New Technologies for Security Policy Enforcement in the Internet of Things (IoT)

Lyndon G. Pierson
lgpiers@gmail.com
Independent Consultant

Senior Scientist, Emeritus, Sandia National Laboratories

Fellow of the University of Southern California
Information Assurance Program

Lecturer at USC

Lecturer at NM Tech

May 17, 2018

Bio: Mr. Lyndon Pierson

- Lyndon Pierson is a Hardware/Software Security Design Engineer with over 35 years experience in high speed secure communications, network security, and information assurance.
- A “Senior Scientist Emeritus” from Sandia National Laboratories, his recent work has focused on the use of Physically Unclonable Functions (PUFs) to improve the "secret-keeping" required for securing key management systems from attack by sophisticated adversaries, and on employing diversely implemented redundant systems to increase the adversary's work factor to penetrate critical systems.
- Recently, as a Fellow of the University of Southern California Information Assurance Program, and as a lecturer at USC, he co-developed and taught major portions of a nine-course Masters of Cyber Security Engineering degree curriculum and is now teaching parts of that curriculum at NM Tech in Socorro, NM.
- Lyndon’s current interests include researching the basic science, first principle elements that should underlie our future cyber security designs, and applying and teaching these elements for the design of more secure systems.

Courses for the NMT Cybersecurity Graduate Certificate:

- CSE 561: **Foundations of Information Security**

  And 9 credits from the following:
- CSE 563: Access Control and System Security
- CSE 570: Privacy in Mobile Environments
- CSE 541: **Advanced Cryptography**
- CSE 564: **Secure System Administration**
- CSE 554: **Network Security**
- CSE 557: **Hardware-Based Network Security / IoT**
- EMGT 572: Systems, Risk, Decision Analysis

This presentation will touch on:

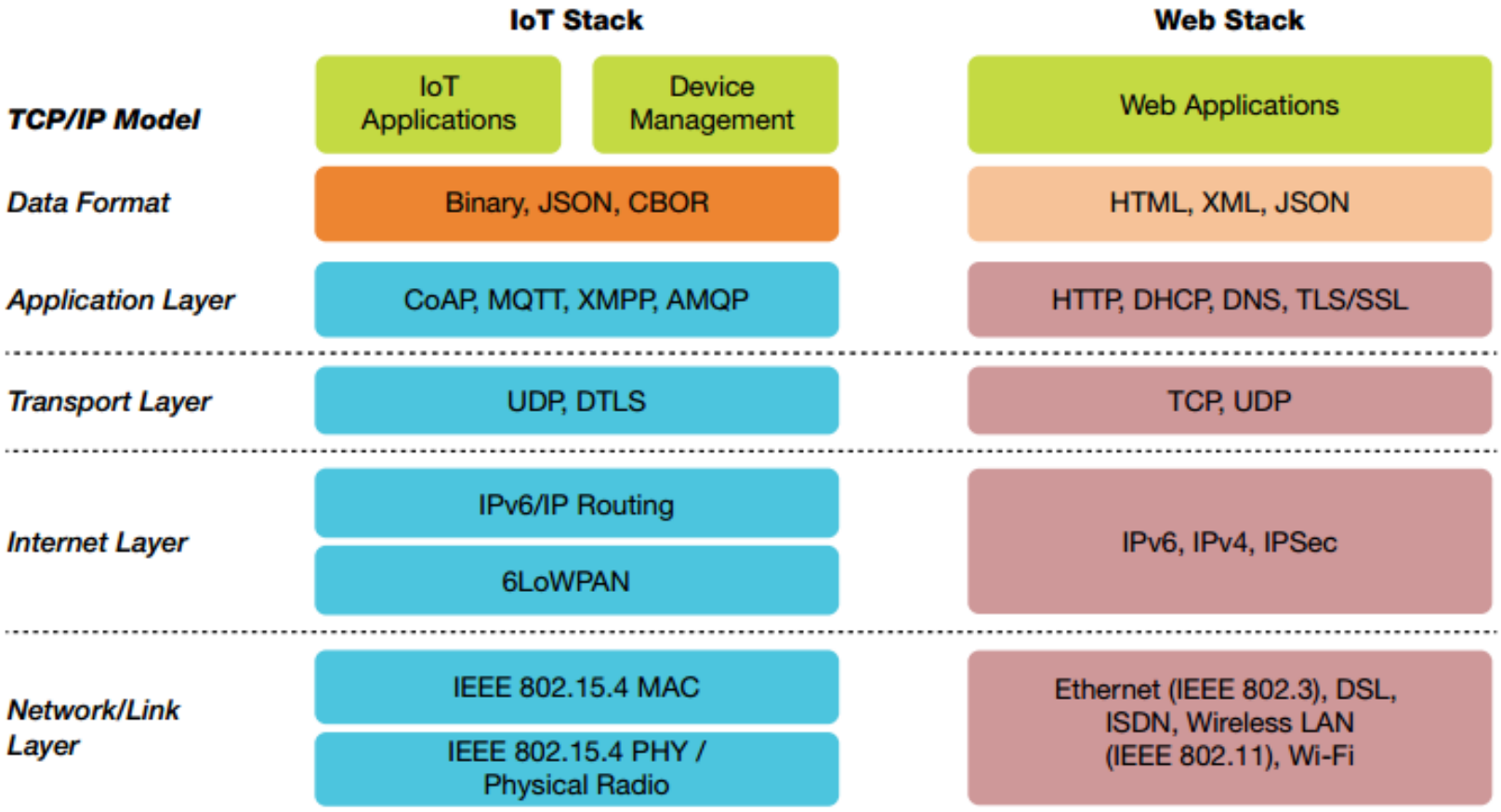
- **Background**
- IoT (Definition)
  - Security Policy (no clear policy, no security)
- Policy Enforcement Technologies
  1. Blockchain-based Distributed Trusted Ledgers (DTL) to log IoT events and authorizations
  2. Physical Unclonable Functions (PUFs)
- Summary/Conclusion

What is the “Internet of Things”?

You can search and find a lot of hyped-up definitions, but the IoT is just the “Internet” with…

- a lot more “intelligent things”, which requires
  - Bigger address space
    - Focus on IPv6 (more addresses)
    - Smaller, cheaper, lower power
  - Easier (for the user) autoconfiguration
    - Called “zeroconf”
    - These autoconfiguration protocols are the new “Achilles Heel” of the “Internet of Things”.
  - Lighter-weight and specialized protocols (CoAP,MQTT,XMPP,AMQT,etc.)
    - That better enable “things” to talk to “things”
    - Interconnect sensors, processes, things, people
    - Device-to-Device, Device-to-Server, Server-to-Server
  - Some Paradigm shifts
    - like Blockchain Trusted Distributed Ledger Technology
      - » Trustworthy “logging” of things “actions”, e.g., enabling “things” to buy “things”)
- **And will pervade our critical infrastructures therefore must be protected against “sophisticated adversaries”…**

Notional IoT Stack vs “Traditional Network Stack”



Policy: a course or principle of action adopted or proposed by a government, party, business, or individual.

- Regulatory policy
- Procurement policy
- **Security policy** is a definition of what it means to *be secure* for a system, organization or other entity.
  - Because it is so difficult to think clearly with completeness about security, rules of operation stated as "sub-policies" with no "super-policy" usually turn out to be rambling rules that fail to enforce anything with completeness. Consequently, a top-level security policy is essential to any serious security scheme and sub-policies and rules of operation are meaningless without it.

Policy involves Assets and Threats against those Assets Cyber Asset-Threat Pairs almost always of the form:

- Protect <asset> against <threat or hazard>

Typically:

- Protect **Confidentiality** of specific Information **against unauthorized disclosure**
- Protect **Integrity** of specific Information **against unauthorized modification** or spoofing
- Protect specific Information Processing **Capability against denial of authorized access (Availability)**

Cyber Asset-Threat Pairs (get specific)

- Protect Confidentiality of Information (which information, location, value) against unauthorized disclosure by …<method A, by method B, etc.>
- Protect Integrity of Information (which information, location, value) against unauthorized modification or spoofing by …<method>
- Protect Information Processing Capability (location, value) against denial of access by authorized users by …<method>

*note that this analysis treats cyber threats as “methods” not “perpetrators”

**note that policy leaves out the “how” (enforcement methods are a separate step)

If you search for IOT Security Policy…

- 6 hottest technologies for IoT security:
  - *https://www.forbes.com/sites/gilpress/2017/03/20/6-hot-internet-of-things-iot-security-technologies/#6a0e897f1b49>*
  - 1) Network Security, 2) authentication, 3) encryption, 4) PKI, 5) security analytics, 6) API security

- Lots of "policy/strategy" documents are just to sell products:
  - https://www.teneo.net/us/technology/endpoint-protection/
    - Apply "anti-virus" (its all we sell)
  - iot.aylanetworks.com/iot-security/security-wp
    - Hygiene; Process; Update; Use an IOT platform that has security and privacy measures built in. (like Ayla's IoT Platform)

- Here's a cool sample (corporate) policy, but it is missing overarching policy like "protect data on the basis of Clearance, Programmatic Authorization, Need-to-Know…"
  - http://www.altiusit.com/files/policies/AltiusITSamplePolicy.doc

IoT Security Policy Thinking is in its Infancy

- Microsoft white paper on IOT policy
  - https://mscorpmedia.azureedge.net/mscorpmedia/2017/05/IoT_WhitePaper_5_15_17.pdf
  - Ya'll improve security, Ya Hear?
- Cisco Framework
  - https://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html
  - Some good thinking about security models; mostly a couple of diagrams
- NIST Smart Cities Architecture (Draft)
  - https://s3.amazonaws.com/nist-sgcps/smartcityframework/ies-city_framework/IES-CityFrameworkdraft.docx
- NIST Framework (Draft)
  - https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf - mostly procedural (detect, respond, etc.)
- IOT Security Foundation
  - https://iotsecurityfoundation.org/wp-content/uploads/2016/12/IoT-Security-Compliance-Framework.pdf
  - Lots of Hype; ongoing work in progress; A checklist / scattergun approach (but can be useful in conjunction with a policy for context)
- Homeland Security "Strategic Principles"
  - https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf
  - Lots of fluff but some good references at end of document

- **Lots of "shallow advice, like " keep patches up-to-date; change default passwords; monitor for problems; etc."**
- **Most of these references emphasize the need for "designing security in" from the beginning, but don't specify how to do that.**
- **"checklists" can be valuable but lose sight of what is important and why**

("Secure" only has meaning with respect to the Assets and the protection Policy regarding those Assets!)

Security is Enforcement of Security Policy

Policy: Don't even think about security without it!

- First identify what to protect
  - Usually:
    - Confidentiality of specific information *and/or*
    - Integrity of specific information *and/or*
    - Availability of specific information or processing capability
- And how to protect it
  - Maybe with "guards, gates, guns" *and/or*
  - With cryptographic encryption *and/or*
  - With cryptographic authentication *and/or*
  - With robust access control mechanisms *etc*.
    - *Mandatory (non-discretionary) Policy (enforced regardless of user)*
      - *Like "check to assure the source address of a packet belongs to this node or source subnetwork" (would eliminate DDOS amplification attacks in which the source node "lies" about its address)*
    - *Discretionary Policy*
      - *Like NTK protections chosen to be applied by users*
- And how hard to work at it (Policy Enforcement)
  - $$$ ≤ value of asset(s) *(this can be hard to assess)*

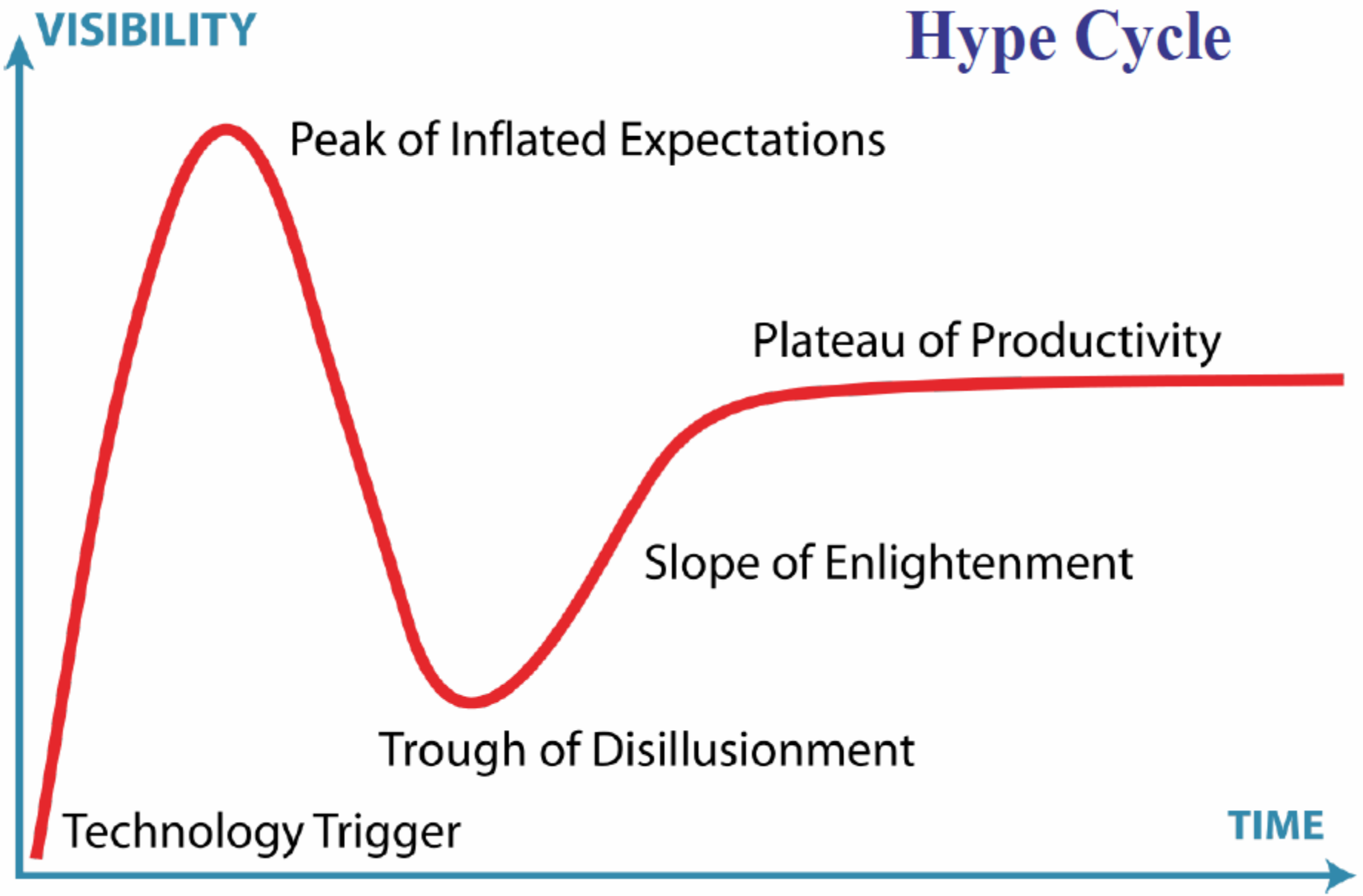
This presentation will touch on:

- Background
- IoT (Definition)
  - Security Policy (no clear policy, no security)
- **Policy Enforcement Technologies**
  1. Blockchain-based Distributed Trusted Ledgers (DTL) to log IoT events
  2. Physical Unclonable Functions (PUFs)
- Summary/Conclusion

Blockchains

- Are “Distributed Trusted Ledgers” (DTL)
  - A blockchain is a way to implement a distributed ledger, but not all distributed ledgers necessarily employ blockchains.
  - Picture an “append-only” spreadsheet that is duplicated thousands of times across a network of computers. Then imagine that this network is designed to regularly update this spreadsheet and you have a basic understanding of the blockchain.
- Blockchains ≠ Bitcoin
  - Bitcoin was the purpose of the blockchain as it was originally conceived. It’s now recognized to be only the first of many potential applications of the technology.
- Blockchains ≠ Cryptocurrency
- Cryptocurrency is:
  1. (typically) the incentive for blockchain nodes to process transactions and validate blocks of transactions.
  2. a new method of exchanging value that threatens to disrupt current banking technology

Hype Cycle



Blockchains are composed of three parts

- Block (the list of transactions, chained by Merkle Hashes)
- Chain (Merkle-hash chained to previous block)
- Network (of blockchain “full nodes” that each contain the full chain of transactions all the way back to the “genesis block”, which work to validate the current block)

Block chain Concept

Making a hash of it

INPUT

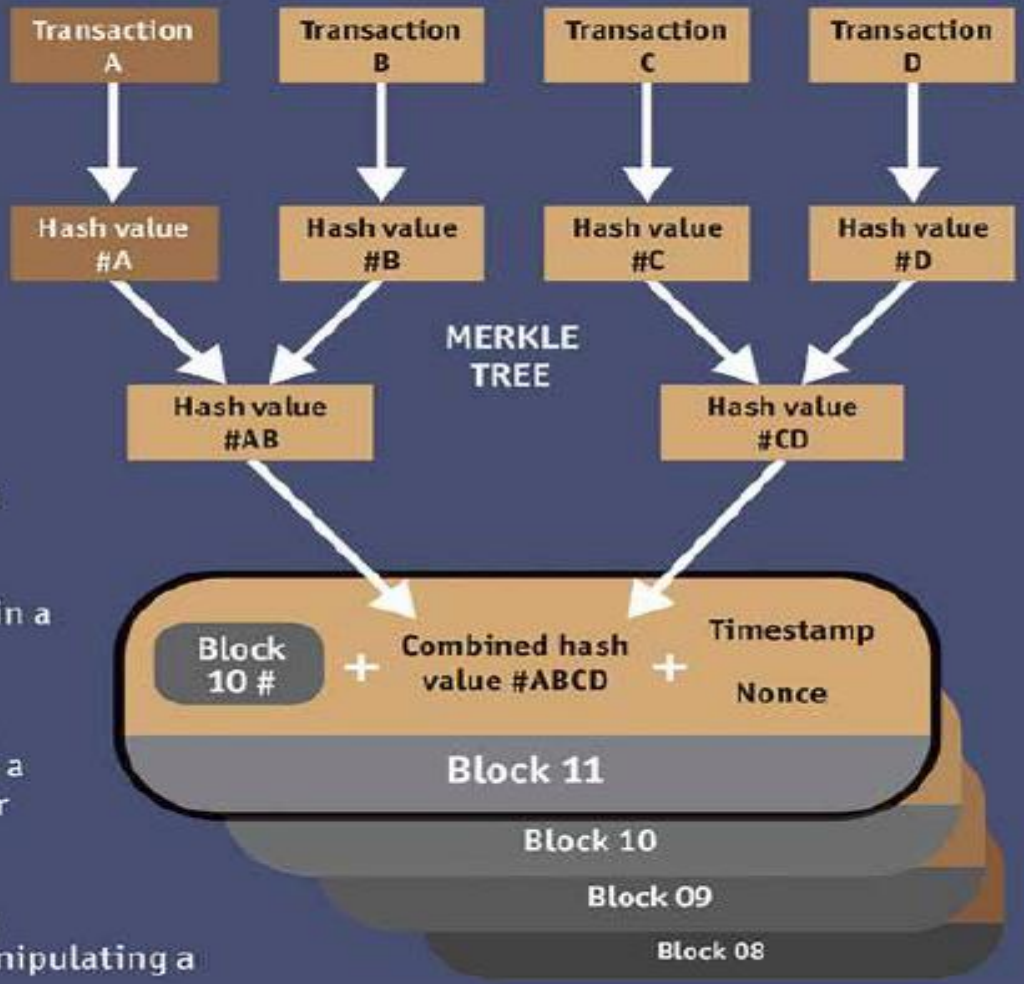
Transaction A

Any length of data

OUTPUT #A

#DFCD 24D9 AEFE 93B9

Unique hash value of fixed length



Each transaction in the set that makes up a block is fed through a program that creates an encrypted code known as the hash value.

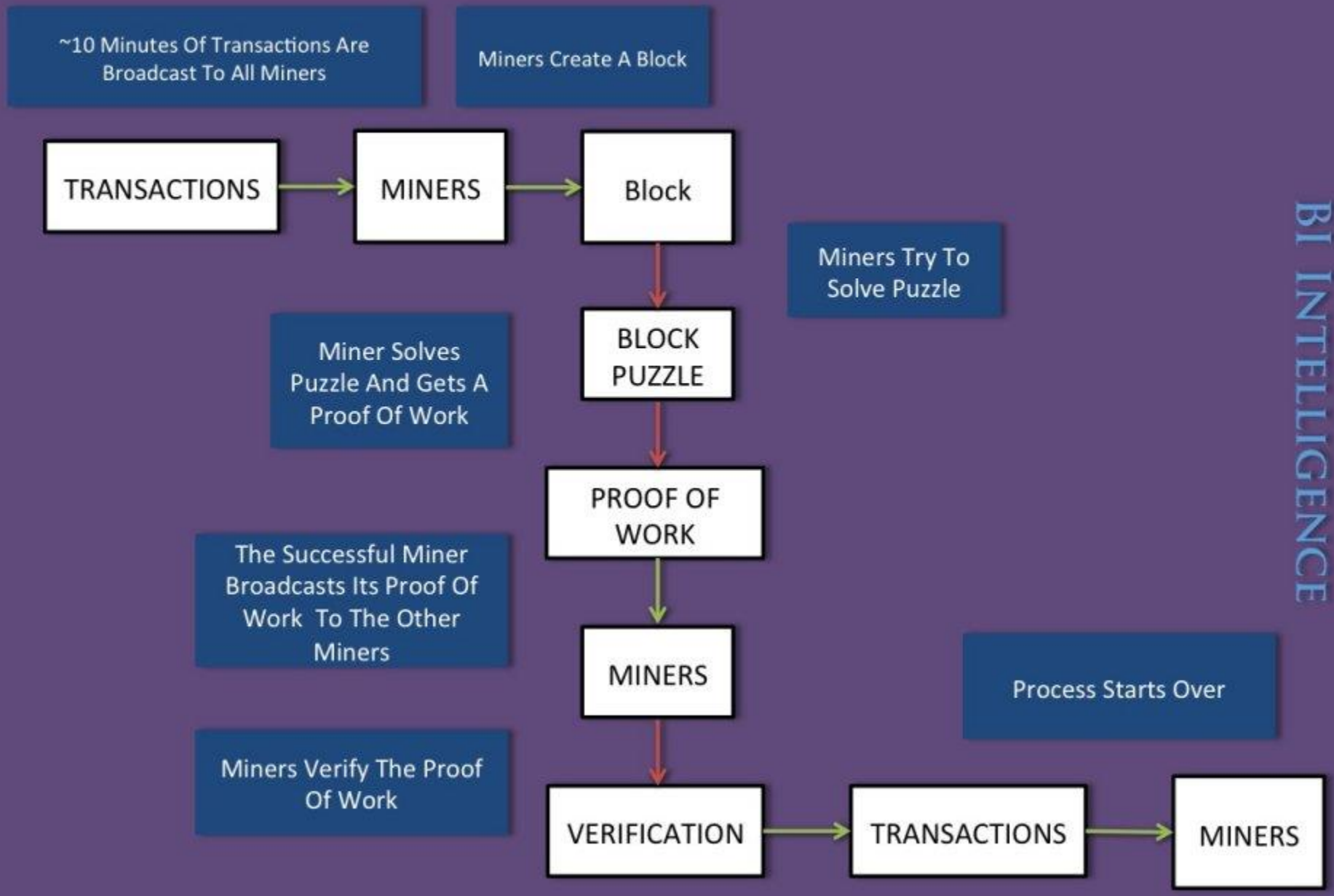
Hash values are further combined in a system known as a Merkle Tree.

The result of all this hashing goes into the block's header, along with a hash of the previous block's header and a timestamp.

The header then becomes part of a cryptographic puzzle solved by manipulating a number called the nonce.

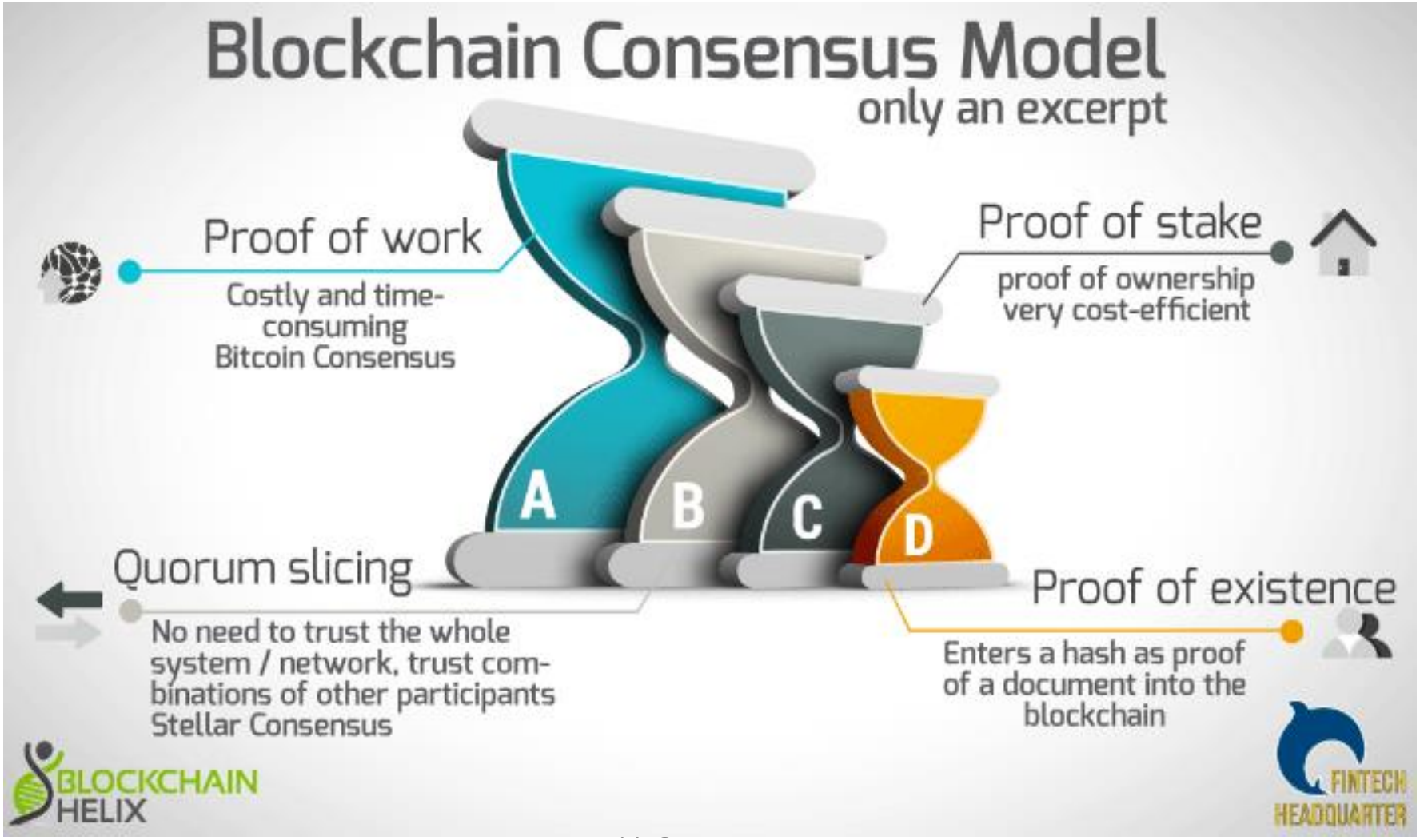
Once a solution is found the new block is added to the blockchain.

HOW THE BITCOIN BLOCKCHAIN WORKS

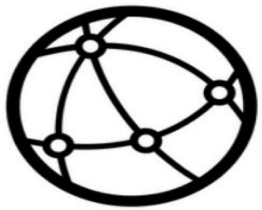


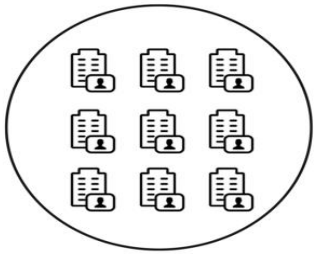
BI INTELLIGENCE

Consensus Models



LEVELS OF BLOCKCHAIN CONSENSUS





Full Decentralization

CONSENSUS LEVEL 3

Public ledger (trust & transparency)

Best for: public transactions

Pre-selected cluster

CONSENSUS LEVEL 2

- Private ledger (mutual trust)

Best for: cross-organizational transactions

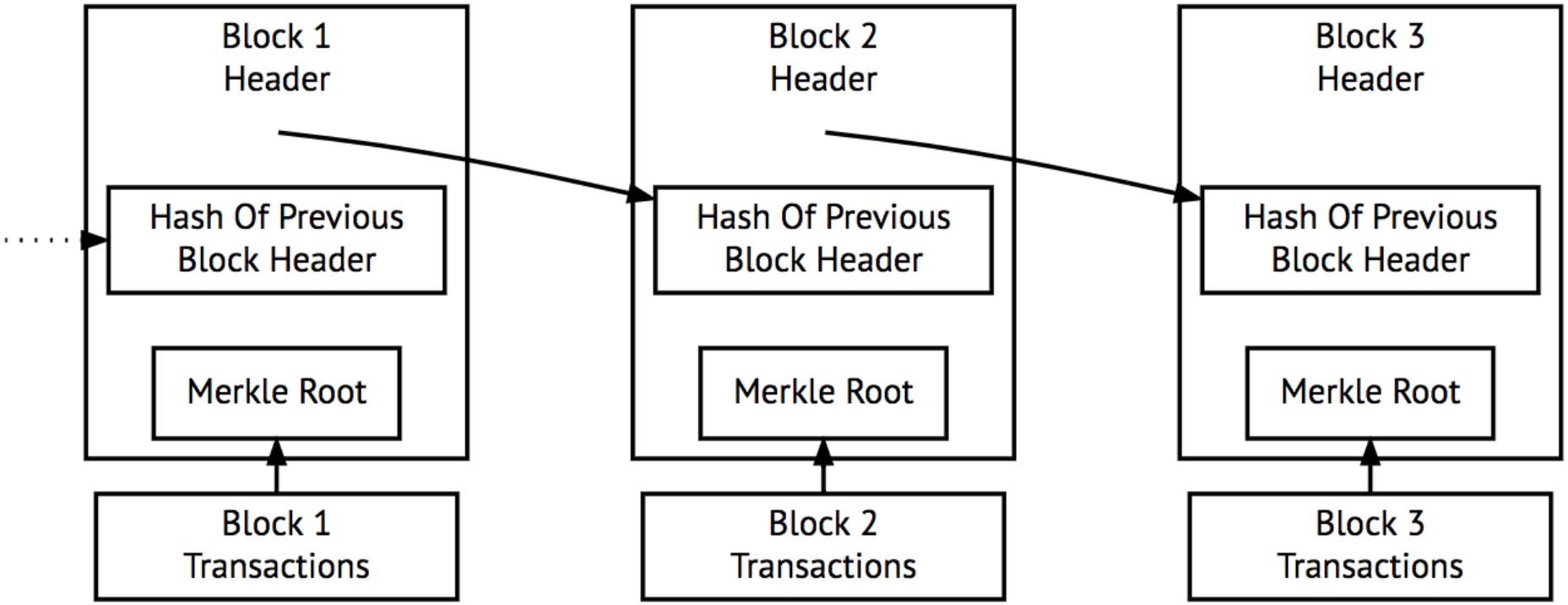
Private

CONSENSUS LEVEL 1

Permissioned database (privacy)

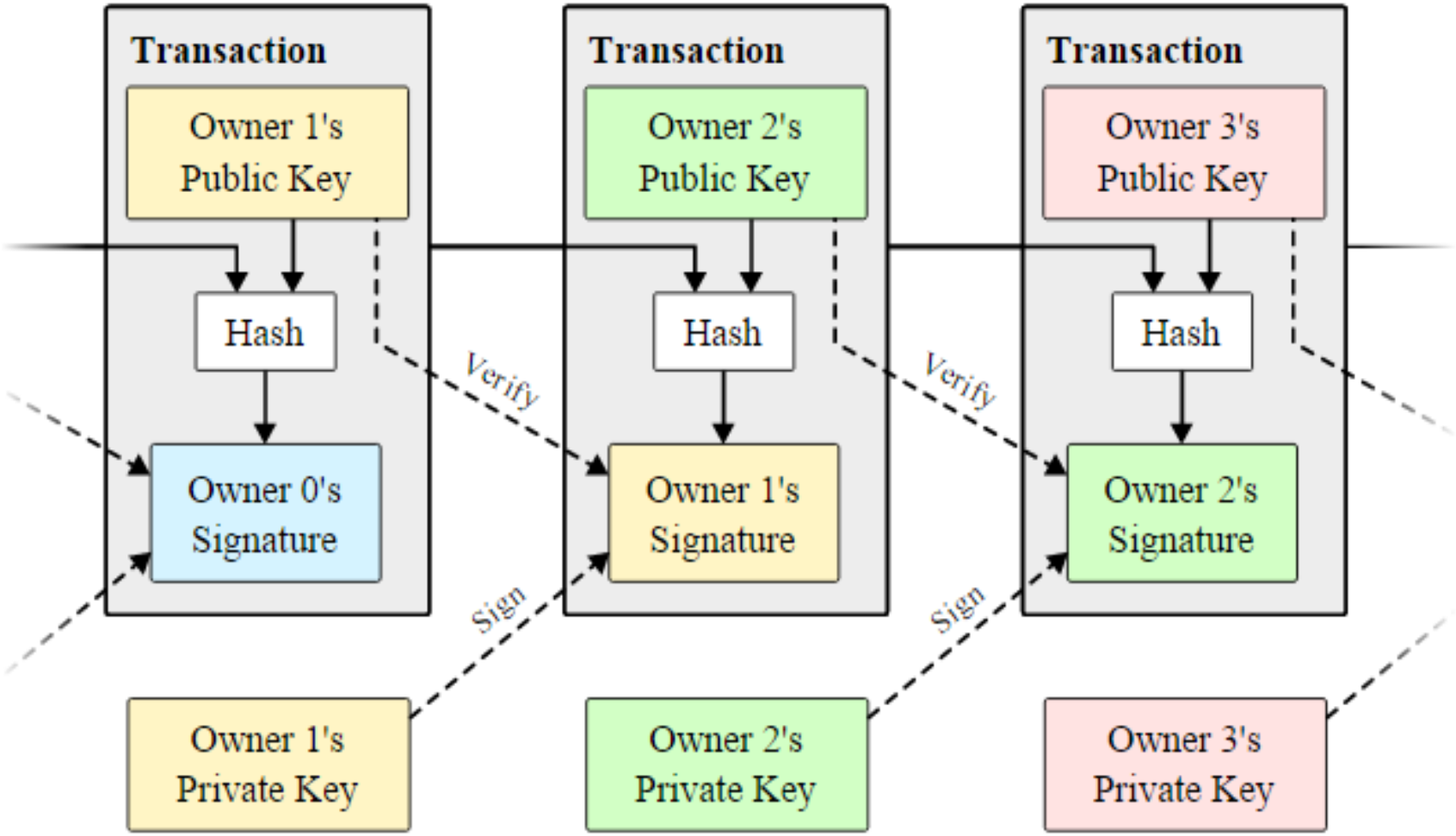
Best for: internal information

Simplified Block Chain

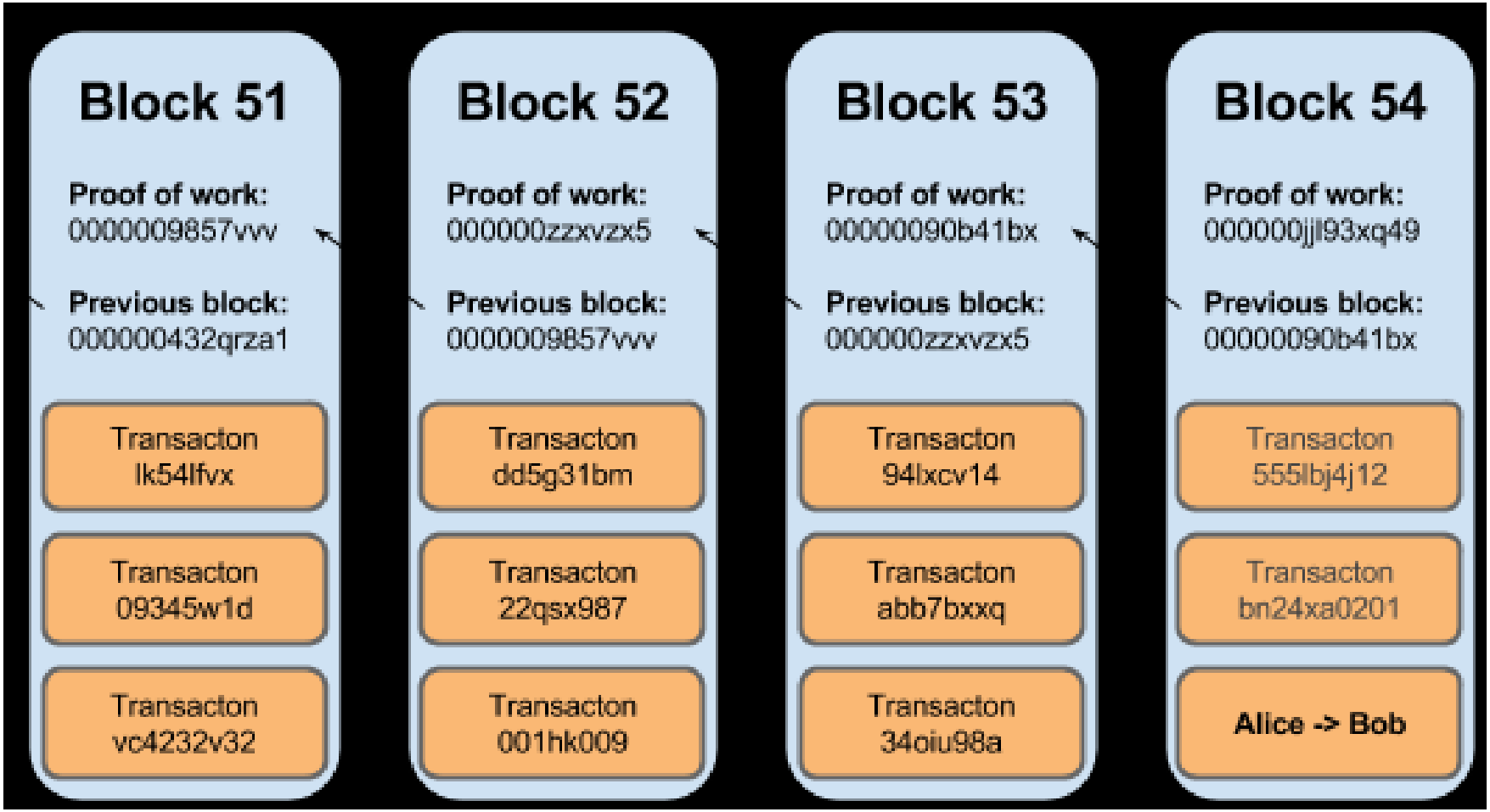


Simplified Bitcoin Block Chain

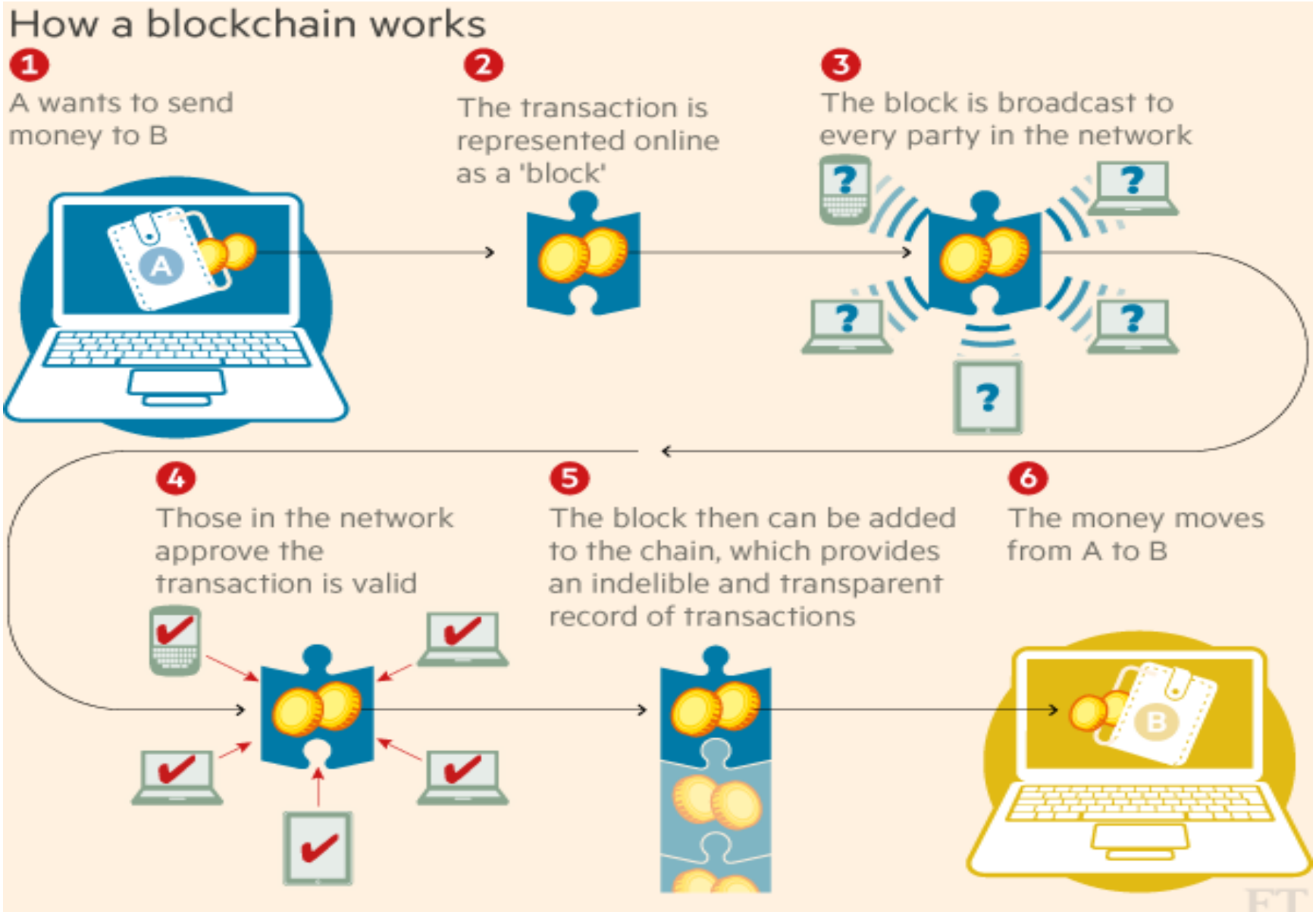
Blockchain Transactions



The Chain of Blocks



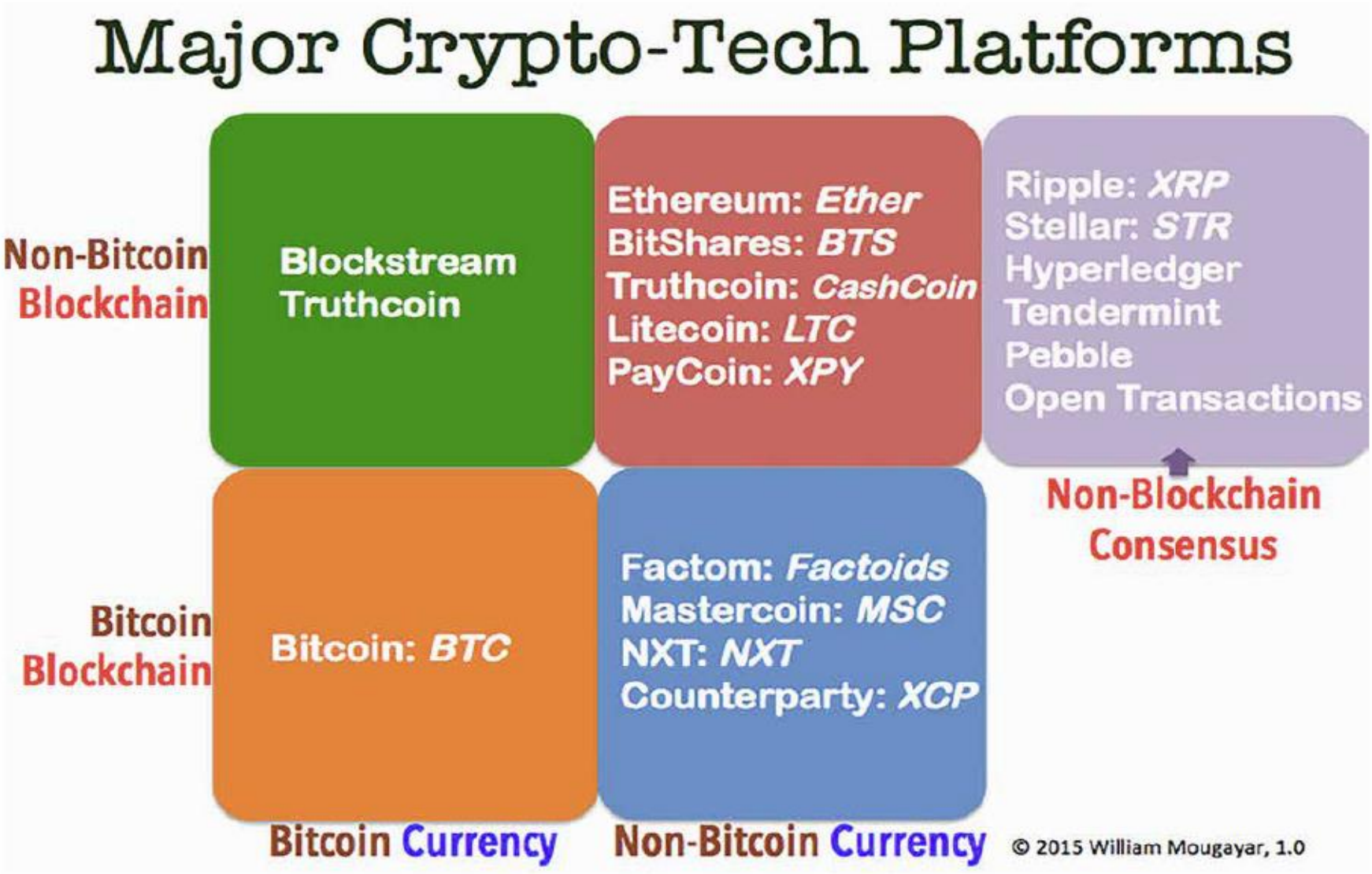
How Blockchain Works



Blockchain scalability problems

- Records (known as blocks) in the bitcoin blockchain are limited in size and frequency.
- The transaction processing capacity of the bitcoin network is limited by the average block creation time of 10 minutes and the block size limit (1 Megabyte).
- These jointly constrain the network's throughput. The transaction processing capacity maximum is estimated between 3.3 and 7 transactions per second.
- Typically takes ~10 minutes to validate a given transaction.
- Transaction fees do not facilitate micro-transactions (like IoT logs, etc.)
- There are various proposed and activated solutions to address these issues. (evolving so swiftly that they are hard to evaluate…)

Distributed Ledger Platforms



IOT-specific “Blockchains” which are really Blockchain-Free Cryptocurrencies (Ledgers)

- Openchain (more centralized?)
- Directed Acyclic Graphs (DAG)
  - Dagcoin
  - Byteball
  - **IOTA** (MIOTA)
  - IoT Chain (IOT)
  - Internet Node Token (INT)
  - IoT Coin (XoT)

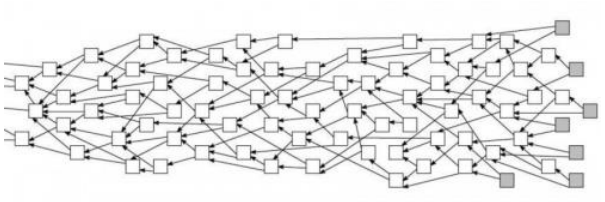
- Combinations of Blockchain and non-blockchain
  - TumbleBit

- Too little known to classify yet:
- IoT Chain (IOT)
- IoT Coin [traded as both a Monetary Unit (XoT) and as an Asset (IoT)].
- Helium (uses “proof of coverage” and “proof of serialization” for locations in a wireless network)

Basically, a blockchain-free cryptocurrency is any distributed database that uses different tools to achieve essentially the same objectives as a blockchain.

IOTA : an attempt to scale a DLT for the IoT

- Uses a “Tangle” (Directed Acyclic Graph [DAG], not a blockchain
  - Designed to scale for use by IOT devices
  - No transaction fees
  - Light “Proof of Work”
  - No mining



- IOTA: Implementation
  - Light Wallets Connect to full nodes
  - Full Wallets Also known as full nodes
  - Uses a “Coordinator” to prevent malicious control until network grows large (Arguably not decentralized)
  - Purports to be “Quantum Safe”
  - No transaction fees (requires validation of two other transactions)
- Currently hard to use
  - documentation rapidly evolving
  - security hard to evaluate
- Growing community
- Does have potential for fast, lightweight transactions needed in the IoT

This presentation will touch on:

- Background
- IoT (Definition)
  - Security Policy (no clear policy, no security)
- **Policy Enforcement Technologies**
  1. Blockchain-based Distributed Trusted Ledgers (DTL) to log IoT events
  2. **Physical Unclonable Functions (PUFs)**
- Summary/Conclusion

All of today's electronic authentication uses Secrets

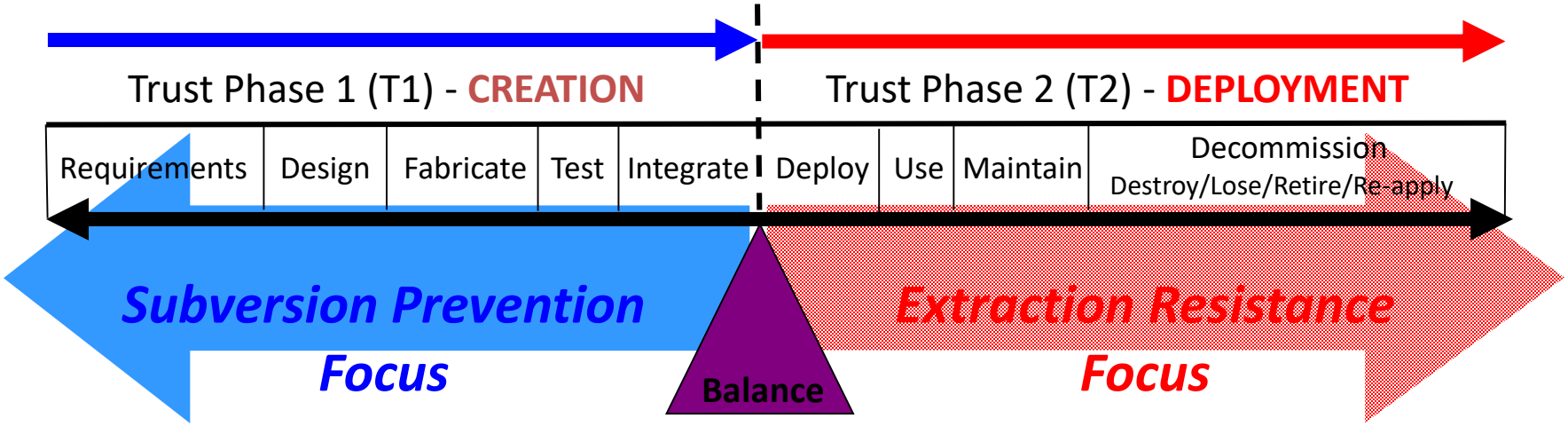
- In contrast with human-culture-based authentication schemes such as human recognition of voice or face associated with a message, all electronic message authentication schemes in use today require protection of a small secret against extraction by an adversary over some portion of the life cycle.

Adversary may choose to spoof or bypass Authentication by any of the 3 attack categories (Myers, 1980):

- Inadvertent Disclosure
  - Phishing, spear phishing, dumpster diving, shoulder surfing, etc.
    - To obtain the small secrets with which to spoof the authentication of commands
- Penetration
  - Exploit vulnerabilities in control mechanism to
    - Obtain the small secrets with which to spoof the authentication of commands
    - Bypass the authentication and falsely trigger the access control decision mechanism (open/close the switch without proper authentication)
- Subversion
  - Insert mechanism to exfiltrate the small secrets with which to spoof the authentication of commands
  - Insert mechanism to bypass the authentication and falsely operate the authorization mechanism (close the switch without proper authentication)
  - Trigger the mechanism at a later time of the adversary's choosing

Hardware/Software System Life Cycle
for High Exposure Systems

- The nation state adversary is uniquely capable of subversion in the creation portion of the life cycle and extraction in the deployment portion of the life cycle
  - Insert “intentional vulnerability” in **Creation** portion of lifecycle, use it later. (Subversion)
  - Use either “intentional vulnerability” or “inadvertent vulnerability” in **Deployment** portion of lifecycle to extract authentication secrets. (Extraction)



Simplified Threat Model for High Exposure Systems

Spoofing Cryptographic Authentication

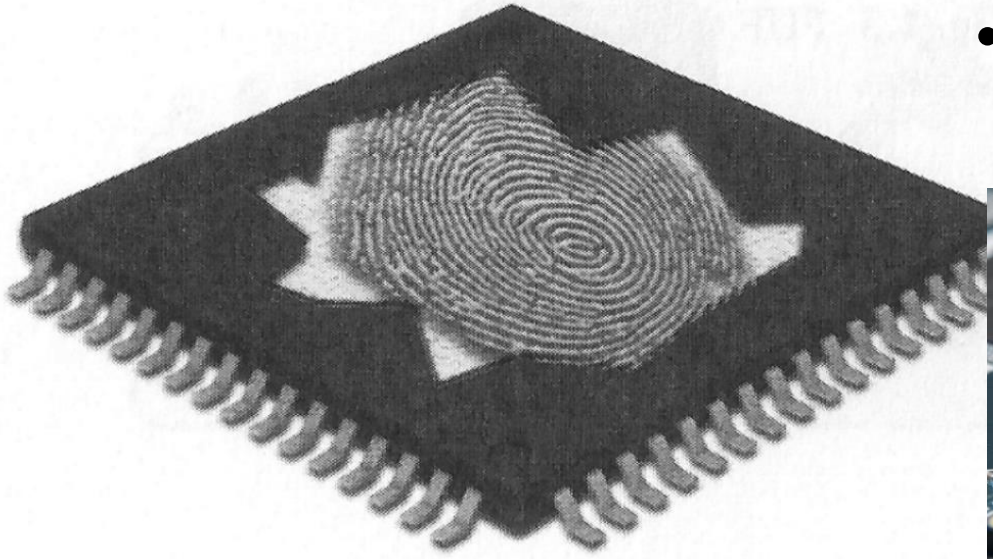
- Software: easy to reverse engineer secrets with a debugging tool; encrypted secrets just mean you have to find the “key encrypting key” first
- Hardware: only a little harder…

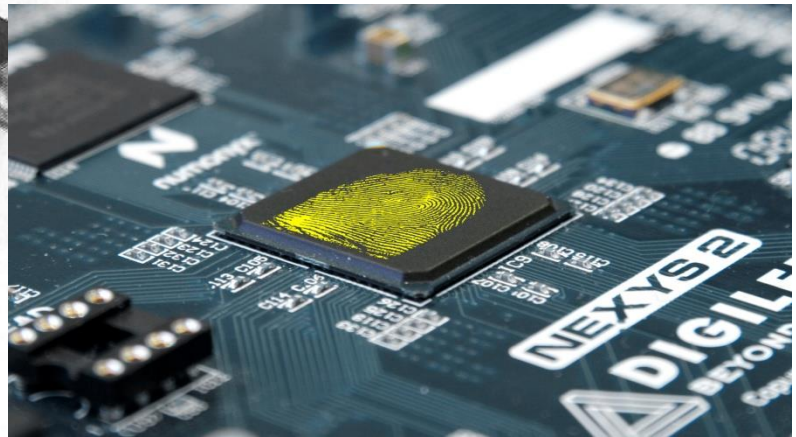
→If you can “reach into a piece of authentication software or hardware and extract the secret key, you can spoof any authentication of message or transaction enabled by that secret!

Physically Unclonable Functions

- PUFs

- A measurement of a physical structure that is easy to evaluate (in hardware) but hard to predict
- Like a “device fingerprint”





Physically Unclonable Functions

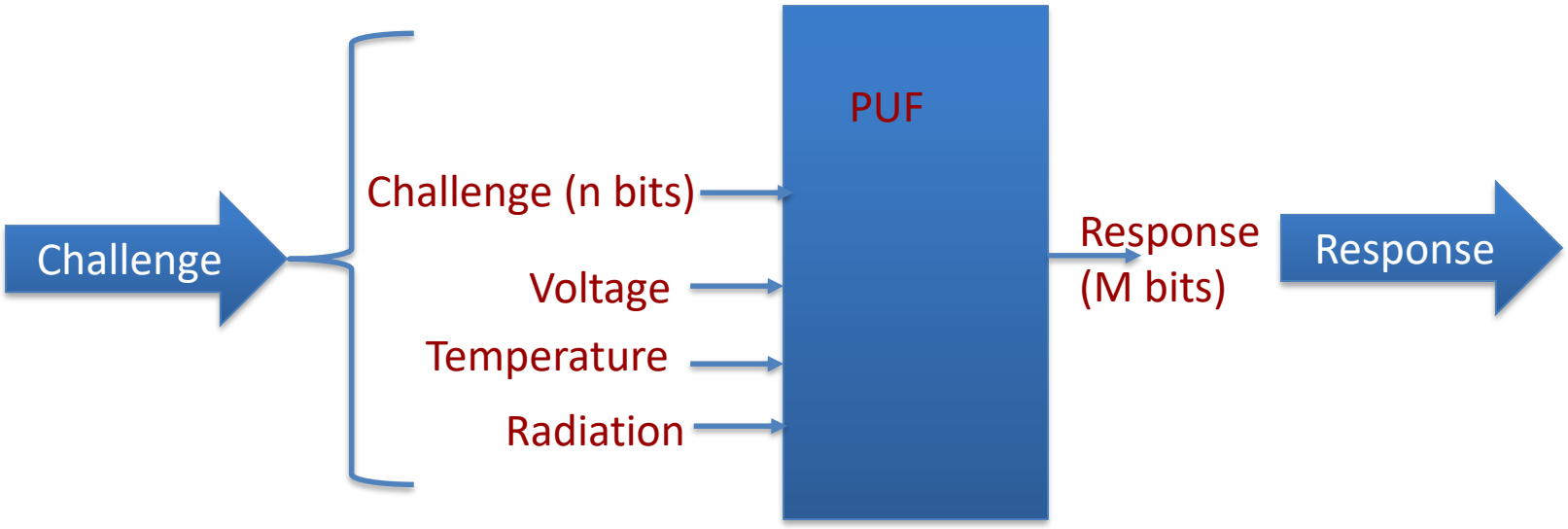
- A measurement of a unique “inherent” property
- Can be used to eliminate the storage of cryptovariables in “non-volatile” hardware memory
- Can be engineered to be altered or destroyed by attempts to extract the “inherent” PUF measurement or even to modify the chip functionality (insert a subversion)
- Thus thwarting many methods of “secret extraction” (except side channel attacks…) and even providing tamper-detection

PUF Uses

- Generate cryptovariables
- IP protection
- Component binding, software & bitstream authentication
- PUFS for random number generation
  - Random Seed
- PUFS for authentication of integrated circuits
  - Device identification & authenticity
  - Tamper evidence/Tamper Detection
  - 2nd Factor Authentication
- Other

PUF Abstraction

- Challenge & environmental inputs, Response Output



  - Weak PUFs, Strong PUFs, Noise Compensation… a lot of engineering goes on here…

Method 1: Variable challenge (Physical Challenge-Response Method) [uses "differencing" technique]

- Yields varying response
  - Challenge-response pairs must be measured and "cataloged" in a database by trusted party during "Enrollment" phase
  - Challenge-response pairs re-measured later in Validation phase
    - Challenge response pairs sent to trusted party
    - **Validation succeeds if responses differ by small Hamming distance (number of differing bit positions)**
- **Subject to "modeling" attacks** (many challenge-response pairs are revealed to the adversary)

Method 2: Constant (random, secret) challenge (Cryptographic Challenge-Response Method)

- Yields "constant" random seed useful in developing cryptovariables
  - Requires "noise compensation" to repeatedly generate the same cryptovariable
    - Called "Fuzzy Extraction"
  - Validation succeeds if device can successfully decrypt a random number encrypted with the devices' public key
- **Not Subject to "modeling" attacks**
  (no challenge-response pairs are revealed to the adversary)

Noise Compensation using Error Correcting Codes

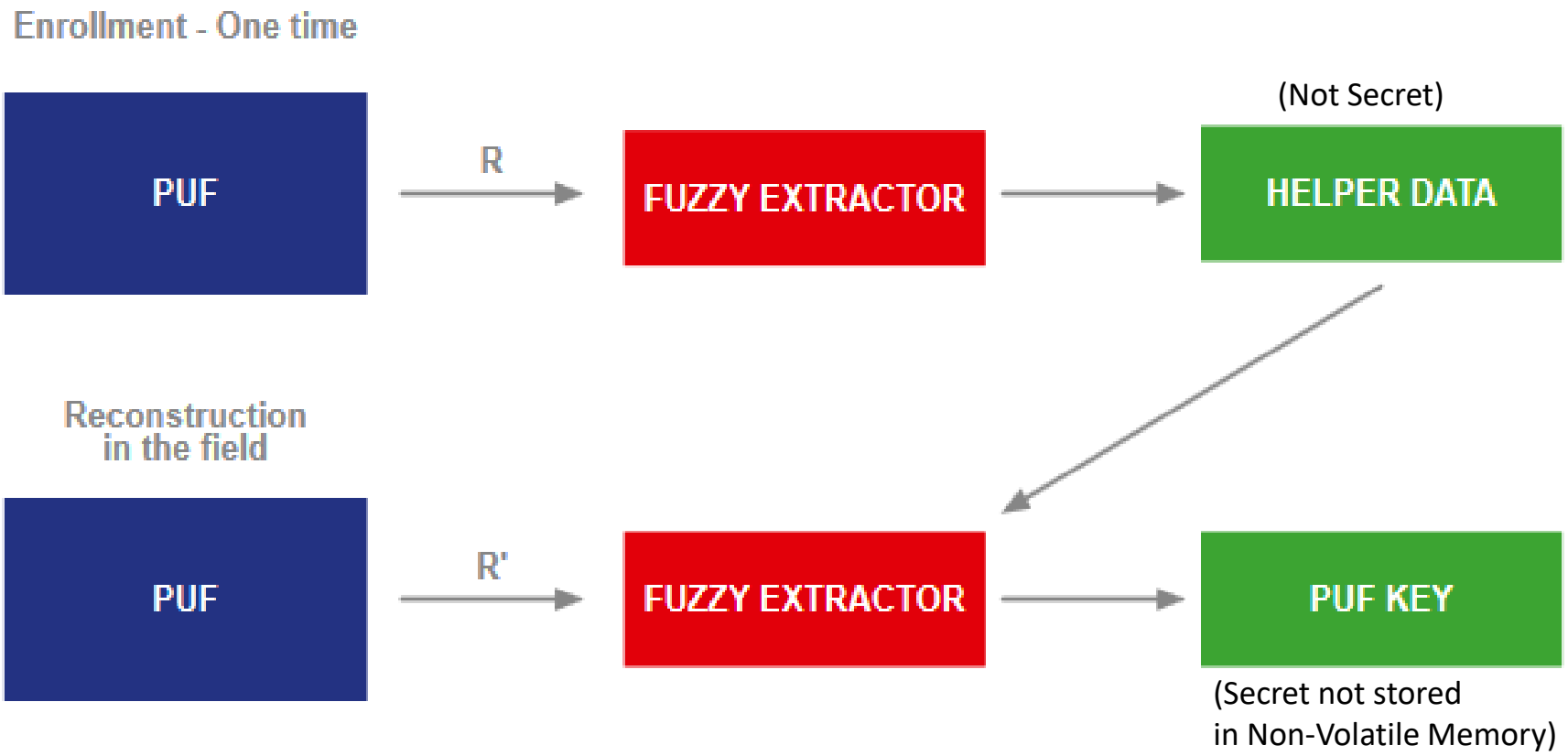


Figure 1: *Enrollment and reconstruction phase for the generation of PUF keys (Note - R is the initial PUF response during enrollment and ' is the PUF response in the field with a noise component*

Fuzzy Extraction

- "helper data" is the difference between the PUF re-measurement W' and the randomly chosen error correction codeword

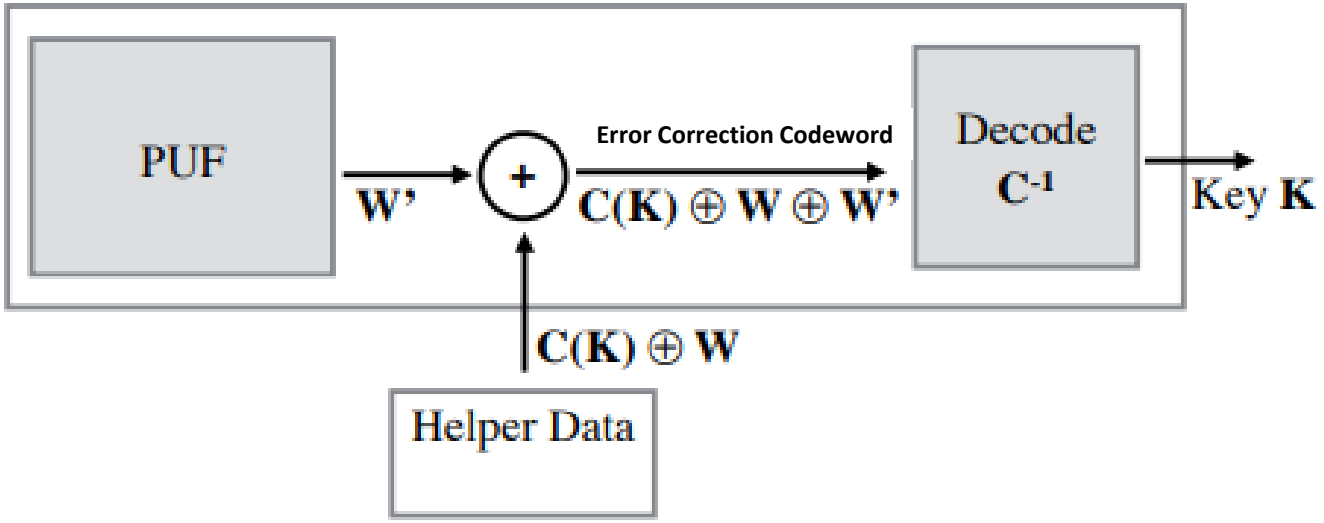


Figure 6.2: PUF-based secret key generation using helper data for error correction. The helper data is generated during a one-time enrollment process and is fixed over the life of the PUF.

Combining these Techniques-

1. PUF measurement within the Integrated Circuit
2. Extract a “share” from the PUF measurement using “fuzzy extraction” (something you have)
3. Biometric Measurement (tamper-protected to differentiate playback)
4. Optionally extract a “share” from a Biometric Measurement using “fuzzy extraction” (something you are)
5. Optionally input a “share” (something you know)
6. Combine these “shares” (up to 3-Factor Authentication) and use the result to “seed” a private key / public key generation process

- Discard the private key (can be regenerated when needed) and output and register the public key with the “public key authentication infrastructure” (so that the private key is never stored in non-volatile storage in the device)
- Repeat steps 1-6 to obtain the private key for signing **Blockchain Transactions**, **decrypting authentication challenges**, etc., then destroy the private key after each use (so that it is not available in the device for “extraction”)

Summary/Conclusions

- IoT security must be discussed in terms of policy enforcement
  - Enforcement mechanisms for specific “Mandatory Policy” embedded in hardware can be extremely effective
- New technologies for policy enforcement include:
  - Distributed Trusted Ledgers (DTL) like Blockchain, Iotachain, etc.
    - For protection of IoT logs, parameters, etc.
    - Can assure integrity of log but not the “logger”
    - Emerging solutions to the “scalability” problems
  - Physically Unclonable Functions
    - For tamper detection in devices
    - For positive identification of devices (the “logger” in the log)
  - The combination of DTL and PUFs will enable new robust policy enforcement in the IoT (PUFs for authentication; DTL for authorization & audit)
- These concepts are mature but the tools are still evolving - Watch for new developments in PUF tools and Blockchain tools and the combination thereof for application to the IoT.

END

- Questions?