

guardtime 

***Improving Cyber Forensics
& Cybersecurity through
Block Chain Technology
with Truth Based Systems***

International Symposium on
Forensic Science Error
Management

Ken Zatyko
July 23, 2015



Introductions



Experience:

National federal labs and cyber center design expertise

- 28 Years experience in cyber crime, fraud investigations, counterterrorism and consulting Fortune 100 companies and US Government (former USAF Lt Colonel and Special Agent)
- Led world's largest accredited digital forensics lab (DCFL), co-chair FBI Regional Computer Forensics Lab, US Secret Service national lab consultant

Education and certifications

- Master of Science in Crime In Commerce – George Washington University (AF scholarship)
- Master of Arts Military Operational Art and Science – Air Command & Staff College (AF scholarship)
- Dual Bachelor of Science degrees Computer Information Science & Business Administration
- Certified Cyber Forensics Professional and Distinguished Panelist
- Certified Information Systems Security Professional and Exam Developer

Data Breaches on the rise and many evidence systems are connected to the Internet. How do we ensure integrity?



Recent trusted insider threats to evidence in the news

January 13, 2015: Missing police evidence includes thousands in cash, Providence, RI. A search warrant affidavit from a missing evidence investigation reveals that a shade under \$12,000 in cash and two diamond rings are unaccounted for, and a now-suspended police officer was the one who logged the evidence into a storage locker.

March 13, 2015: Cash missing from Springfield police evidence room *Investigation launched last month when cash could not be located*

February 11, 2015: District Attorney launches investigation into evidence missing from Upper Darby police station. One of two people responsible for the evidence room discovered that an envelope, which contained drugs and cash, was missing

May 15, 2015: Evidence Missing from Sheriff's Office. To get inside the evidence room, those with authorization to enter are equipped with a key fob to activate the door. Then they must submit a fingerprint with their right index finger to open the door. "It's all electronic and magnetic," Fisher said. Cameras, operating on a 90-day loop, continuously record inside and outside of the evidence room. Augusta County. Explanation given, \$4000 fell in trash can.

Digital Forensics

This scientific process contains the following eight steps:

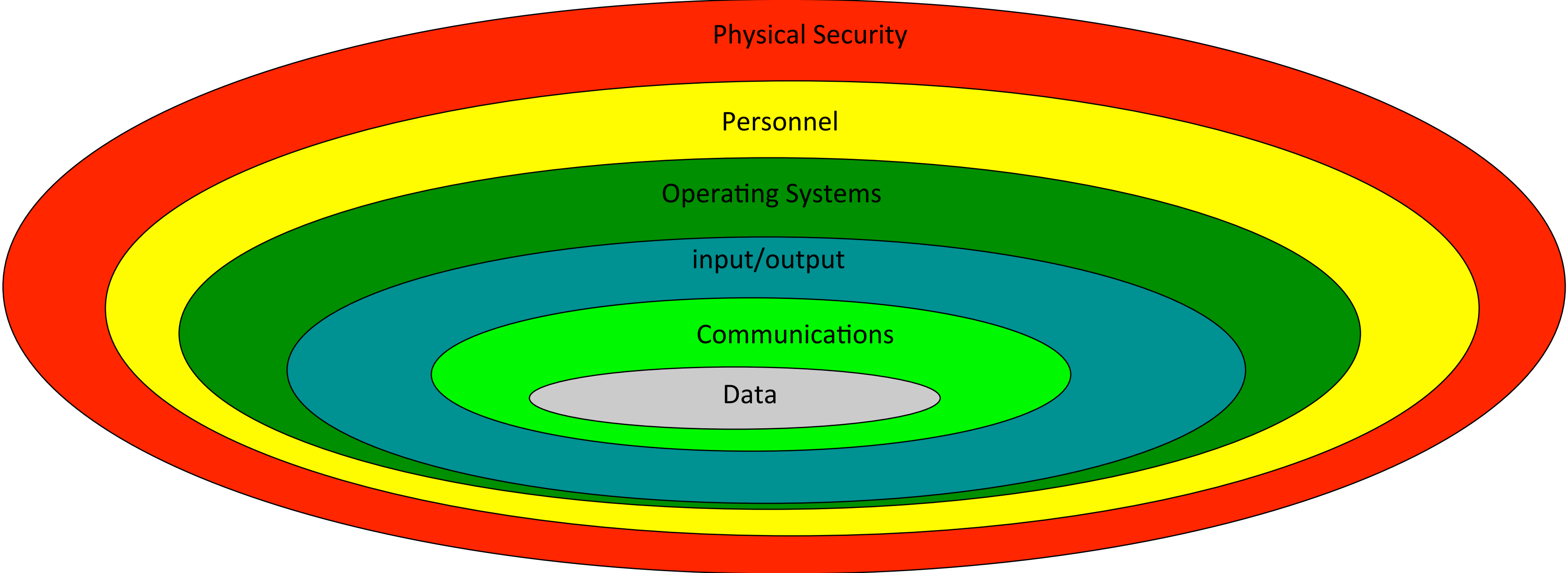
1. Search authority
2. Chain of custody
3. **Imaging/hashing function**
4. Validated tools
5. Analysis
6. Repeatability
7. Reporting
8. Possible expert presentation

“Why data centric security? It is unique and ideal for forensics readiness! It performs hash validation with a block chain and timestamp. It also ensures a forensics workstation’s clean state integrity and repeatability preventing contamination and inaccurate results with unique information on location, who had access, and when.”

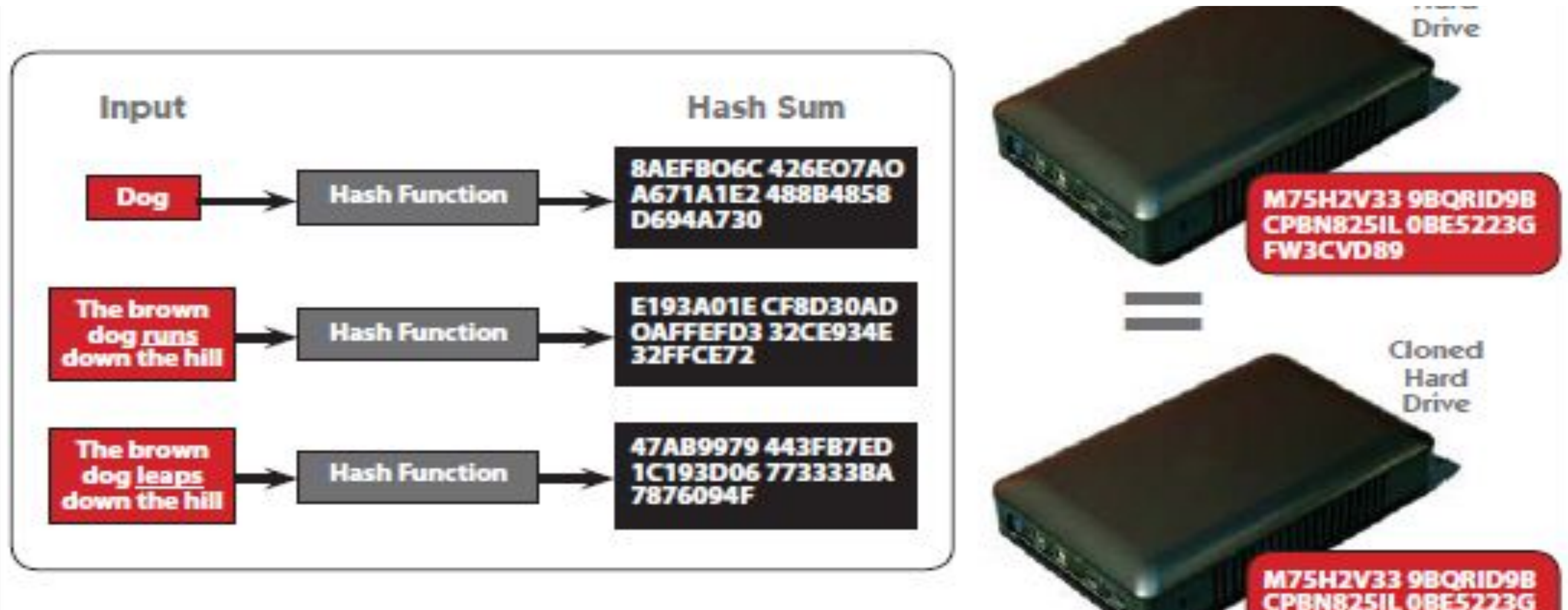
(Source: Zatyko, Forensic Magazine)

Seven Rings of Threat

Good Operating Practices and an Adequate Budget



The digital forensics imaging process. Work with the duplicate and not the original, validate with a “hash.”




KSI is Based on Cryptographic Hash Functions

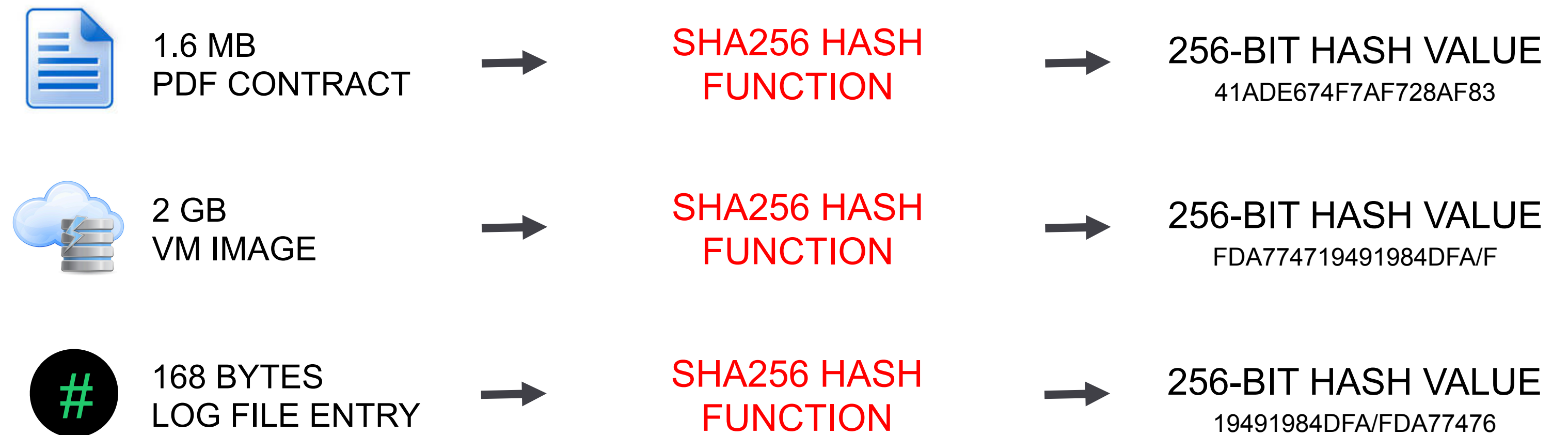
A hash function takes arbitrarily-sized data as input and generates a unique fixed-size bit sequence as output.

The output is known as the hash value, message digest, or digital fingerprint of the input.

A hash value is often used as representative of the input data.



 ONE-WAY ONLY.
REVERSING IMPOSSIBLE



Chain of Custody: Where is the continuous integrity check for this file?

CHAIN OF CUSTODY WORKSHEET				
Subject		Case Number		Date __/__/__
Date and Time Property Recovered Date __/__/__ Time _____		Location Property Recovered		
Description of Property			To Be Processed	
Item #1			Yes	No
Item #2				
Item #3				
Item #4				
RECORD OF PROPERTY TRANSFER				
Date	Time	Recovered By:	Received By:	Purpose of Transfer:

Value proposition

Harnessing industrial data centric security block chain
to support forensics activities bringing clear chain of custody on an examiner's interaction with
the victim and/or any data or images/objects

Forensics services

- Traditionally, after the fact investigations upon alert of an incident
- Moving toward proactive approach or cyber crime diagnostics others call it “hunting.”
- New issue is the cloud as the crime scene
- New need: Cloud computing as a platform for forensics

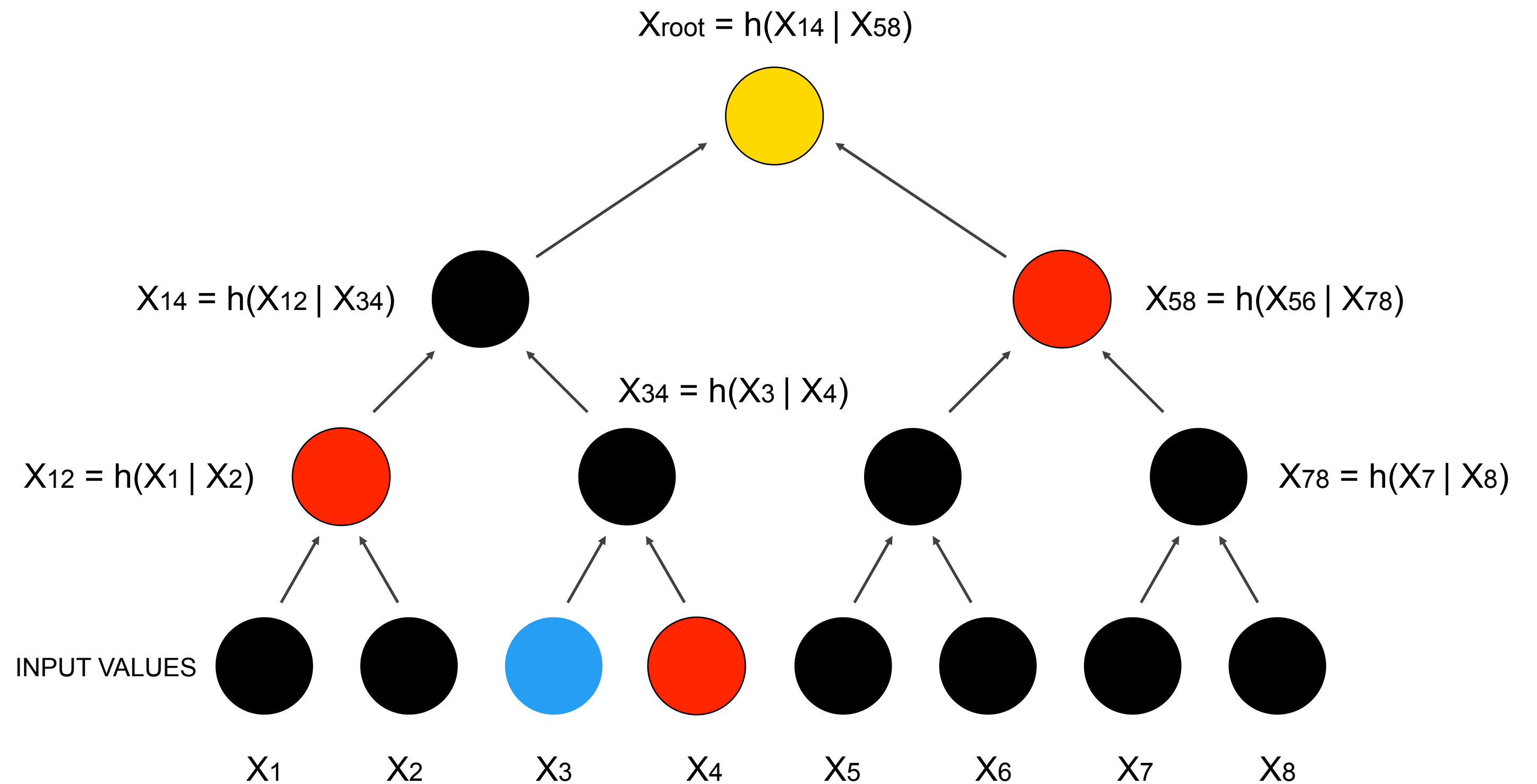
Key discriminators for Data Centric Security: security, contamination prevention, and integrity safeguards

- Keyless Security Infrastructure (KSI) used to ensure validation of virtual machine gold copy operating system and forensics toolkit
- KSI used to ensure forensic workstation calibration
- KSI used to ensure no change to client data during exam process
- KSI used for chain of custody integrity
- KSI used to ensure lab workstation reset for next case

Turning Individual Hash Values into Hash Trees

A hash tree takes hash values as inputs and, via repeated hash function application, aggregates them into a single root hash value.

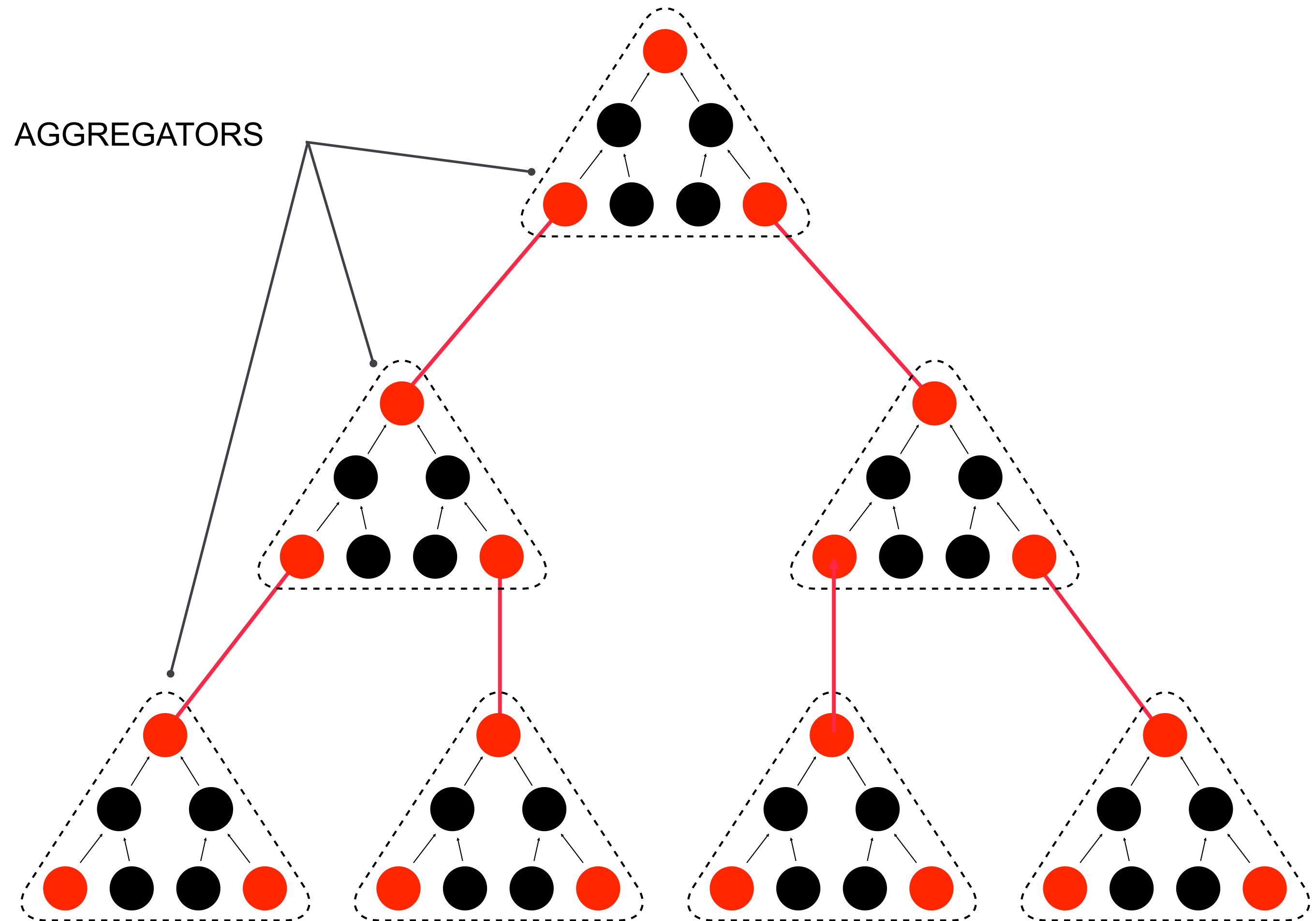
The construct can be viewed as a special kind of hash function, and it has some very useful properties.



Geographically Distributed Hash Trees

A distributed hash tree is built by a hierarchy of geographically separate computational units called aggregators.

Each aggregator operates asynchronously. It receives hash values from its children, generates its own hash tree, then sends its root hash value to multiple parents. This root hash value becomes a leaf at each connected parent.



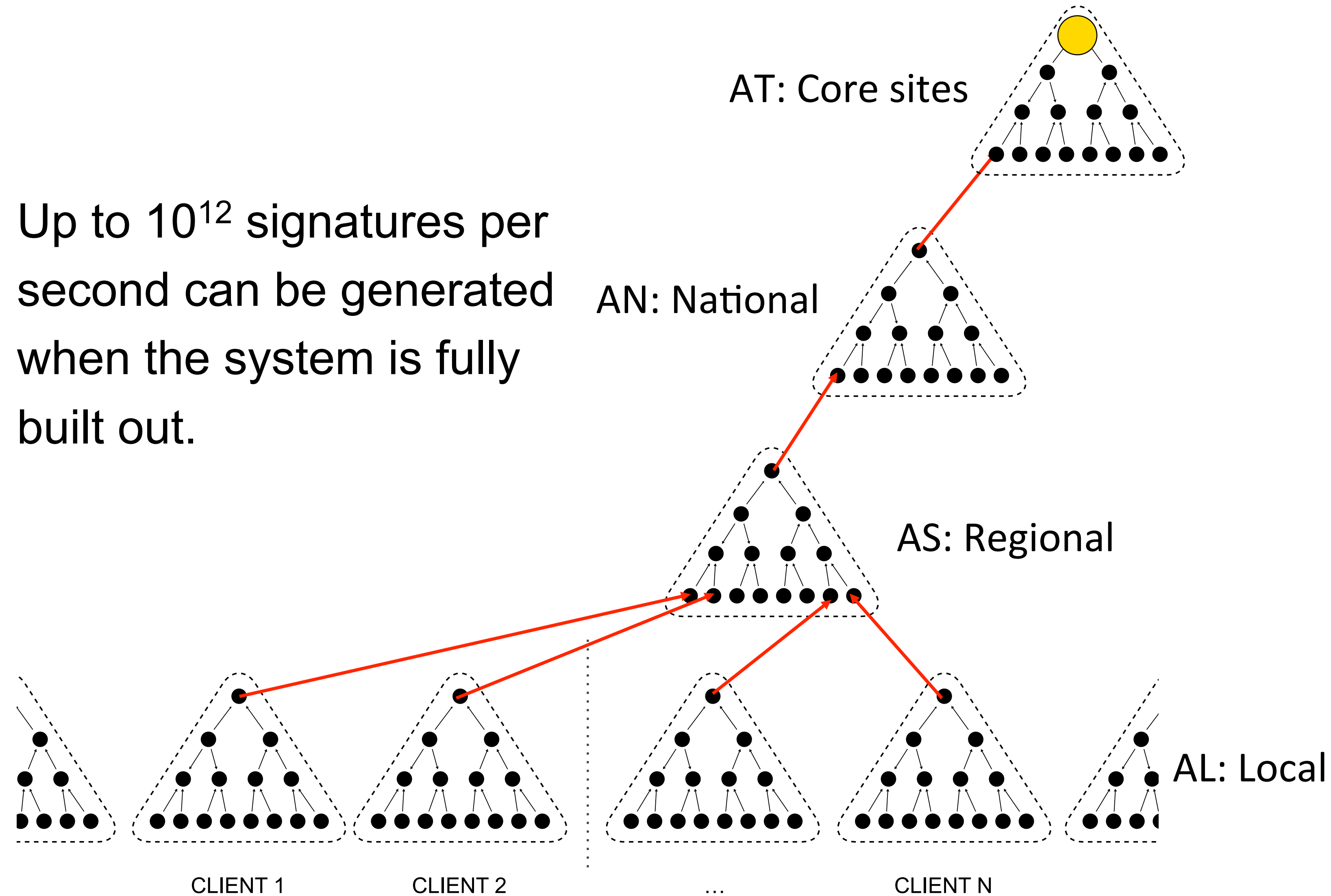
KSI Scalability

Each parent aggregator can support up to 1000 children.

This gives capacity of 10^{3n} signatures per round where n is the number of aggregation layers.

KSI currently contains four aggregation layers.

The top-level cluster “beats” once per second i.e. there is one top level root hash value generated each second.



Up to 10^{12} signatures per second can be generated when the system is fully built out.

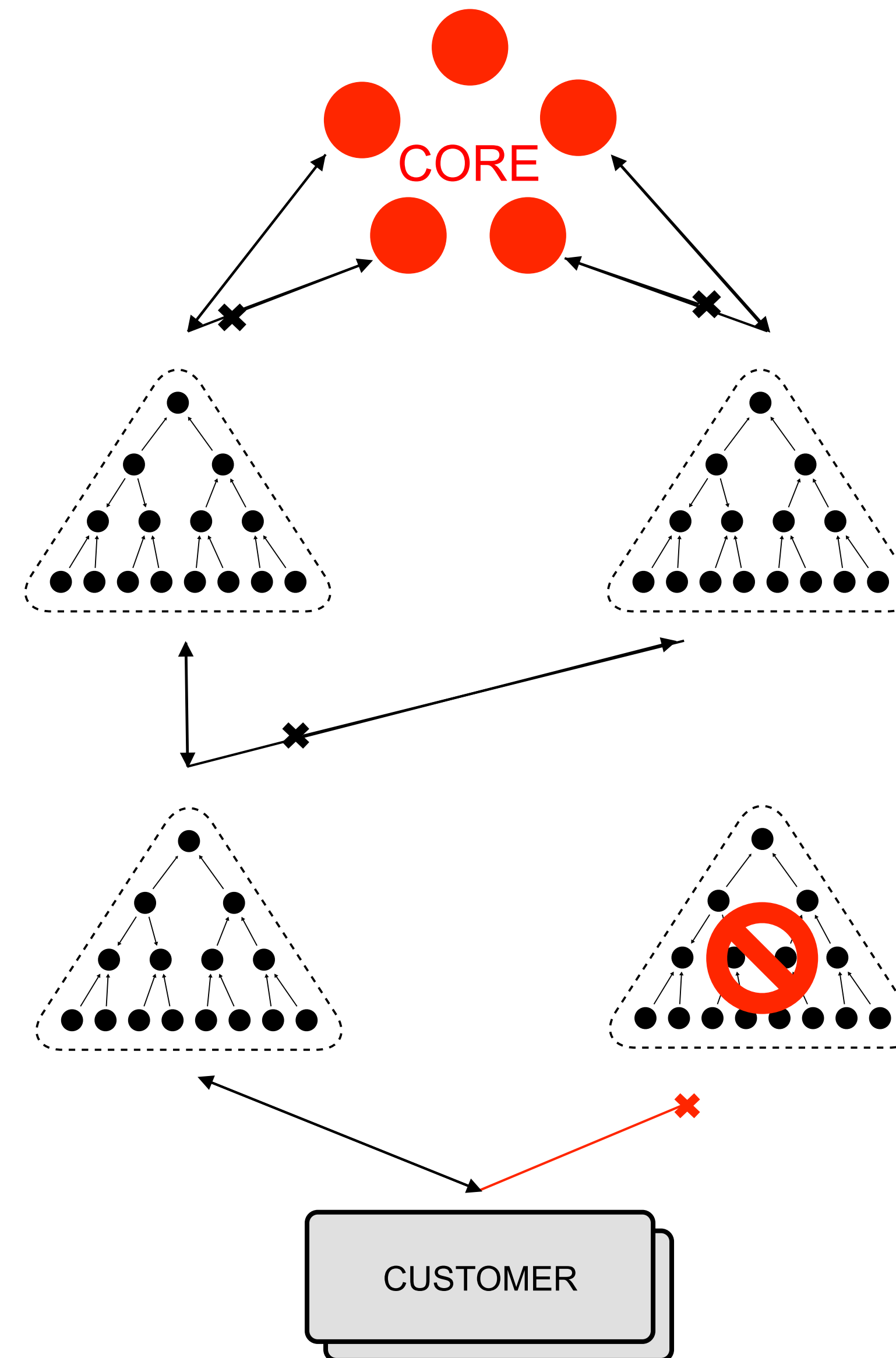
High Availability & Resiliency

Aggregators run in redundant clusters.

Each logical aggregator is implemented as a cluster of fully redundant servers, hosted at independent locations.

Each request is sent to each member of the upstream aggregation cluster. First correct response is accepted.

This ensures there is no single point of failure. Re-routing around network and server failures is transparent, since there are multiple paths from each leaf to the root.

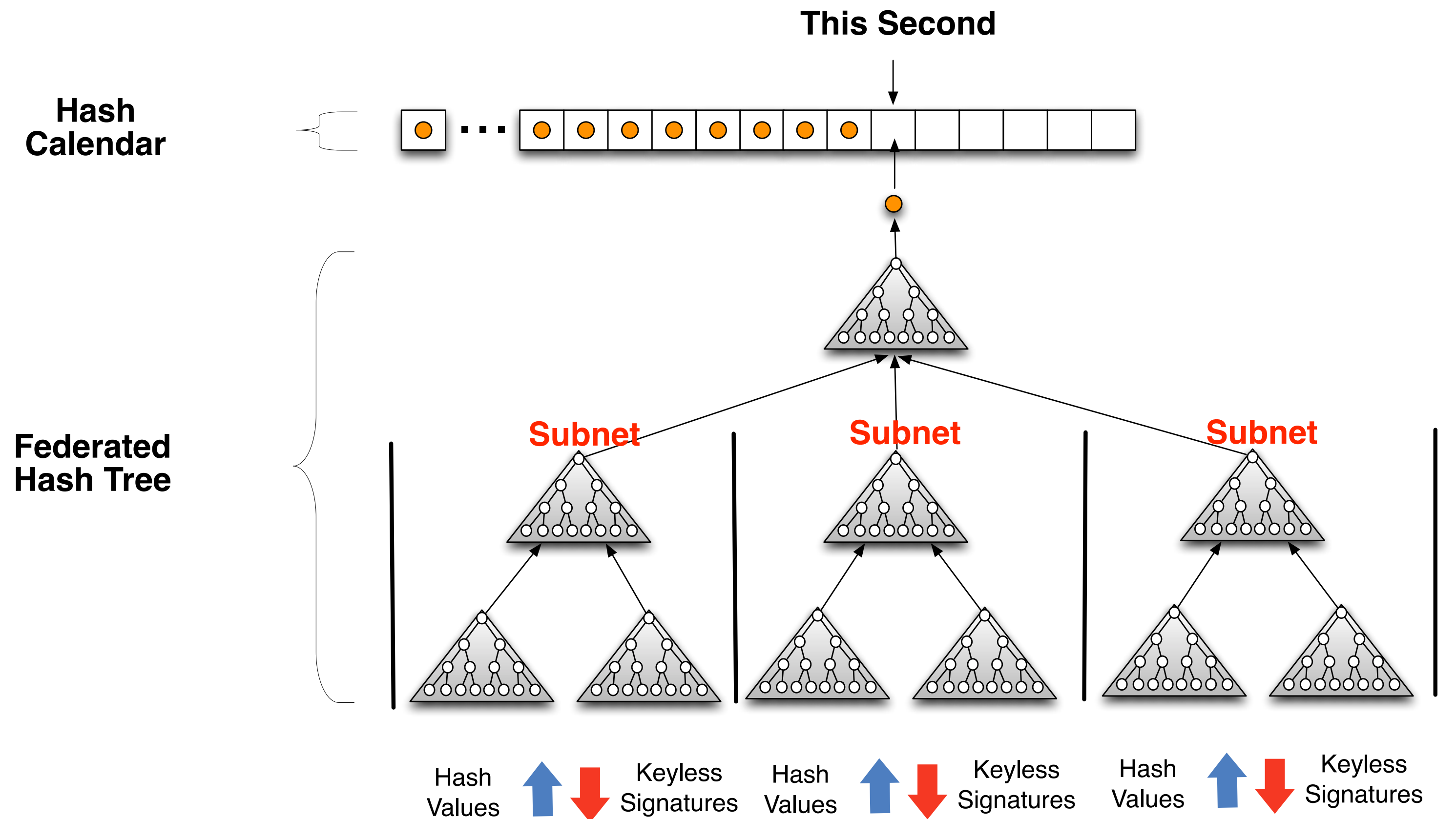


Introducing the Calendar Block Chain

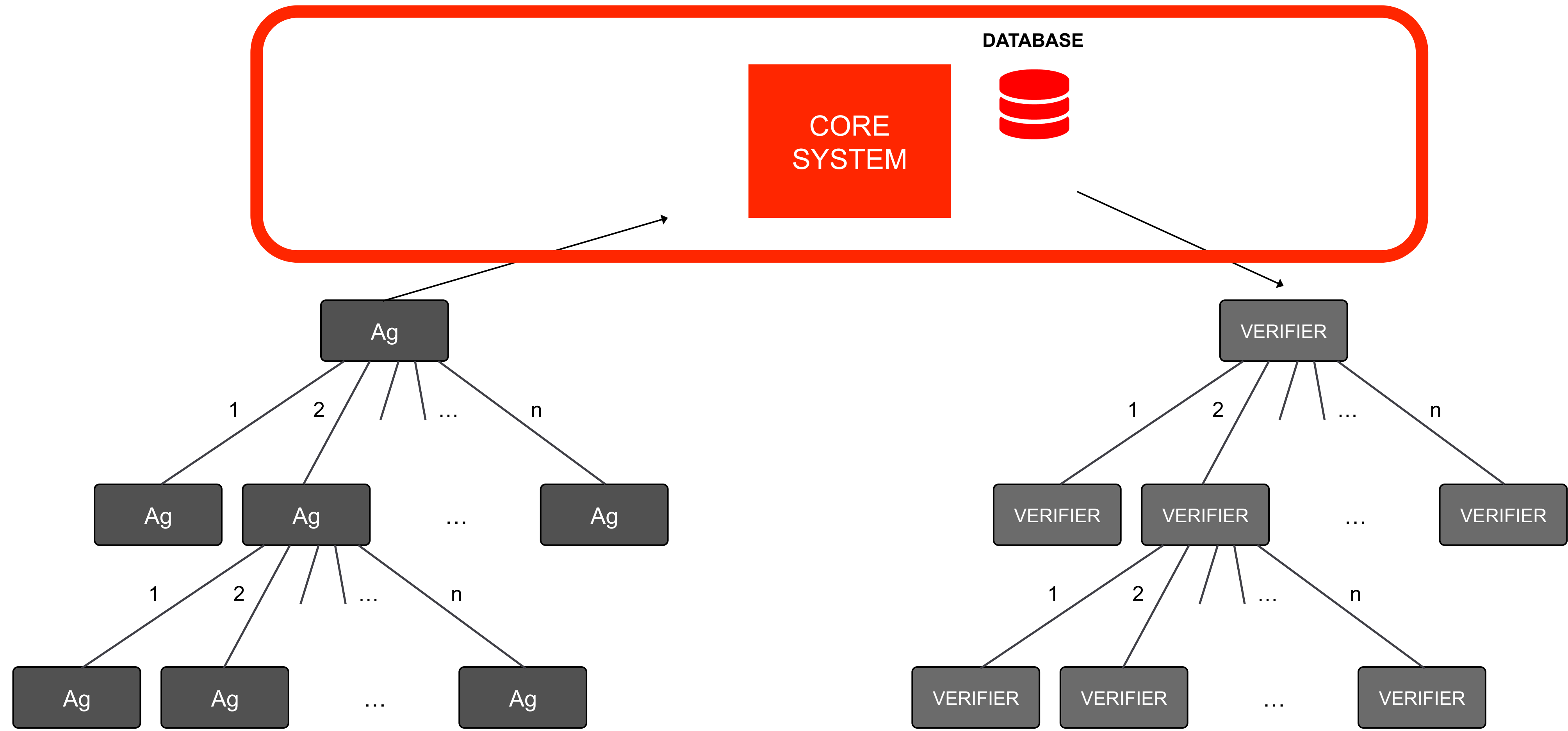
The global aggregation infrastructure operates asynchronously.

Hash values are submitted to the tree and unique hash chains are returned. The same tree is never rebuilt.

Only the root hashes are kept in a public calendar database.



The Core Cluster Keeps the Hash Calendar



Distributed Consensus

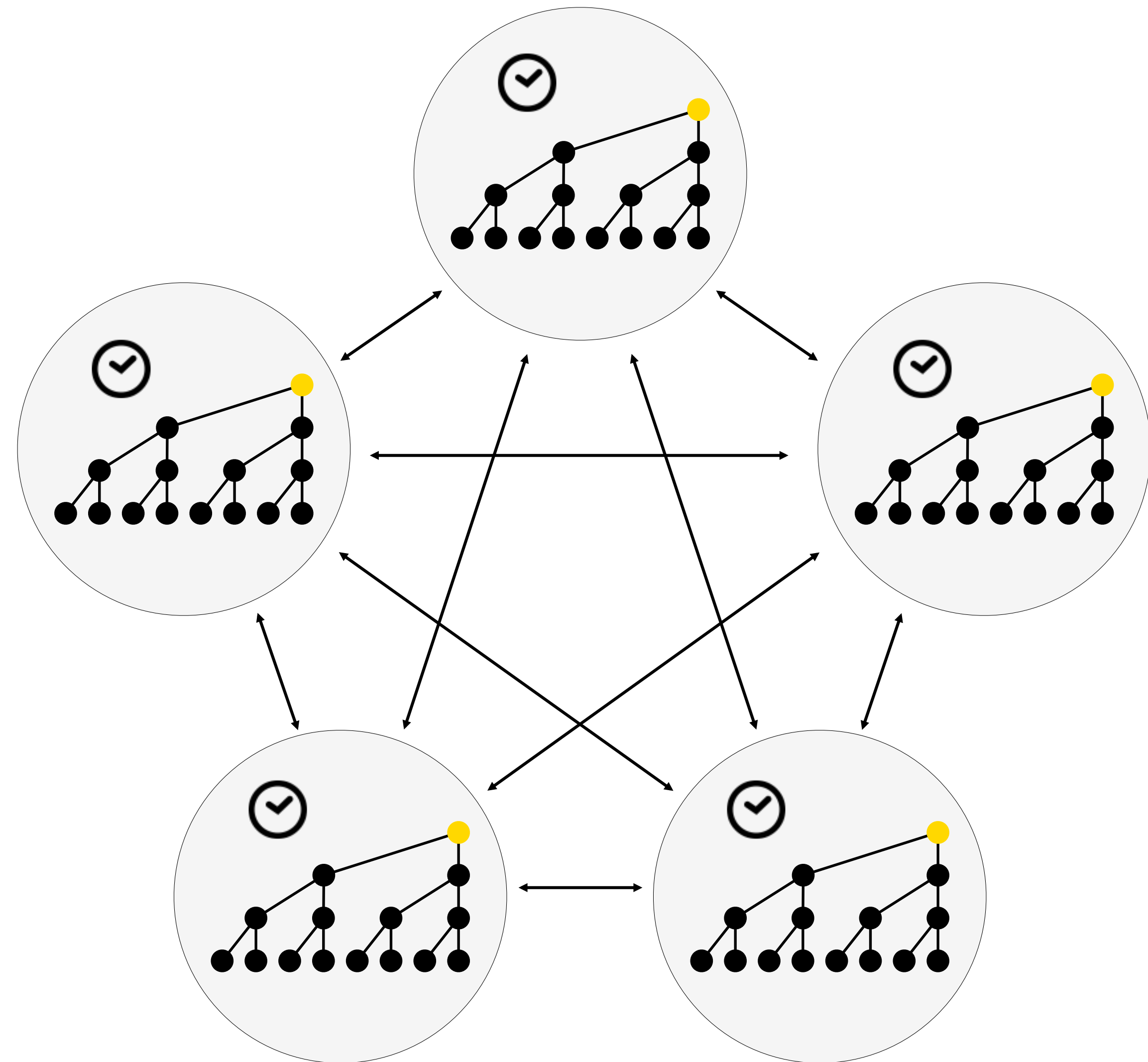
The top of the hash tree would be a single point of failure; therefore we use a cluster of N servers.

Selecting a single hash value from multiple nodes is a variation of the Byzantine Fault Tolerance problem.

We use majority voting to ensure uniqueness of the top. Therefore, $\lfloor N/2 \rfloor$ sites can fail.

Sites run as a synchronized state machine.

Each core node is synchronized to UTC and contains an atomic clock.



Going further – makes forensics native - eliminates costly eDiscovery imaging and hashing

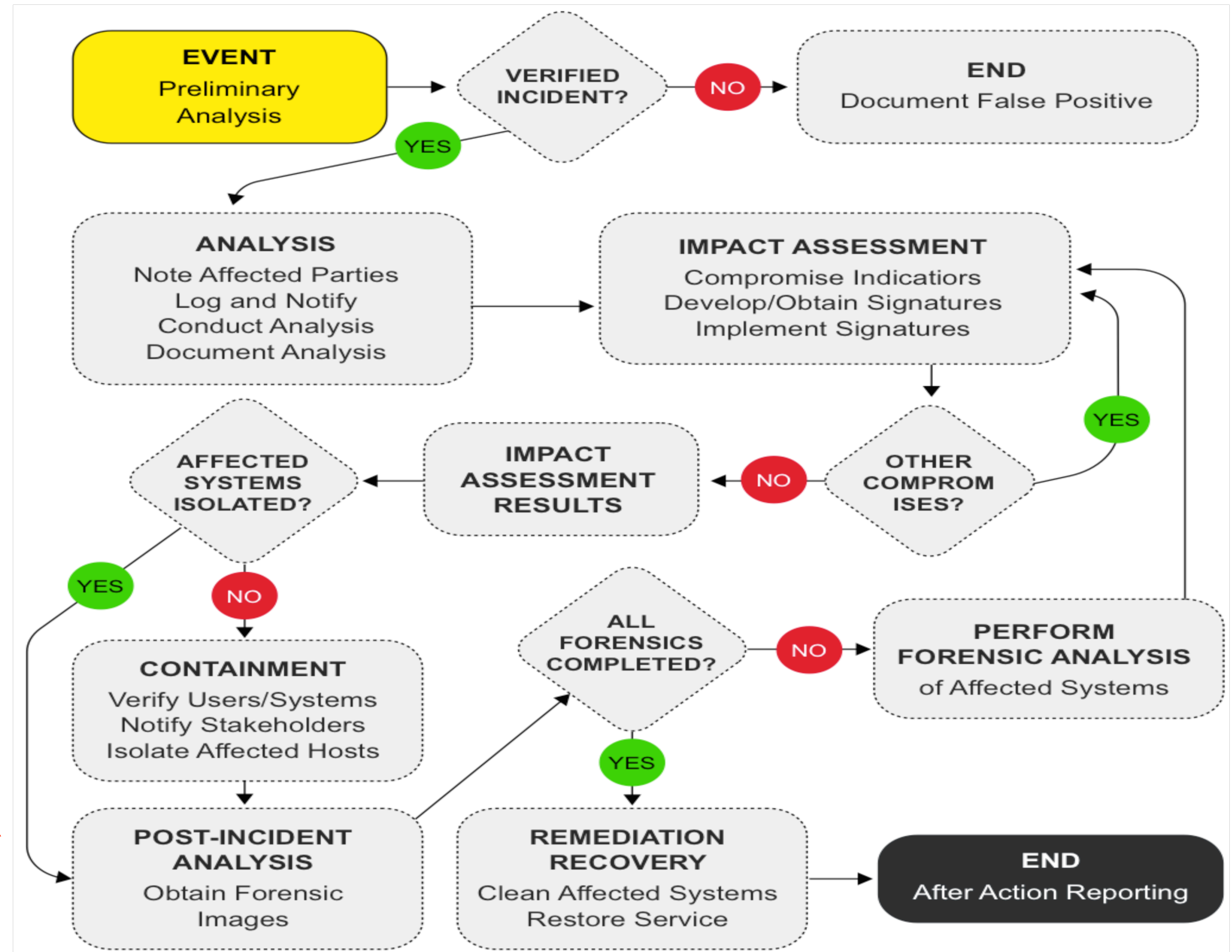
- Provide a “ready” environment for the remote incident response by the forensics technicians and examiners through hash enabled time stamped files, ease of timeline analysis, and secure forensics artifact storage with flawless chain of custody procedures.
- Moreover it provides for remote cyber forensics through cloud forensics increasing the speed of results and overcoming current cloud challenges.

In a KSI enabled environment with signature tokens on each file, one could simply conduct hash set comparisons to find known good, known bad, and unknown or questionable files for further investigation speeding up incident response and investigations. This forensics ready environment is well suited for prompt investigative response and pre-defined data reduction techniques.

Today versus tomorrow: Slow Incident Response versus KSI “Forensics Readiness”

A KSI enabled Cloud environment provides a “forensics ready” environment in which the time consuming task of Forensic hashes exists and forensics imaging is not required.

This saves critical time during incident response for eradication and remediation.



Summary: Improving Cyber Forensics and Cybersecurity through Block Chain Technology with Truth Based Systems

- Cyber threats are dramatically on the rise. Its not just data ex-filtration, but data integrity is a growing concern
- Cyber forensics is maturing
- Hashing is improving with time stamps and block chaining
- Forensics workstations and systems integrity could be improved with block chain technologies
- Evidence control systems could be made forensics ready for improved security and validation

guardtime 

Questions?

Ken.Zatyko@verizon.net

