guardtime

A Global Industrial Blockchain

Guardtime and Keyless Signature Infrastructure

Oct 2015

guardtime

Introducing Guardtime

Who we are:

- Systems engineering company, fundamental and applied research into cryptographic applications
- Founded in 2007 in Tallinn, Estonia
- Offices in Amsterdam, Irvine (California), Washington DC, Tallinn and Tartu
- ~100 people globally, 19 PhD's
- 27 patents granted or pending
- Employee owned company

The Billions of Known Records Compromised Since 2013

(Approximately 33% of human population)

*Source: BreachLevelIndex.com

Technology is experiencing a breakdown of trust

Military systems have become more digitally dependent on a fundamentally insecure and poorly instrumented foundation. Integrity now needs to be the focus. True integrity should not rely on increased use of confidentiality or human trust.


guardtime
Keyless Signature Infrastructure® (KSI®)
is a blockchain technology
for verifying the integrity of data-at-rest
at unprecedented scale.

guardtime

KSI® signature verification based on **formal mathematical methods** only, there are no secrets that can be compromised and conclusive proof of asset integrity is independent of any insiders or third parties.

The massive scale of the KSI® enables signing and verification of **billions of data items** every second.

KSI® is **quantum immune**, meaning it's security is not vulnerable to quantum algorithms run in existing or upcoming quantum computers, unlike i.e. RSA algorithm commonly used in PKI implementations.

The KSI® does not ingest any customer data – instead it is based on one-way cryptographic hash functions that represent the data, but are irreversible such that one cannot start with the hash value and reconstruct the data. Complete data **privacy is guaranteed** at all times.

guardtime

Born in Estonia: The World's Only True Digital Society

- 100% electronic health records
- 99.8% of electronic banking transactions
- 24% of votes via Internet during last election
  Over 1,000 other government e-services accessed using smartcard or mobile ID
- Home of NATO CCDCOE
- Home of European Union IT Agency
- Home of Keyless Signature Infrastructure (KSI)

guardtime

KSI Blockchain Key Advantages

KSI is focused on Data Integrity at Scale.

Our approach solves two major problems present in *every other blockchain*.

Scalability

Other blockchains grow according to the number of transactions they process.

The KSI blockchain grows steadily over time, regardless of the number of transactions.

Commitment time

KSI consensus is achieved synchronously by permissioned nodes.

No Proof-of-Work is used and a new commitment occurs each second.

Billions of individual events can be secured each second.
Minimal storage, compute, and network overhead.

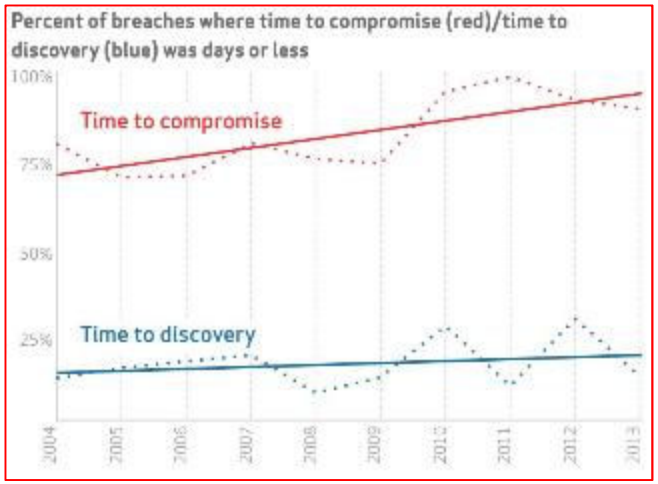
guardtime

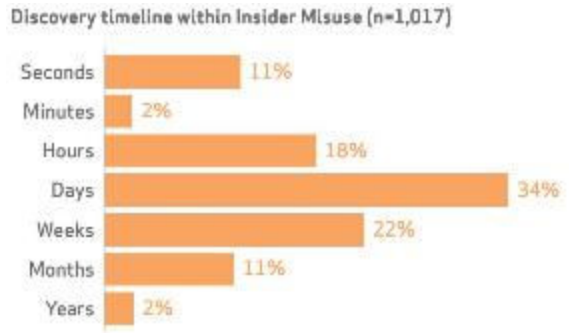
Align time to discovery with time to compromise

Over the last decade:

- Time to compromise has decreased, 90% less than a day
- Time to discovery has remained flat, only 15% found in less than a day
- For insider threat, 69% of compromise detections take more than a day; 35% take weeks or more

Source: 2014 Verizon Data Breach Report



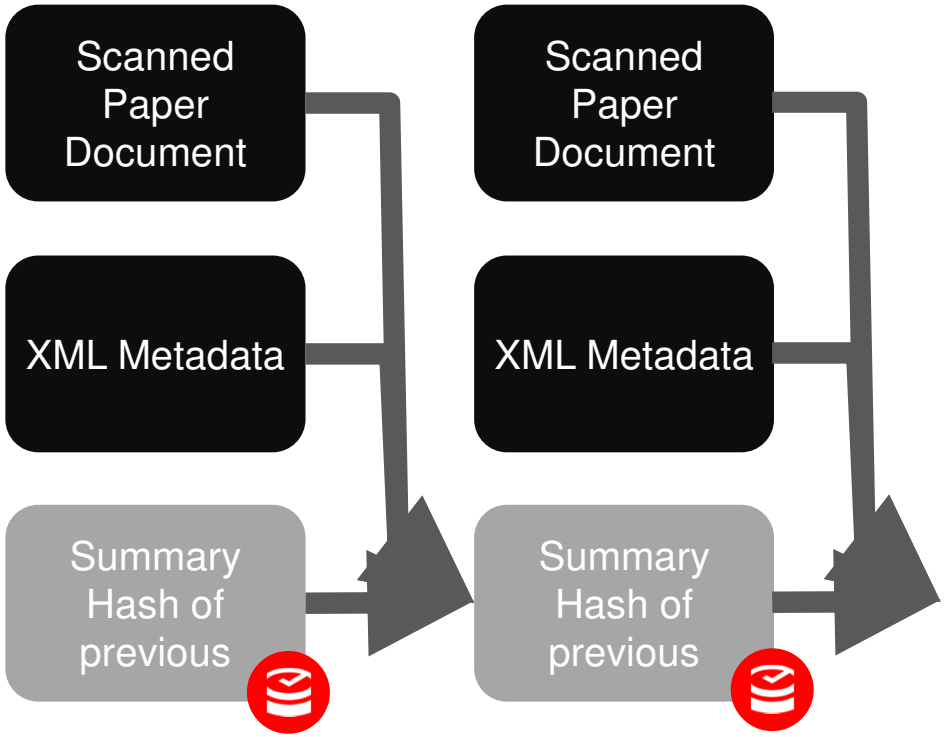


guardtime

Case Study: Estonian Succession Registry

Electronic records and associated metadata are chained to the previous record, signed and stored in a database.

- Provable ordering
- Impossible to delete a record undetectably
- Metadata provides attribution and government transparency
- Monitored and verified in real-time



guardtime

Black Lantern™ – Extending the Power of the Blockchain for Data Protection

Black Lantern Protects Against:

- Advanced Persistent Threats (APT-s)
- Privileged Unlawful Access (Insider Threat)
- Distributed Denial of Service (DDOS)
- Side Channel Attacks
- Introduction of Executable Code
- Boot Code, Service and Operating System Modification
- Physical Access to Hardware
- Low-Level Reverse Engineering
- Cryptanalysis Attacks
- Zero-day Exploits

Black Lantern Hardware Features

- PPC based real-time operating environment with JVM
- Secondary x86 based operating environment, monitored by real-time integrity hooks over the PCIe bus
- Hardware encryption SoC
- Real-time, high-precision networking with multiple 10G fiber and 1G copper interfaces

guardtime

Conclusion

“The blockchain is the most important technology since the Internet itself”

- Marc Andreessen

Guardtime’s KSI is the only industrial-grade blockchain, selected and being validated by the US Government for multiple use-cases. We have a highly experienced team, a validated business model that is scaling to address a 10BN USD annual market and a partner ecosystem that includes the world’s largest defense and telecom vendors.

guardtime

Thank You!

matthew.johnson@guardtime.com

guardtime

Case Study: AML/KYC

Guardtime is working with Financial Institutions in the Channel Islands to establish a blockchain based AML/KYC

Immutable records covering key AML/KYC components

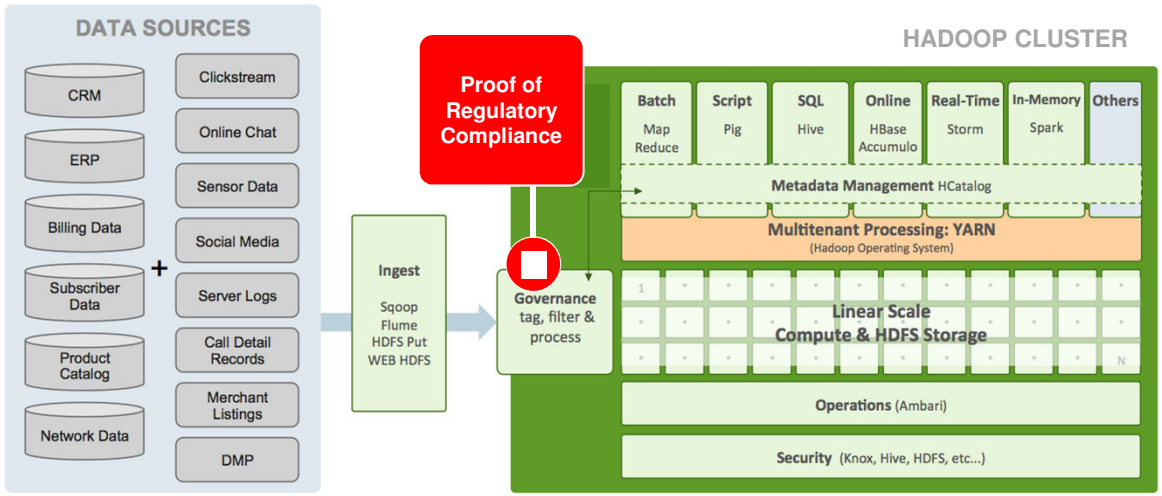
- Source of Funds
- Identity/Address of customer
- Authorized individuals/beneficiaries
- Investigation results

Data can be maintained in central repository, and access controlled by the applicant. Serves as a “fast-track” for compliance by providing the most recent, cryptographically verifiable evidence to support application processing.

guardtime

Big Data Regulatory Compliance: Hadoop Data Lakes

- Problem. Enterprises and Operators wish to use Hadoop data lakes for large scale data storage of logs and PII information, but Hadoop provides *no representation of veracity* at data asset level and make it impossible to comply with the regulations.
- Solution. Guardtime introduces a blockchain-based standard of veracity at the level of digital assets. No matter where the data is located, it *remains trackable* throughout its lifecycle from collection through to analysis and delivery, and the data engine algorithms can be assured.



guardtime

Keyless Signature Infrastructure (KSI): An Industrial Scale Blockchain

KSI enables real-time massive-scale data integrity validation.

The technology overcomes two major weaknesses of traditional blockchains:

Scalability

One of the most significant challenges with traditional blockchain approaches is scalability – they scale at O(n) complexity i.e. they grow linearly with the number of transactions.

In contrast the KSI blockchain scales at O(t) complexity – it grows linearly with time and independently from the number of transactions.

Settlement time

In contrast to the widely distributed crypto-currency approach, the number of participants in KSI blockchain distributed consensus protocol is limited. By limiting the number of participants it becomes possible to achieve consensus synchronously, eliminating the need for Proof of Work and ensuring settlement can occur within one second.

guardtime

Latest Press

WIRED

"While Black Lantern could be used by governments to protect its secrets, it just as easily could be used as a tool to keep government accountable."

"...unlike RSA, its cryptographic scheme "cannot be efficiently broken" even if an attacker uses quantum-computing algorithms."

SCIENTIFIC AMERICAN

‹re/code›

"…by enabling this distributed consensus, it can actually create a true record of events, past and present, in the digital world."

"...in the case of Bitcoin the values represent transactions; in the case of Guardtime, it's the hashed signatures of the assets being tracked."

NETWORKWORLD