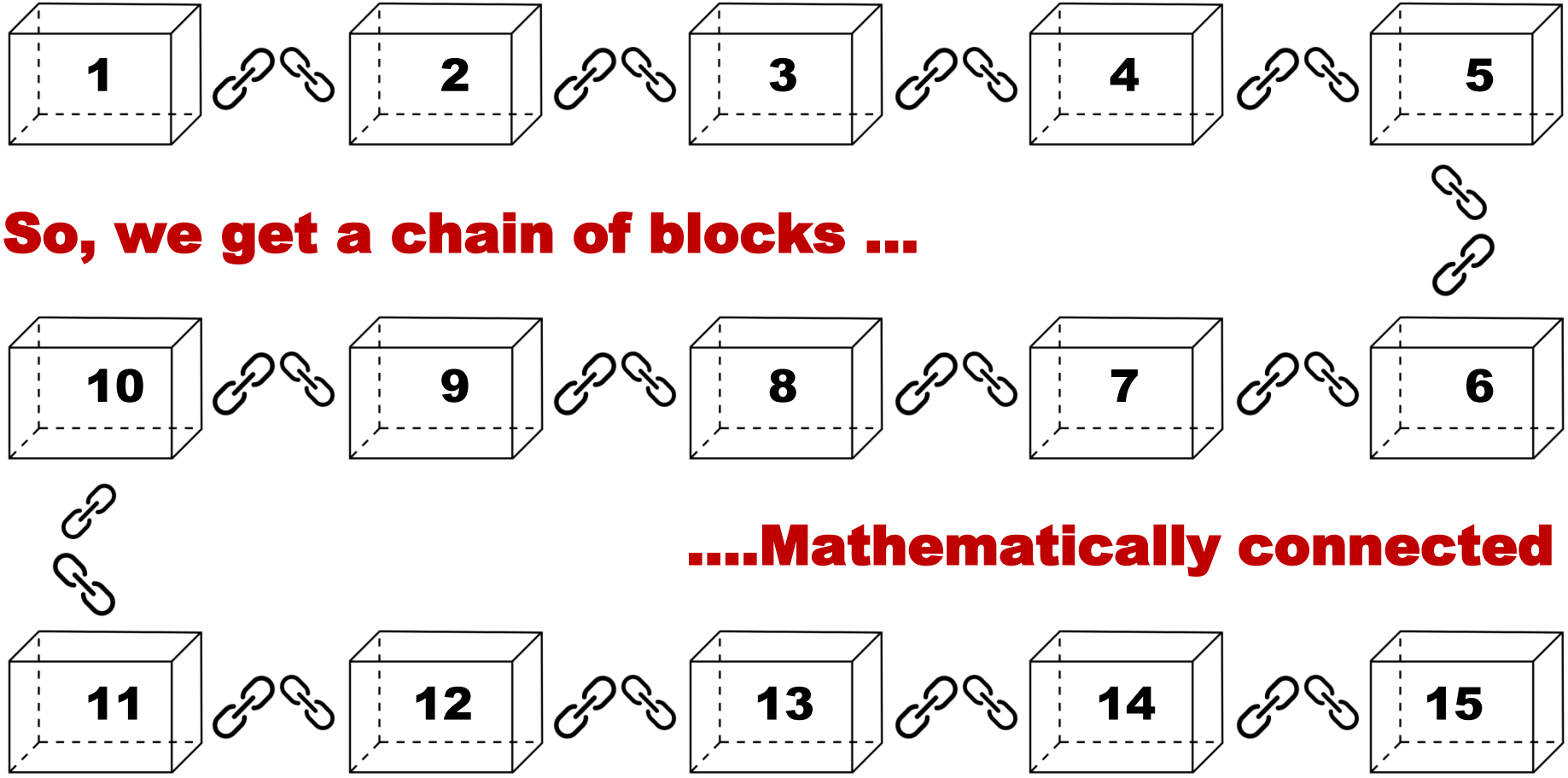


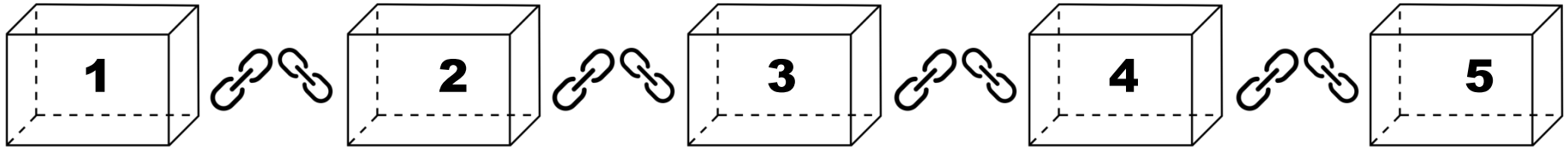
Mathematically connected Hash of **Block 3** embedded in **Block 4**






1
2
3
4
5
So, we get a chain of blocks ...
6
7
8
9
10
11
12
13
14
15

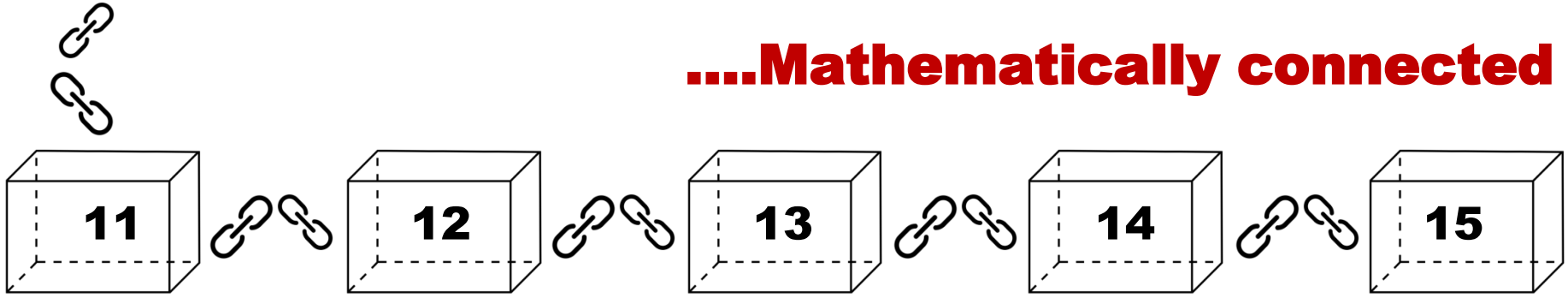

1
2
3
4
5
So, we get a chain of blocks ...
10
9
8
7
6
....Mathematically connected
11
12
13
14
15

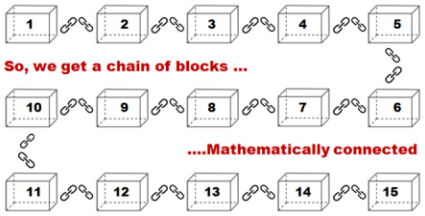


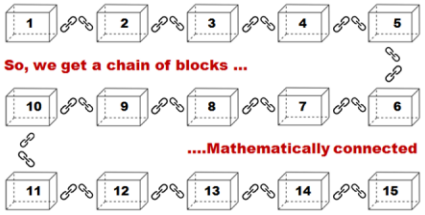
So, we get a chain of blocks ...

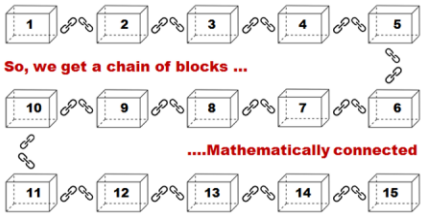
BLOCKCHAIN

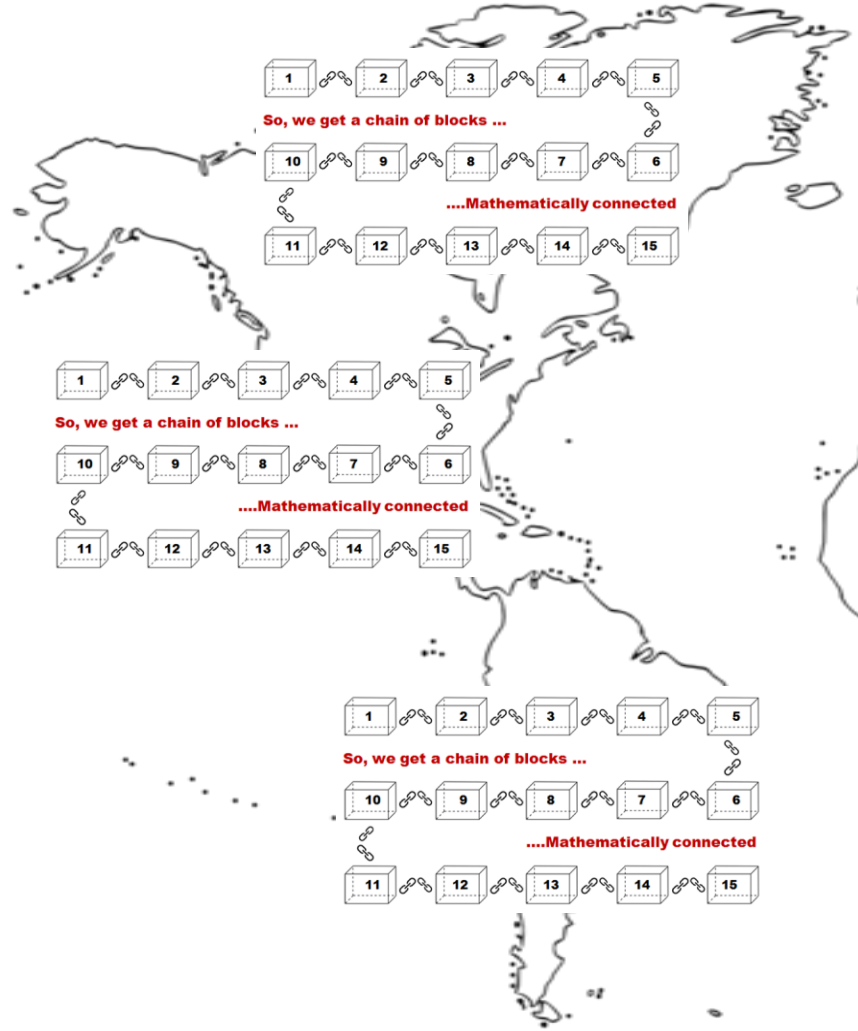
....Mathematically connected

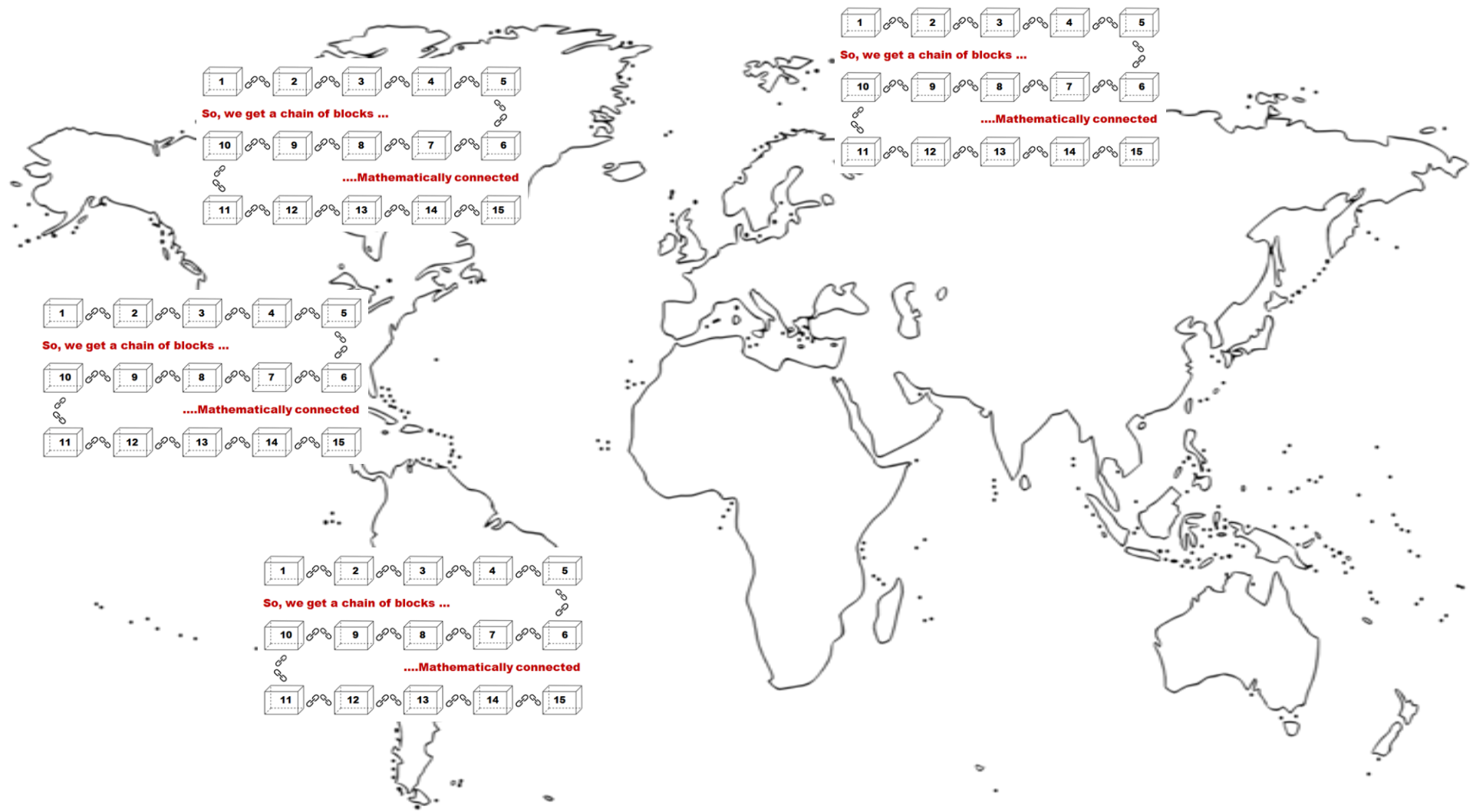


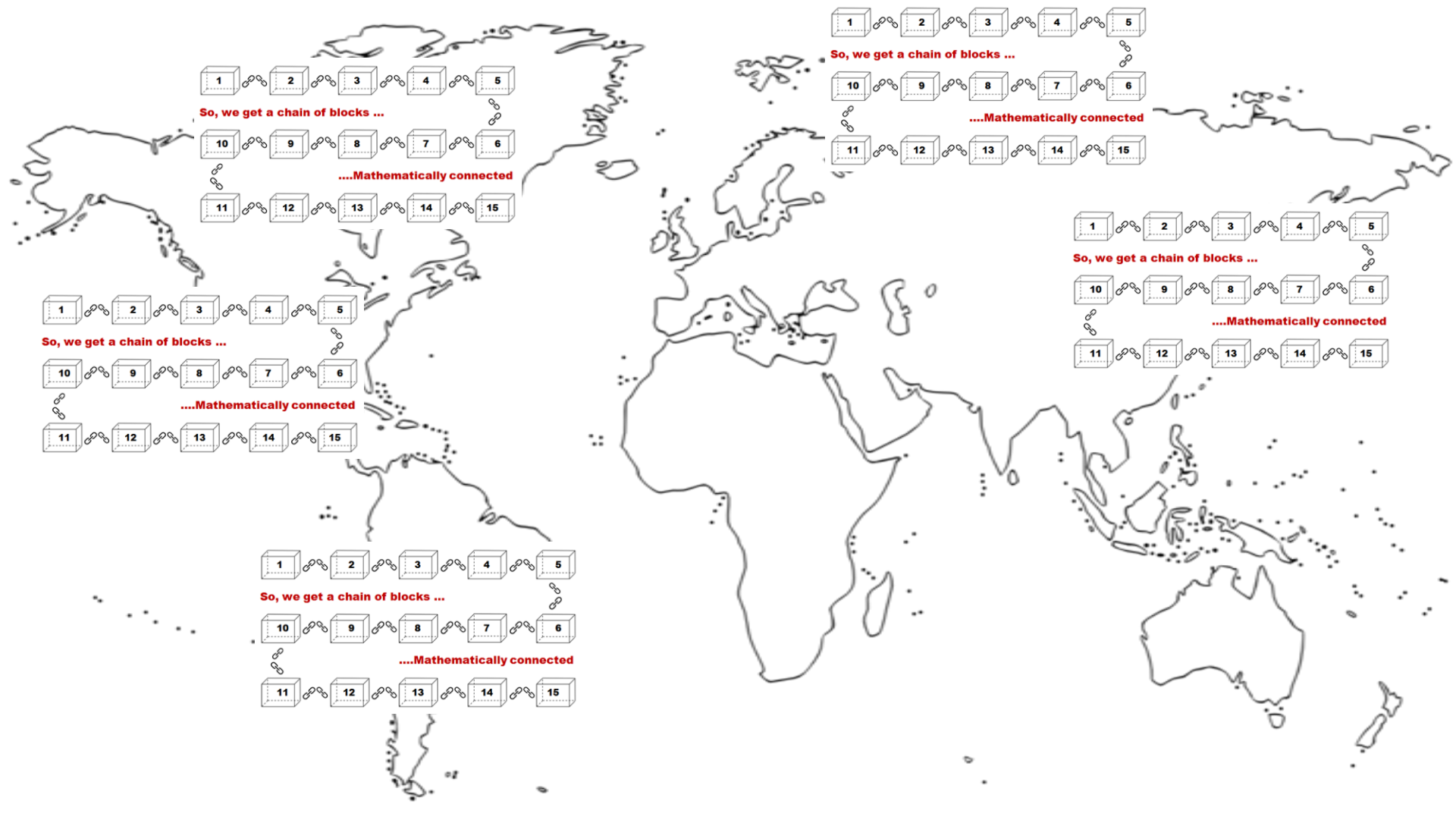

1
2
3
4
5
So, we get a chain of blocks ...
10
9
8
7
6
....Mathematically connected
11
12
13
14
15

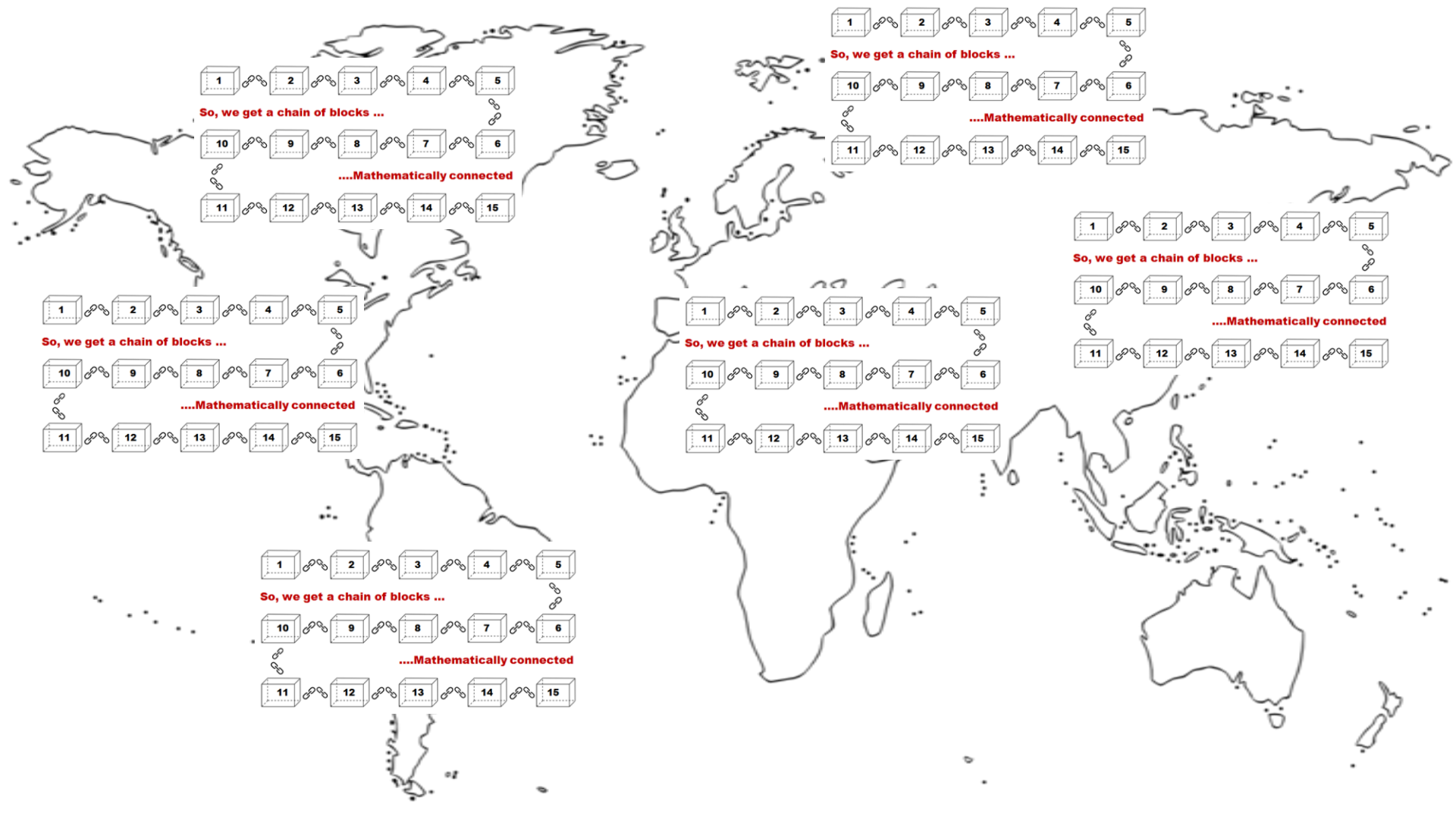

1
2
3
4
5
So, we get a chain of blocks ...
10
9
8
7
6
....Mathematically connected
11
12
13
14
15

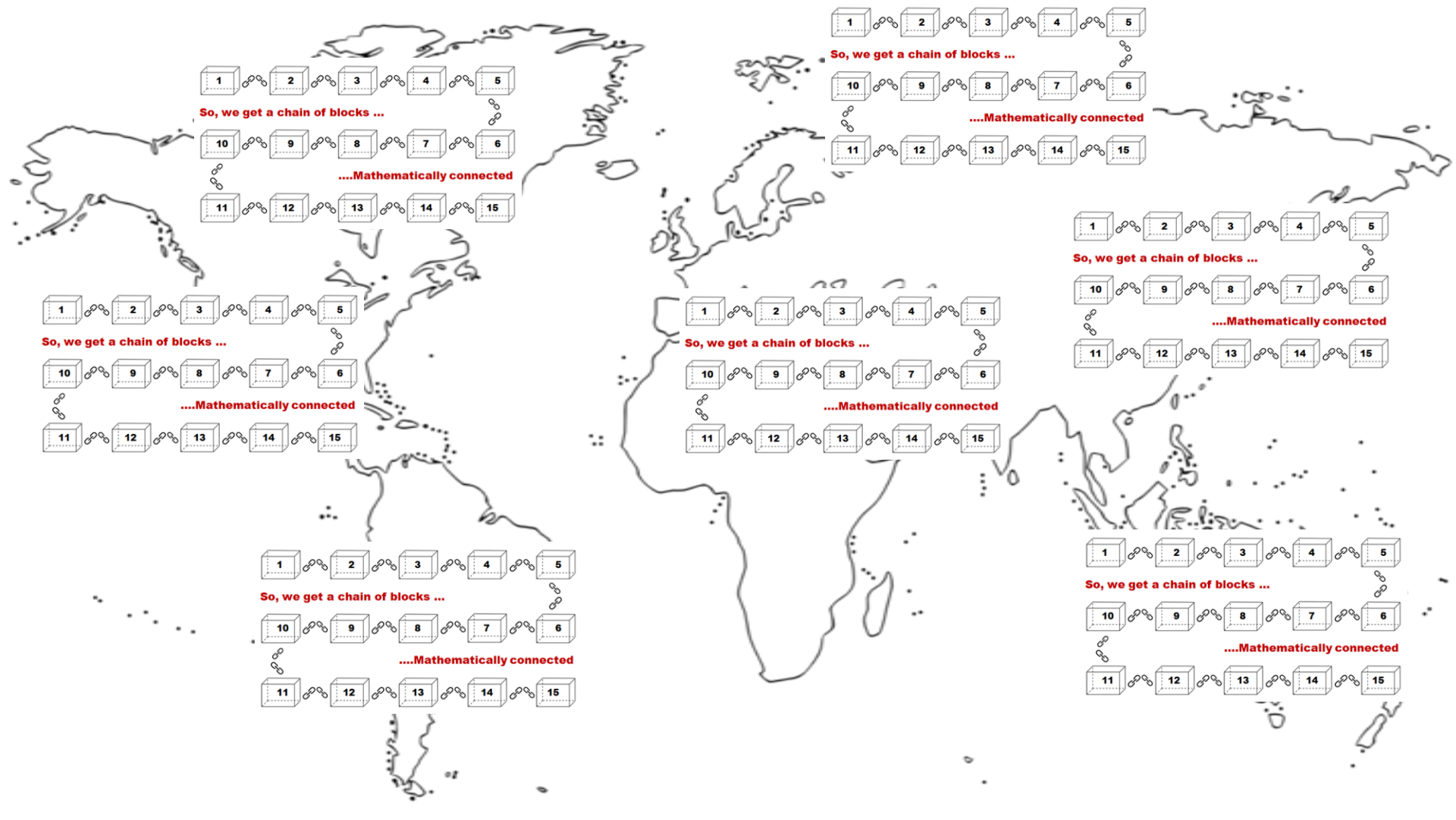

1
2
3
4
5
So, we get a chain of blocks ...
10
9
8
7
6
....Mathematically connected
11
12
13
14
15


1
2
3
4
5
So, we get a chain of blocks ...
10
9
8
7
6
....Mathematically connected
11
12
13
14
15
1
2
3
4
5
So, we get a chain of blocks ...
10
9
8
7
6
....Mathematically connected
11
12
13
14
15
1
2
3
4
5
So, we get a chain of blocks ...
10
9
8
7
6
....Mathematically connected
11
12
13
14
15


1 2 3 4 5
So, we get a chain of blocks ...
10 9 8 7 6
....Mathematically connected
11 12 13 14 15


1 2 3 4 5
So, we get a chain of blocks ...
10 9 8 7 6
....Mathematically connected
11 12 13 14 15


1 2 3 4 5
So, we get a chain of blocks ...
10 9 8 7 6
....Mathematically connected
11 12 13 14 15


1 2 3 4 5
So, we get a chain of blocks ...
10 9 8 7 6
....Mathematically connected
11 12 13 14 15

Trust | Third party Negation |Hash Cash| Public Keys | Private Keys | y2 = x3 + 7 | RIPEMD-160 | SHA-256 | Finite Fields | Secp256k1 standard | Distributed Ledger | 03 Jan 2009 | Satoshi Nakamoto | ASIC | Mining | Proof of work | Consensus | ECDSA| Prime Numbers| Immutability | Cryptography | Transactions | Wallets | Wallet file | data extraction | Linux system | Bitcoin Core | Bitcoin Scripts | Bloom filters | BIP0037 Bloom filters | Getting Merkle blocks | getting transactions of interest | Using multiple hash functions | Gossip Protocol | GPU |FPGA | The transaction lifecycle | The transaction data structures | Types of scripts | Coinbase transactions | Transaction validations |Transaction bugs | Difficulty adjustment and retargeting algorithms | Kimoto Gravity Well Difficulty adjustment and retargeting algorithms | Kimoto Gravity Well | [illegible] Wave | [illegible] | Hashing algorithms | Difficulty adjustment algorithms | Inter-block time | Block rewards | Reward halving rate | Block size and transaction size | Bitcoin Development Environment | Compiling Bitcoin Core from the Source Code | Selecting a Bitcoin Core Release | Configuring the Bitcoin Core Build | Building the Bitcoin Core Executables | Running a Bitcoin Core Node | Running Bitcoin Core for the First Time | Configuring the Bitcoin Core Node |Bitcoin Core Application Programming Interface (API) | Getting Information on the Bitcoin Core Client Status | Exploring and Decoding Transactions | Exploring Blocks | Using Bitcoin Core's Programmatic Interface | Advanced Transactions and Scripting | Multisignature | Pay-to-Script-Hash (P2SH) | P2SH Addresses | Benefits of P2SH | Redeem Script and Validation | Data Recording Output (RETURN) | Timelocks | Transaction Locktime (nLocktime) | Check Lock Time Verify (CLTV) | Relative Timelocks | Relative Timelocks with nSequence | Relative Timelocks with CSV | Median-Time-Past | Timelock Defense Against Fee Sniping | Scripts with Flow

WHAT DOES BLOCKCHAIN TECHNOLOGY ACTUALLY ACHIEVE?

Decentralization

Traceability

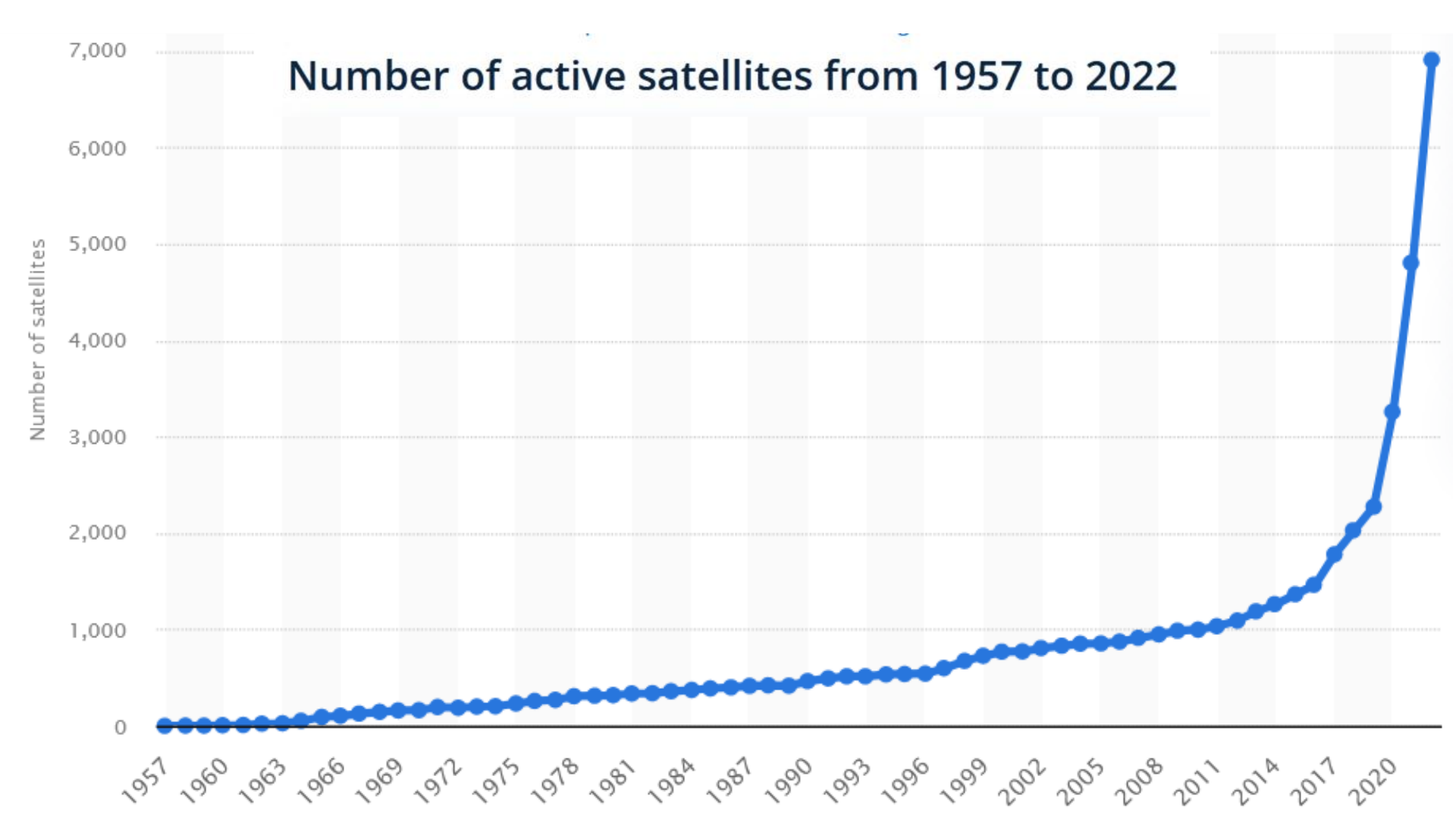
Transparency

Data Privacy

Data Security

Smart Contracts


TRUST


Number of active satellites from 1957 to 2022
Number of satellites
7,000
6,000
5,000
4,000
3,000
2,000
1,000
0
1957
1960
1963
1966
1969
1972
1975
1978
1981
1984
1987
1990
1993
1996
1999
2002
2005
2008
2011
2014
2017
2020

SpaceX may want to launch 42,000 internet satellites - about 5 times more spacecraft than humanity has ever flown

Amazon gets a green light to launch 3,000-satellite Kuiper constellation

By Andrew Jones published February 23, 2023

Comments (1)

SPACE

Amazon is about to go head to head with SpaceX in a battle for satellite internet dominance

In its bid to catch up with Starlink, the company plans to build as many as four satellites a day.

SPACE IS CHANGING

- MORE COOPERATION BETWEEN STATE ACTORS INTERNATIONALLY
- MORE COOPERATION BETWEEN COMMERCIAL ACTORS
- MORE & MULTIPLE PARTIES INVOLVED
- INFRASTRUCTURE AS A SERVICE (IaaS)
- SATELLITE AS A SERVICE (SaaS)
- GROUND STATION AS A SERVICE (GSaaS)


BUILDING
TRUST

REVOLUTION

EVOLUTION
NOT
REVOLUTION

BLOCKCHAIN TECHNOLOGY FOR SPACE

Letter

Satellite-Aided Consensus Protocol for Scalable Blockchains

Xintong Ling [1,2], Zheng Gao [1], Yuwei Le [1], Li You [1,2], Jiaheng Wang [1,2,*], Zhi Ding [3] and Xiqi Gao [1,2]

1 National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China; xtling@seu.edu.cn (X.L.); zgao@seu.edu.cn (Z.G.); ywle@seu.edu.cn (Y.L.); liyou@seu.edu.cn (L.Y.); xqgao@seu.edu.cn (X.G.)

2 The Purple Mountain Laboratories, Nanjing 210023, China

3 Department of Electrical and Computer Engineering, University of California, Davis, CA 95616 USA; zding@ucdavis.edu

* Correspondence: jhwang@seu.edu.cn

Received: 30 August 2020; Accepted: 26 September 2020; Published: 1 October 2020

check for updates

MSNET-Blockchain: A New Framework for Securing Mobile Satellite Communication Network

Ming Feng
Department of Electrical and Biomedical Engineering
University of Nevada
Reno, NV
mingf@nevada.unr.edu

Hao Xu
Department of Electrical and Biomedical Engineering
University of Nevada
Reno, NV
haoxu@unr.edu

A Blockchain Protocol for Authenticating Space Communications between Satellites Constellations

by Mohamed Torky [1,*,†], Tarek Gaber [2,3,†], Essam Goda [4,†], Vaclav Snasel [5] and Aboul Ella Hassanien [6,*,†]

[1] Department of Computer Science, Higher Institute of Computer Science and Information Systems, Culture & Science City, 6th of October City 3226010, Egypt

[2] School of Science, Engineering and Environment, University of Salford, Manchester M50 2EQ, UK

[3] Faculty of Computers and Informatics, Suez Canal University, Ismailia 8366004, Egypt

[4] College of Computing and Information Technology (CCIT), Arab Academy for Science, Technology and Maritime Transport (AASTMT), Giza 3650111, Egypt

Open source goes outer space

Translate

European Space Agency (ESA) to fund first blockchain based open source satellite network

Romain Laruelle Published on: 02/10/2019 News

Founded in 2017, SpaceChain is a community-based space platform that combines space and blockchain technologies to build the world's first open-source blockchain-based satellite network. In April 2019, SpaceChain announced its expansion and operations in the United Kingdom to explore opportunities in Europe's commercial space ecosystem. Most recently, SpaceChain UK has been awarded funding from ESA to further develop and identify commercial use-cases for its satellite blockchain technology, under the Kick-start Activity program.

AGENCY

Beyond Bitcoin: Leveraging the Blockchain for Space 4.0

https://www.esa.int/About_Us/Digital_Agenda/Beyond_Bitcoin_Leveraging_the_Blockchain_for_Space_4.0

Integration of Blockchain and IoT in Satellite Monitoring Process

Publisher: IEEE

Cite This

PDF

M. Shyamala Devi ; R. Suguna ; P.M. Abhinaya **All Authors**

3
Paper
Citations

633
Full
Text Views

Abstract:

The Internet of Things is evolving as a complete matured technology to be used in all the Smart applications and it establishes itself in the future generations of internet. As like Internet of Things, Blockchain is the blooming technology in which each node involved in the blockchain contains the distributed ledger which enhances the security and data transparency. Illegal users are not able to perform any fault transaction in the blockchain network due to its ability of performing smart contract and consensus. The Internet of Things can be merged with the blockchain to improve the performance of the application in real time. However, managing the devices connected to the sensors in IoT environment and mining the block chain remains the

Association for Computing Machinery

ACM Transactions on Internet Technology– Special Issue on

Blockchain-based Zero Trust Cybersecurity in the Internet of Things

Special Issue Guest Editors

Dr. Shancang Li
(Corresponding GE)
University of the West of England, Bristol, UK

The Internet of Things (IoT) connects a massive number of smart devices to the Internet, in which all data, applications, devices, and users require connectivity, security and trust. Traditional security approaches assume that all participants within the network perimeter are trustworthy. However, in IoT environment data, applications, devices, and users are gradually moving outside the traditional

Aims to bring together researchers from both academia and industry to discuss the most recent advances on zero trust cybersecurity and associate with blockchain in the IoT environment

DoraHacks and Cryptosat Run the First Cryptographic Trusted-Setup for Zero-Knowledge in Space

Cryptosat

January 12, 2023 · 4 min read

- **January 12, 2023 / DoraHacks, a leading global hackathon organizer and open source incentive platform announced today that they have successfully performed the first experiment to initiate a Zero-Knowledge (ZK) proof system in space.**

- **Event took place on the International Space Station (ISS)**

A Pragmatic Approach to Massive MIMO for Broadband Communication Satellites

Publisher: IEEE

Cite This

PDF

Piero Angeletti ; Riccardo De Gaudenzi All Authors

33
Paper
Citations

3091
Full
Text Views

Secure Combination of IoT and Blockchain by Physically Binding IoT Devices to Smart Non-Fungible Tokens Using PUFs

by Javier Arcenegui *, Rosario Arjona, Roberto Román and Iluminada Baturone

Microelectronics Institute of Seville (IMSE-CNM), University of Seville, CSIC, C/Américo Vespucio 28, 41092 Seville, Spain

* Author to whom correspondence should be addressed.

Sensors **2021**, *21*(9), 3119; **https://doi.org/10.3390/s21093119**

Received: 31 March 2021 / Revised: 22 April 2021 / Accepted: 27 April 2021 / Published: 30 April 2021

(This article belongs to the Collection **Security, Trust and Privacy in New Computing Environments**)

Secure Combination of IoT and Blockchain by Physically Binding IoT Devices to Smart Non-Fungible Tokens Using PUFs

by Javier Arcenegui *, Rosario Arjona, Roberto Román and Iluminada Baturone

Microelectronics Institute of Seville (IMSE-CNM), University of Seville, CSIC, C/Américo Vespucio 28, 41092 Seville, Spain

* Author to whom correspondence should be addressed.

Sensors **2021**, *21*(9), 3119; **https://doi.org/10.3390/s21093119**

Received: 31 March 2021 / Revised: 22 April 2021 / Accepted: 27 April 2021 / Published: 30 April 2021

(This article belongs to the Collection **Security, Trust and Privacy in New Computing Environments**)

Secure Combination of IoT and Blockchain by Physically Binding IoT Devices to Smart Non-Fungible Tokens Using PUFs

by Javier Arcenegui *, Rosario Arjona, Roberto Román and Iluminada Baturone

Microelectronics Institute of Seville (IMSE-CNM), University of Seville, CSIC, C/Américo Vespucio 28, 41092 Seville, Spain

* Author to whom correspondence should be addressed.

PUF security

Sensors **2021**, *21*(9), 3119; https://doi.org/10.3390/s21093119

Received: 31 March 2021 / Revised: 22 April 2021 / Accepted: 27 April 2021 / Published: 30 April 2021

(This article belongs to the Collection **Security, Trust and Privacy in New Computing Environments**)


NFT
non-fungible token
Standards

NFT Standards

non-fungible token

ERC-20
ERC-55
ERC-67
ERC-721
ERC-777
ERC-827
ERC-884
ERC-918
ERC-948
ERC-3100
ERC-1969
ERC-1973
ERC-223
ERC-2470
ERC-2535
ERC-2612
ERC-2665
ERC-2917
ERC-3000
ERC-821
ERC-998
ERC-1155
ERC-1400
ERC-1581
ERC-1967
ERC-3156
ERC-3664
ERC-4088
ERC-721x
ERC-779

IPFS-tiny: attempting to take IPFS to Space

April 12, 2023 *Nikoletta Triantafyllopoulou* Updates *No Comments*

The Libre Space Foundation (LSF) has been working on developing IPFS-tiny. A project aimed to bring the InterPlanetary File System (IPFS) to…*other planets* and Space.

The development of IPFS-tiny is funded by Protocol Labs.

IPFS-tiny is built in C++, and it is operating and file system agnostic. It is designed to work well on embedded systems and resource-limited devices, such as satellites and spacecraft.

Inter Planetary File System

Content Addressing

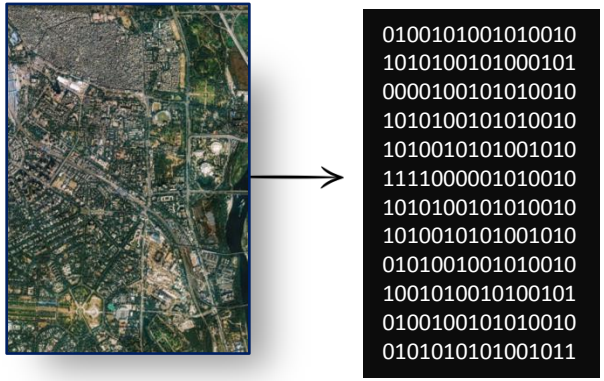
Instead of being location-based, IPFS addresses a file by WHAT'S IN IT, or by its CONTENT

HOW? EXAMPLE

Inter Planetary File System

INPUT

Inter Planetary File System



INPUT **BINARY**

Inter Planetary File System

0100101001010010
1010100101000101
0000100101010010
1010100101010010
1010010101001010
1111000001010010
1010100101010010
1010010101001010
0101001001010010
1001010010100101
0100100101010010
0101010101001011

0101010100
1010101010
1010100101

0101010100
0010100111
0011010101

1101010010
1010101001
0101010011

0101010010
1010010100
1101100011

1010101001
0101010100
1010101011

INPUT BINARY CHUNK

Inter Planetary File System

0100101001010010
1010100101000101
0000100101010010
1010100101010010
1010010101001010
1111000001010010
1010100101010010
1010010101001010
0101001001010010
1001010010100101
0100100101010010
0101010101001011

0101010100
1010101010
1010100101

0101010100
0010100111
0011010101

1101010010
1010101001
0101010011

0101010010
1010010100
1101100011

1010101001
0101010100
1010101011

9a5bf94e37
7276200aa9
1e59ec5db9

b4f03dcd07
a63d034811
4e86aa92cff

dcff4f2c7b3
32c30ce18f
75226703d8

f0e343f0bfa
4b60071589
df3a51b376

5bfca34076
d421527f85
9c7bd5668b

INPUT **BINARY** **CHUNK** **DIGEST**

Inter Planetary File System

0100101001010010
1010100101000101
0000100101010010
1010100101010010
1010010101001010
1111000001010010
1010100101010010
1010010101001010
0101001001010010
1001010010100101
0100100101010010
0101010101001011

0101010100
1010101010
1010100101

0101010100
0010100111
0011010101

1101010010
1010101001
0101010011

0101010010
1010010100
1101100011

1010101001
0101010100
1010101011

9a5bf94e37
7276200aa9
1e59ec5db9

b4f03dcd07
a63d034811
4e86aa92cff

dcff4f2c7b3
32c30ce18f
75226703d8

f0e343f0bfa
4b60071589
df3a51b376

5bfca34076
d421527f85
9c7bd5668b

QmNrgEMcUygbK*********

QmT5NvUtoM5n**********

QmbWqxBEKC************

QmjsdhfrYYTF************

QmOIjuFtgftsDRT*********

INPUT BINARY CHUNK DIGEST CID

Inter Planetary File System

0100101001010010
1010100101000101
0000100101010010
1010100101010010
1010010101001010
1111000001010010
1010100101010010
1010010101001010
0101001001010010
1001010010100101
0100100101010010
0101010101001011

0101010100
1010101010
1010100101

0101010100
0010100111
0011010101

1101010010
1010101001
0101010011

0101010010
1010010100
1101100011

1010101001
0101010100
1010101011

9a5bf94e37
7276200aa9
1e59ec5db9

b4f03dcd07
a63d034811
4e86aa92cff

dcff4f2c7b3
32c30ce18f
75226703d8

f0e343f0bfa
4b60071589
df3a51b376

5bfca34076
d421527f85
9c7bd5668b

QmNrgEMcUygbK*********

QmT5NvUtoM5n**********

QmbWqxBEKC************

QmjsdhfrYYTF************

QmOIjuFtgftsDRT*********

Qmd286K6pohQcTKYqnS1YhWrCiS4
gz7Xi34sdwMe9USZ7u

INPUT BINARY CHUNK DIGEST CID BASE CID

multiformats/
multihash

Self describing hashes - for future proofing

Blockchain Network for Space Object Location Gathering

Publisher: IEEE Cite This PDF

Mason J. Molesky ; Elizabeth A. Cameron ; Jerry Jones ; Michael Esposito ; Liran Cohen ; Chris Beauregard

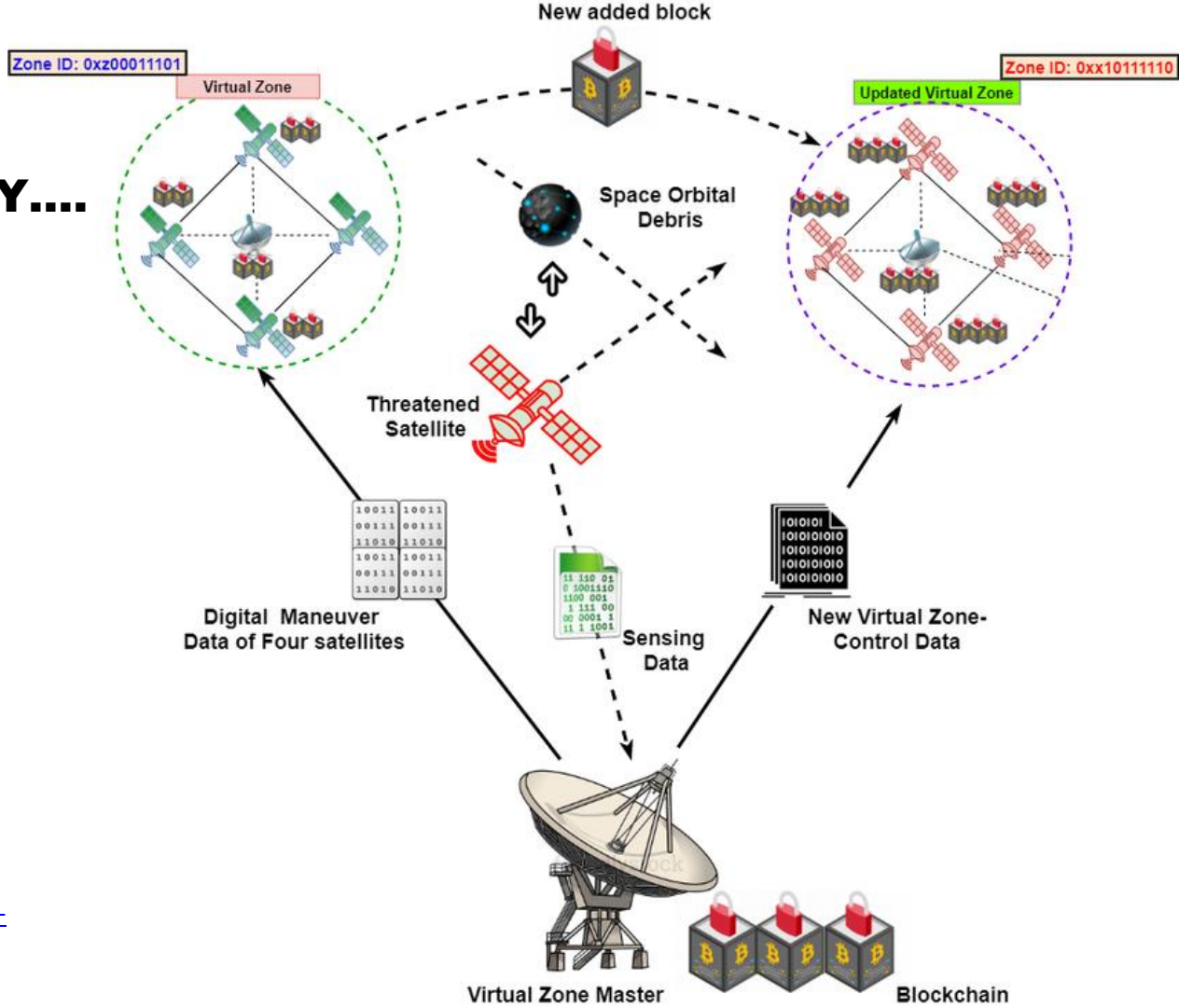
By utilizing blockchain, trusted positional data can predict and prevent collisions, saving significant costs and time. The paper presents a technological design, rationale, and risk analysis for this solution.

Digital Currency Design for Sustainable Active Debris Removal in Space

Publisher: IEEE Cite This PDF

Kenji Saito ; Shinji Hatta ; Toshiya Hanada All Authors

DON'T WORRY ABOUT SMALL FONT & UNDERSTANDING SUCH FRAMEWORKS IN HURRY....



https://www.researchgate.net/figure/Protecting-virtual-zones-against-orbital-space-debris-using-blockchain_fig3_339617040

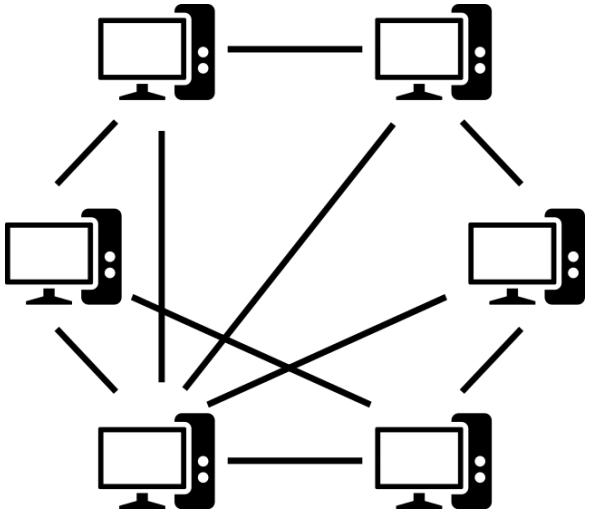
ConsenSys Unveils Ethereum-Based Satellite Tracker

Blockchain software technology company ConsenSys unveils Ethereum-based satellite tracking app TruSat.

TruSat is designed to be a citizen-powered system for creating a globally-trusted record of satellite orbits — a freely available resource that can be used to assess orbital operations in light of the space sustainability standards.

"We envision a space program in which any person can participate and contribute. So we're building collaboration platforms to diversify, democratize, and decentralize space endeavors."

SMART CONTRACTS



SELF-EXECUTING PROGRAM that **automates the actions required** in an agreement or contract.

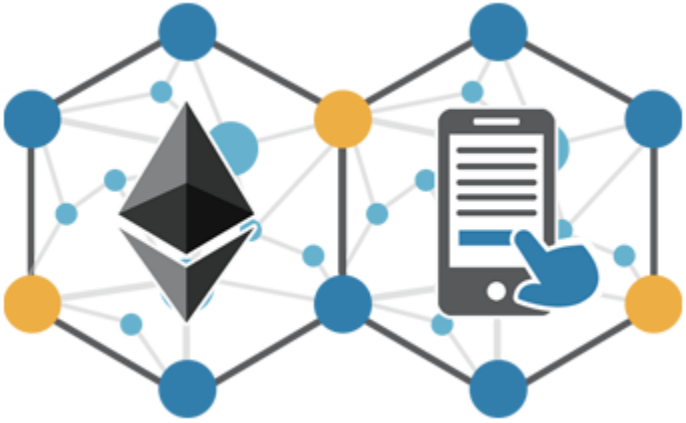
Research on Satellite Network Security Mechanism Based on BlockChain Technology

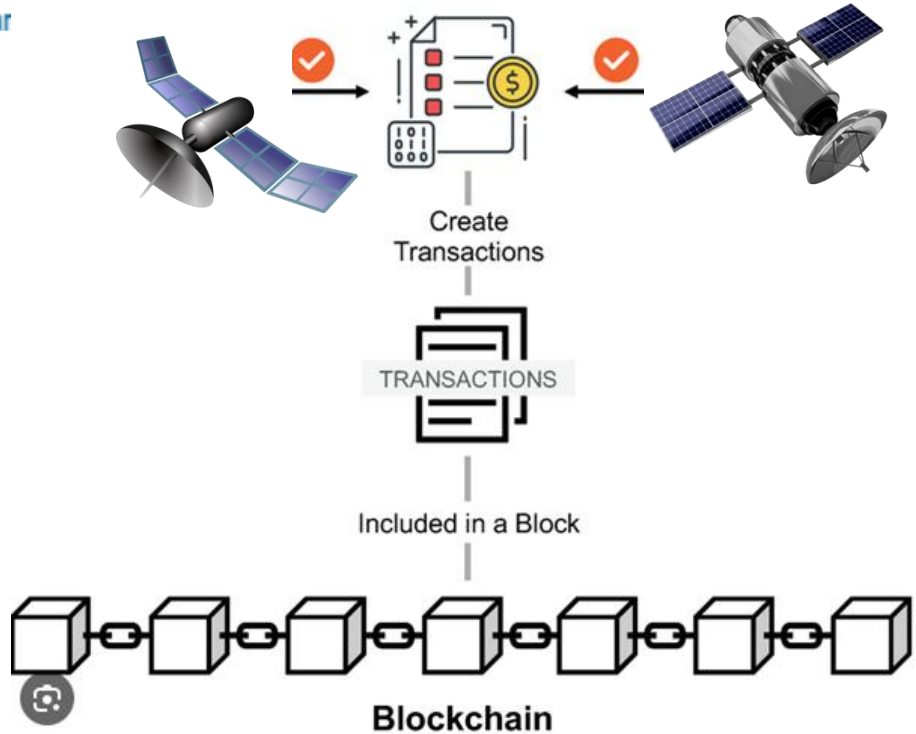
Publisher: IEEE

Cite This

PDF

Chengjie Li ; Lidong Zhu ; Michele Luglio ; Zhongqiang Luo ; Zhen Zhar





Blockchain application within a multi-sensor satellite architecture

Rohit Mital
SGT KBRWyle
Jack de La Beaujardiere
U. of Maryland, College Park
Rohan Mital
U. of Colorado, Colorado Springs
Marge Cole
NASA ESTO and SGT KBRWyle
Charles Norton
NASA Headquarters

https://ntrs.nasa.gov/api/citations/20180006549/downloads/20180006549.pdf

Onyx by J.P. Morgan launches blockchain in space

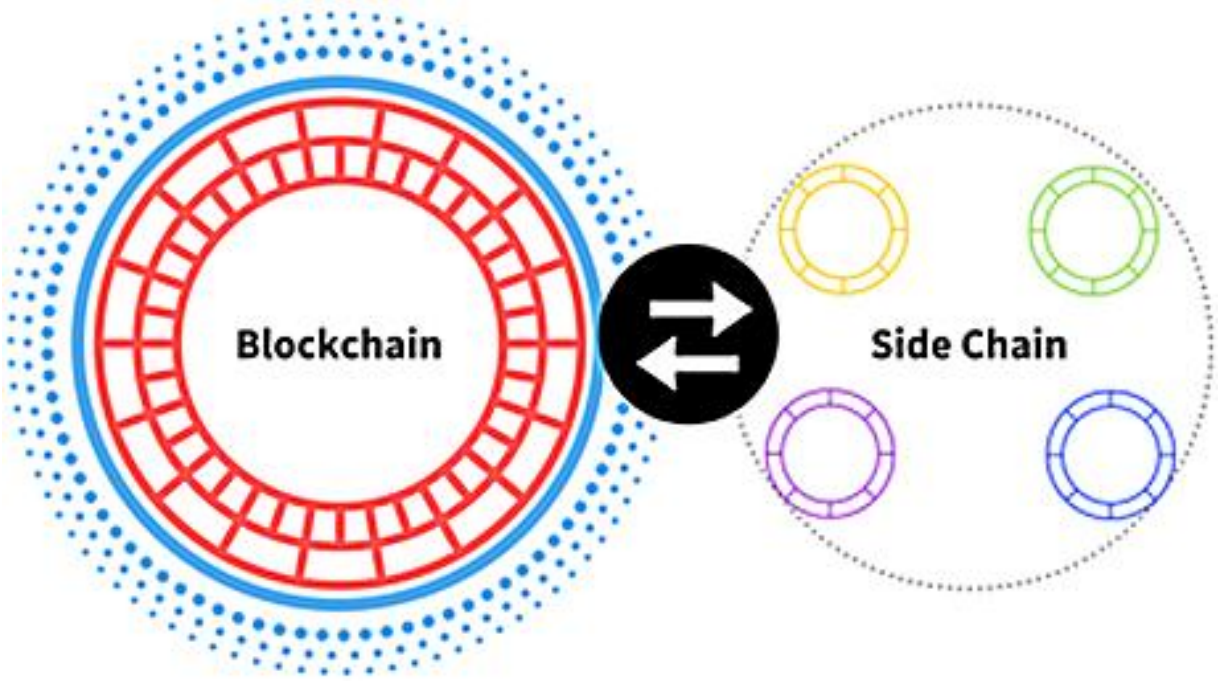
J.P. Morgan has tested the world's first bank-led tokenized value transfer in space, executed via smart contracts on a blockchain network established between satellites orbiting the earth.

BLOCKCHAIN and Satellite Space Cybersecurity

Challenges

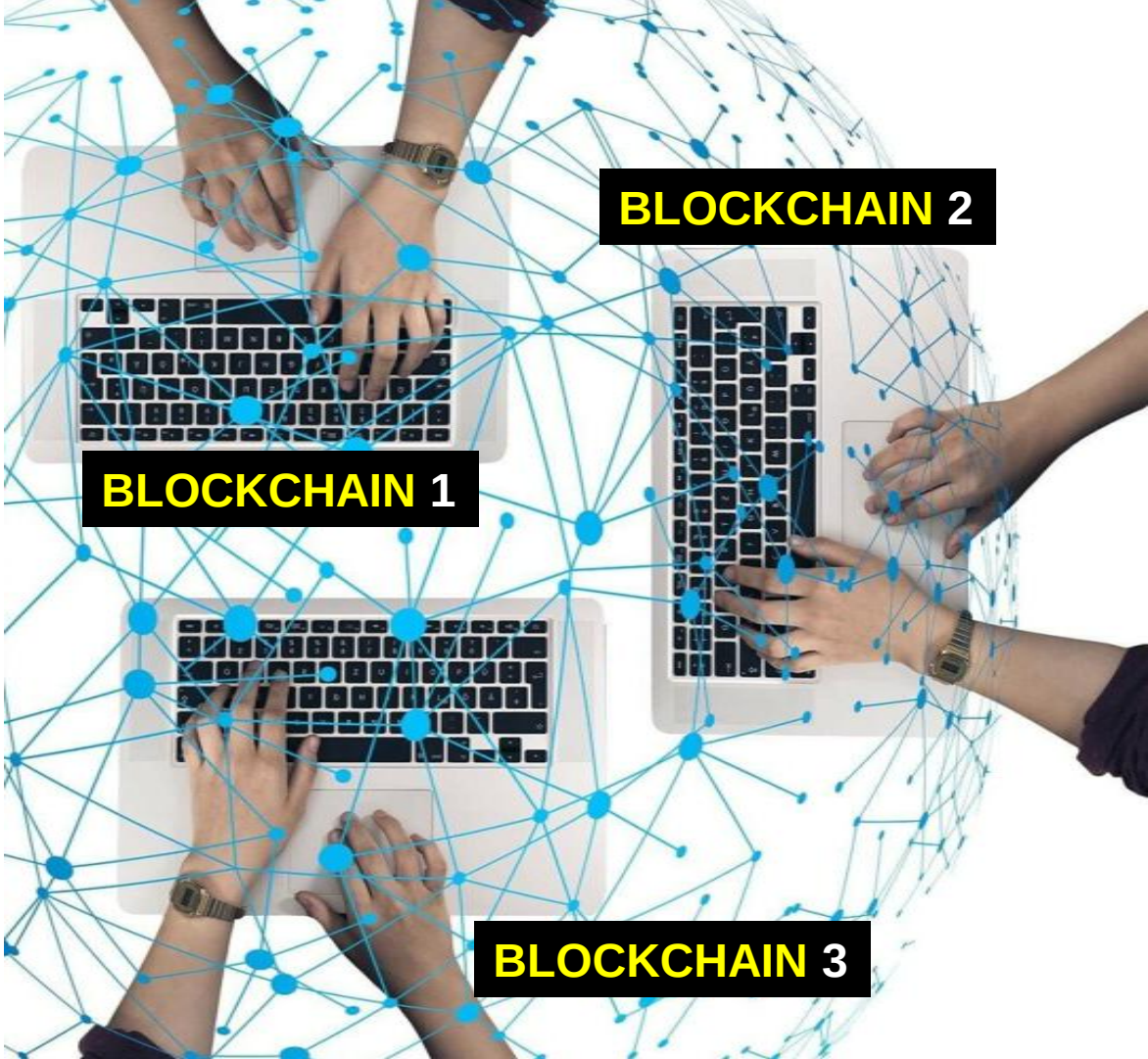
Challenges

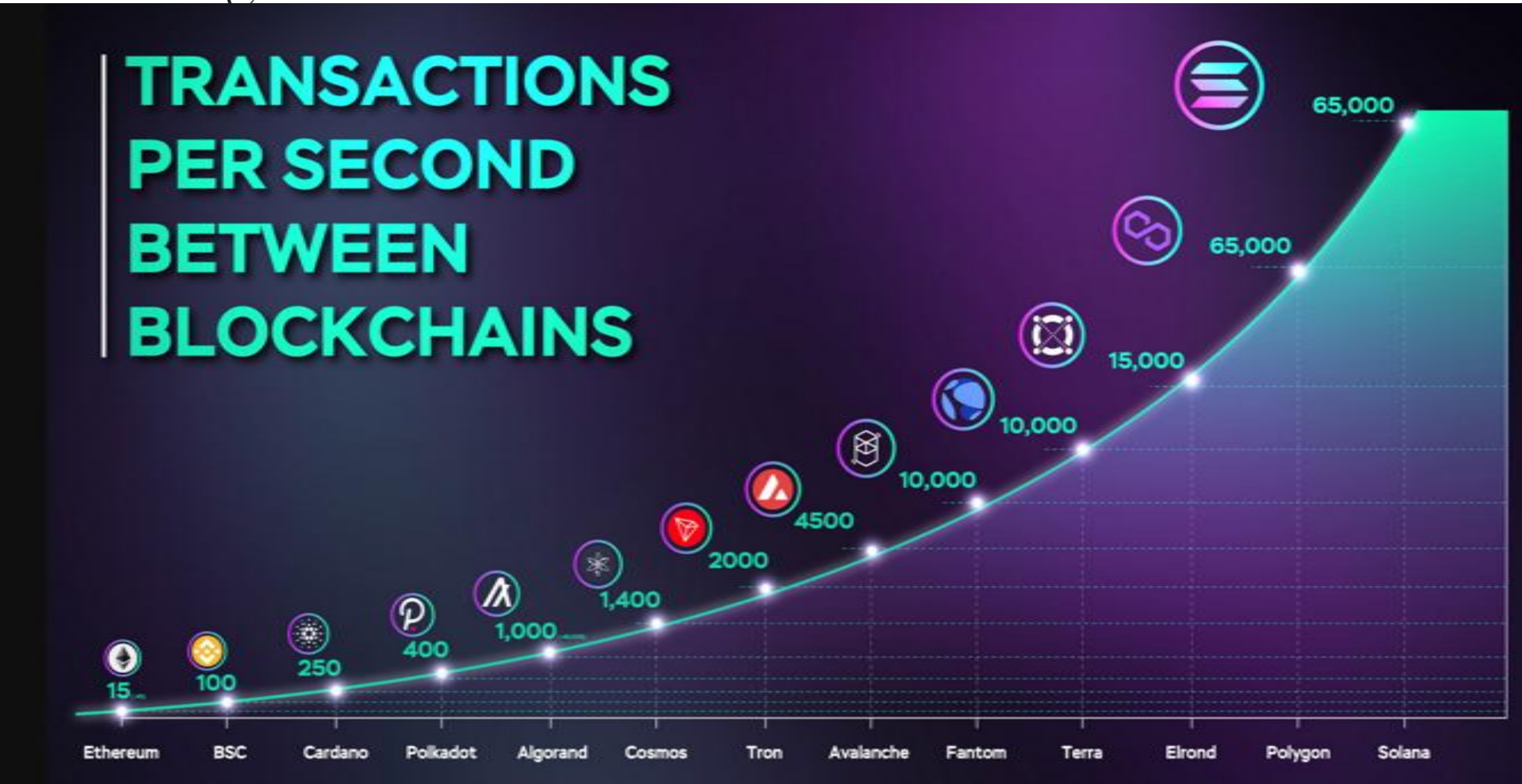
COMMON "GLOBAL"
BLOCKCHAIN PLATFORM



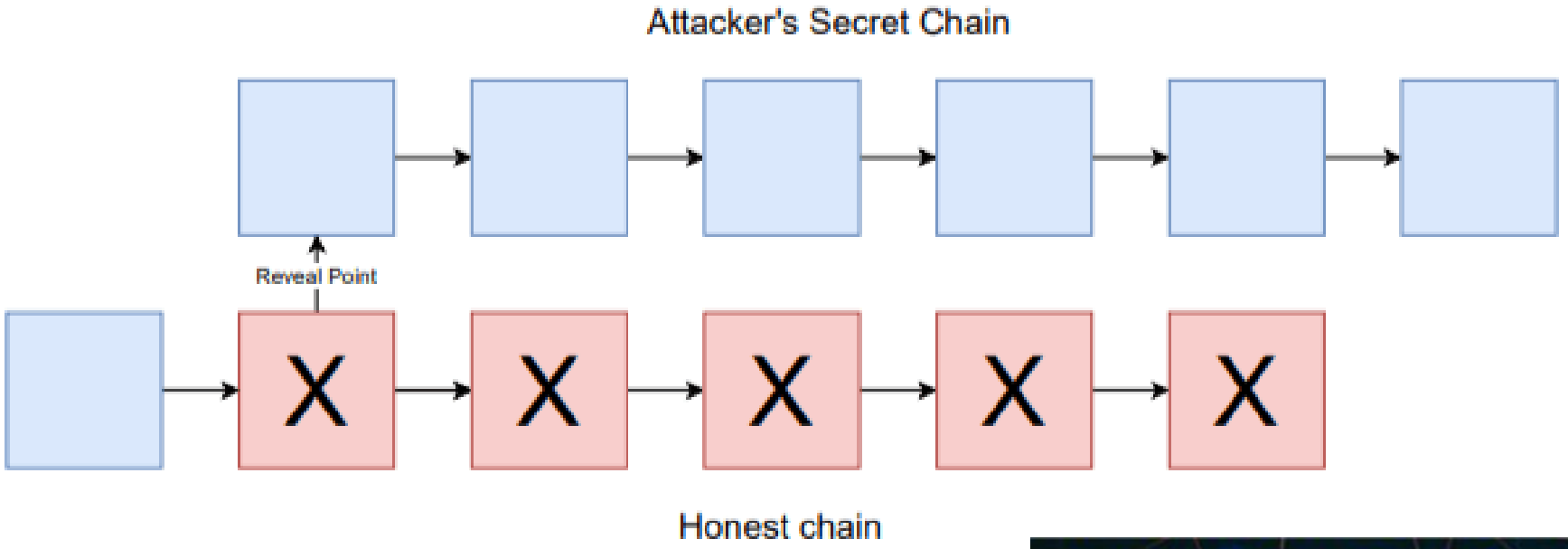
Challenges

INTER OPERABILITY




TRANSACTIONS PER SECOND BETWEEN BLOCKCHAINS
15
100
250
400
1,000
1,400
2000
4500
10,000
10,000
15,000
65,000
65,000
Ethereum
BSC
Cardano
Polkadot
Algorand
Cosmos
Tron
Avalanche
Fantom
Terra
Elrond
Polygon
Solana

Challenges

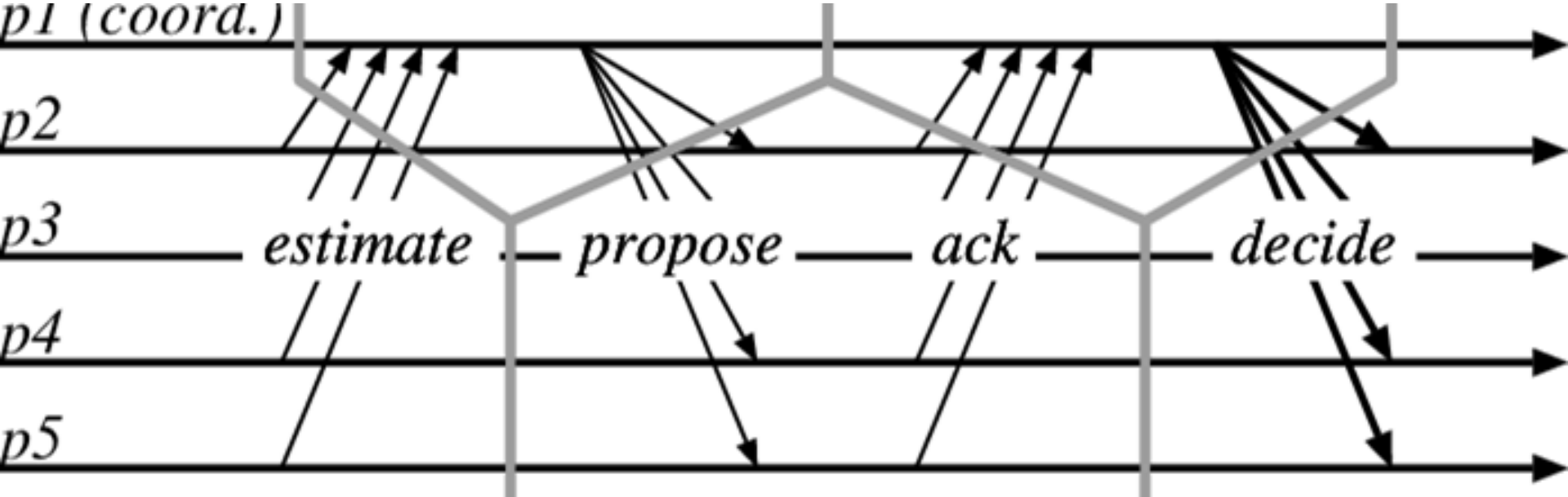


PUBLIC BLOCKCHAIN

51% Attack

Challenges

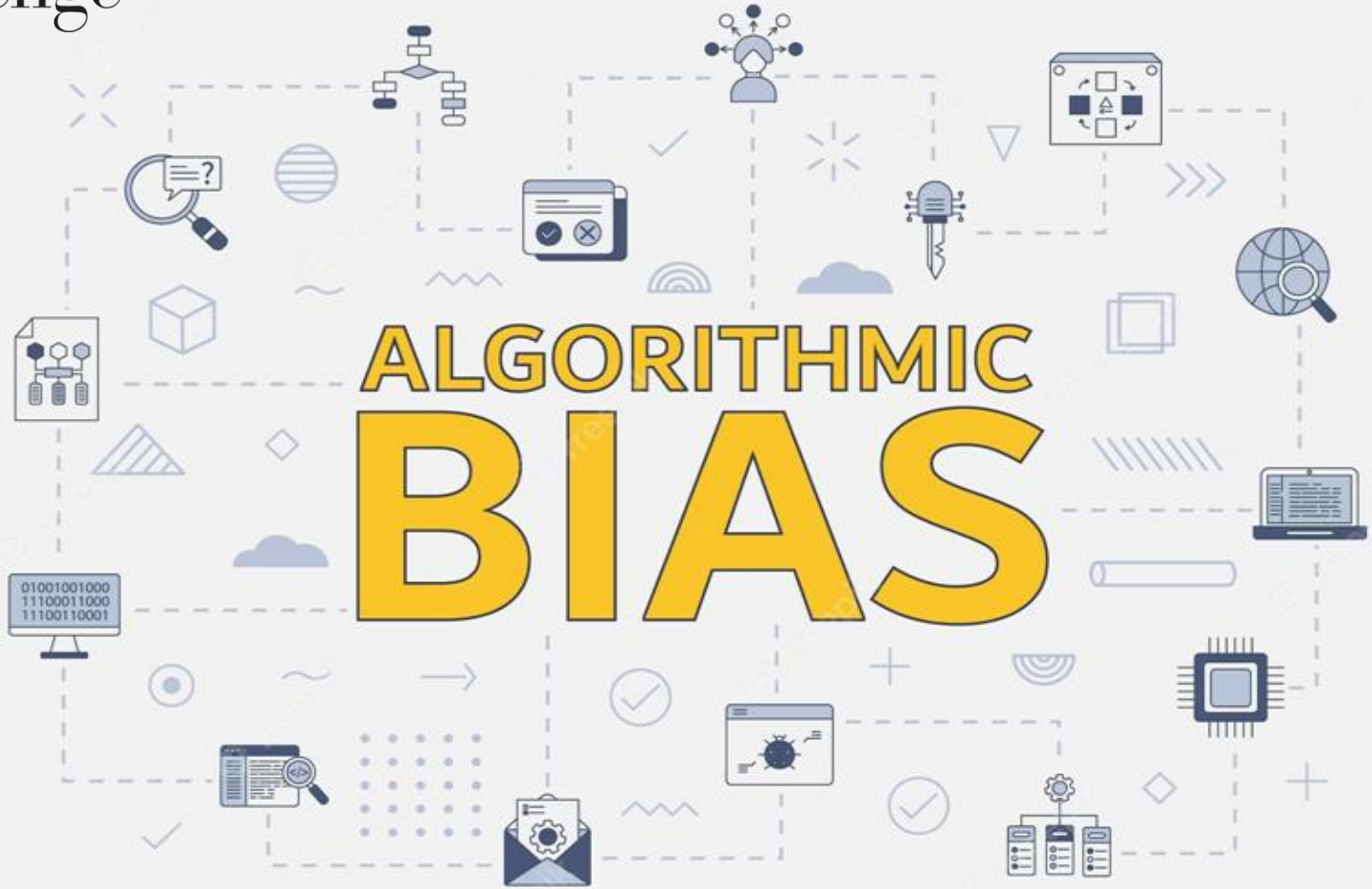
SLOW Consensus PROTOCOLS



Challenges

Challenges

Challenges



Challenges

BLOCKCHAIN

standards

Challenges

WHAT ARE WE DOING ?

NATIONAL STRATEGY ON BLOCKCHAIN

Towards Enabling Trusted Digital Platforms

Ministry of Electronics & Information Technology (MeitY)
Government of India
December 2021

NATIONAL STRATEGY ON BLOCKCHAIN

Towards Enabling Trusted Digital Platforms

सत्यमेव जयते

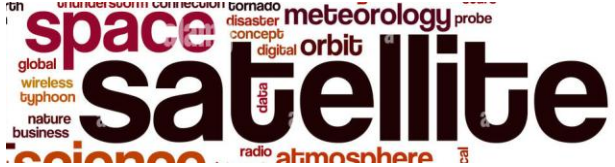
Ministry of Electronics & Information Technology (MeitY)
Government of India
December 2021

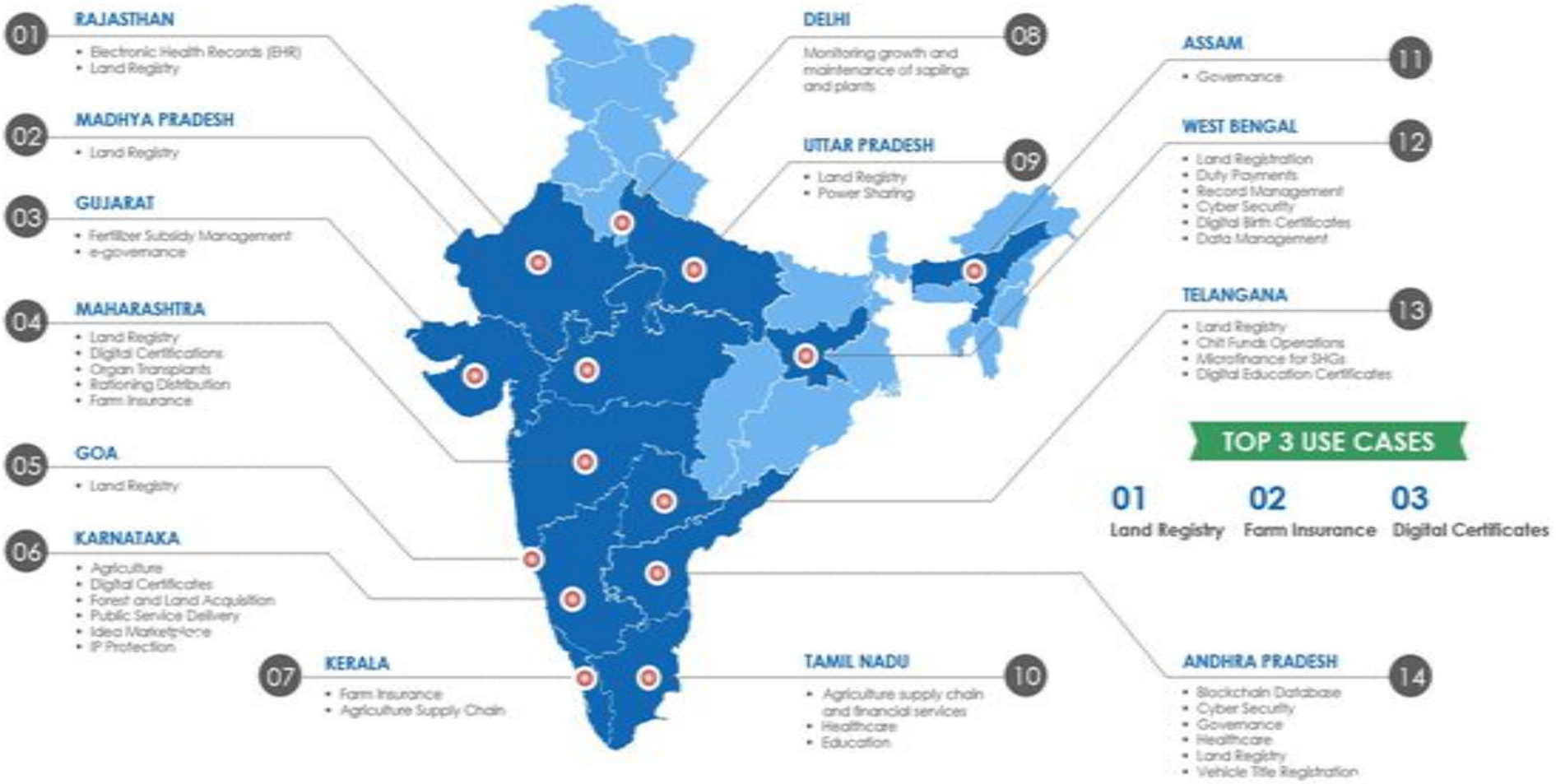
NOT

mentioned

anything

Space





https://avasant.com/report/blockchain-adoption-indian-states/

TAMIL NADU BLOCKCHAIN POLICY 2020

INFORMATION TECHNOLOGY DEPARTMENT

SOLUTION

RESEARCH & DEVELOPMENT

Hmm... I Know!!

Quick

Fast Paced

Contact me at anupam@pm.me for a **COPY OF THE PRESENTATION.** **[https://orcid.org/0000-0002-9097-2246]**

HMM... I KNOW!!

Quick

Fast Paced

JAI HIND

जय हिन्द

Thank You

Contact me at anupam@pm.me for a **COPY OF THE PRESENTATION.** **[https://orcid.org/0000-0002-9097-2246]**