

# RSA<sup>®</sup>Conference2017

Singapore | 26–28 July | Marina Bay Sands

POWER OF  
OPPORTUNITY

SESSION ID: SDS-R02

## Changing Data Protection: Heading towards a Blockchain-Operated Future



**Eugene Aseev**

Head of Singapore R&D Centre  
Acronis  
@toxzique

# Agenda



## Blockchain yesterday

Background

Blockchain 1.0:  
cryptocurrencies



## Blockchain today

Blockchain 2.0: smart  
contracts

Data protection  
solutions based on  
blockchain

Blockchain as a  
platform: transparent  
trusted timestamping

Innovating in  
conventional market

Legislation



## Blockchain tomorrow

Blockchain 3.0:  
decentralized web

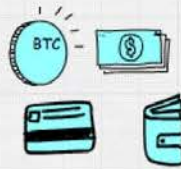
Opportunities and  
challenges

# Blockchain explained in 1 minute

- Distributed ledger
- Unique tokens
- Anonymized processing (mining)
- Immutable, encrypted, pseudo
- Smart contracts
- Consensus mechanisms



**BLOCKCHAIN Gen 1**  
2010-2015



Digital Currency & Payments led by Bitcoin



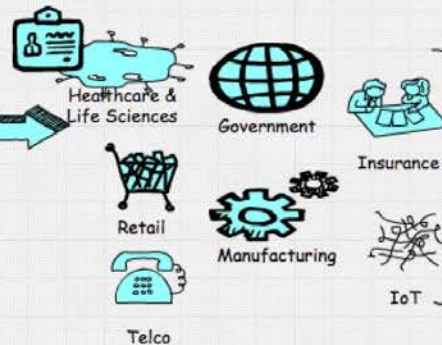
**BLOCKCHAIN Gen 2**  
2014 Onwards



Decentralized Documents & Contracts



**BLOCKCHAIN Gen 3**  
2015 and beyond



Diverse and Disruptive Applications in established Vertical Markets



# Blockchain 1.0: Cryptocurrencies

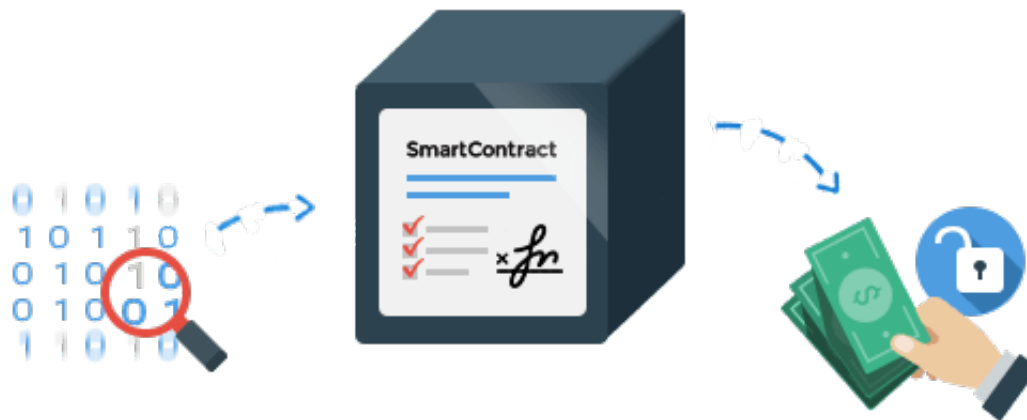


Current payment systems require third-party intermediaries that often charge high processing fees ...

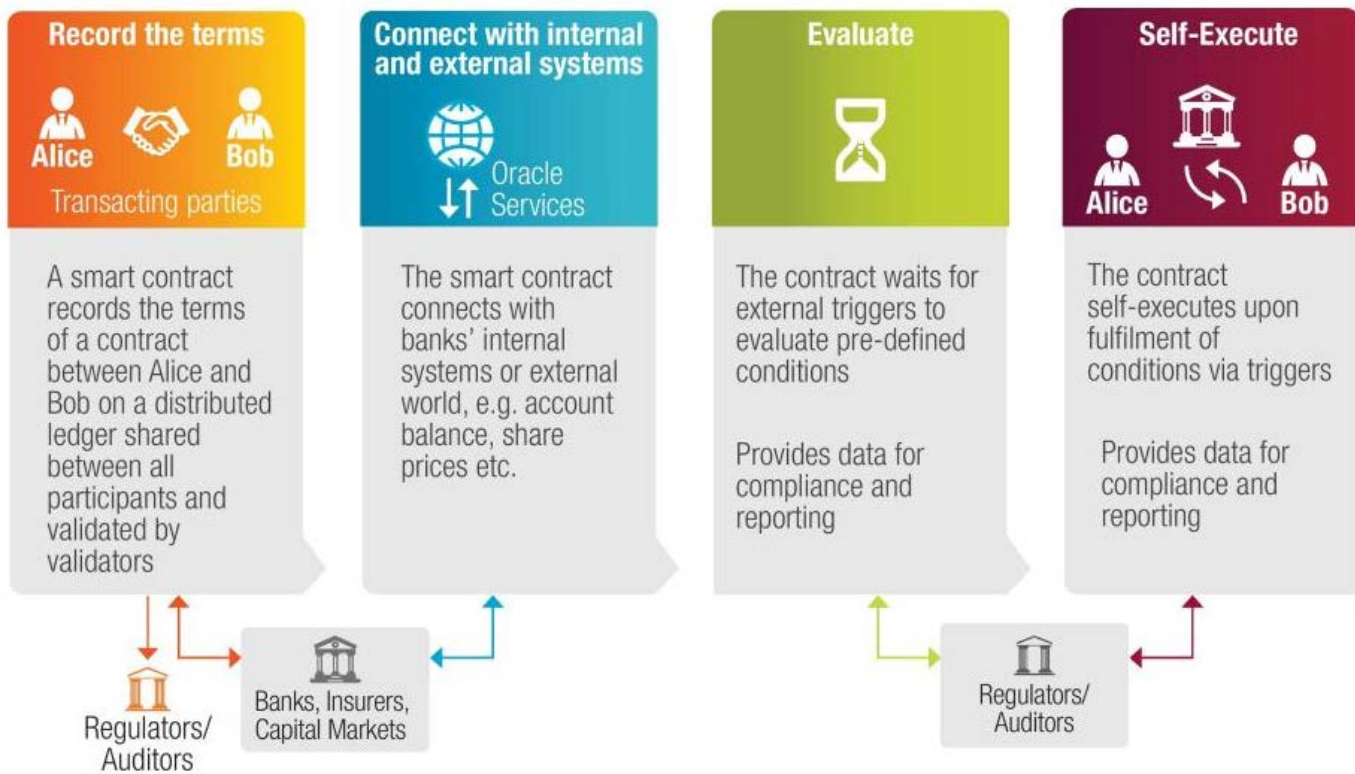


... but machine-to-machine payment using the Bitcoin protocol could allow for direct payment between individuals, as well as support micropayments.

# Blockchain 2.0: Smart Contracts



# Smart Contract Lifecycle



# Traditional vs. Smart Contracts



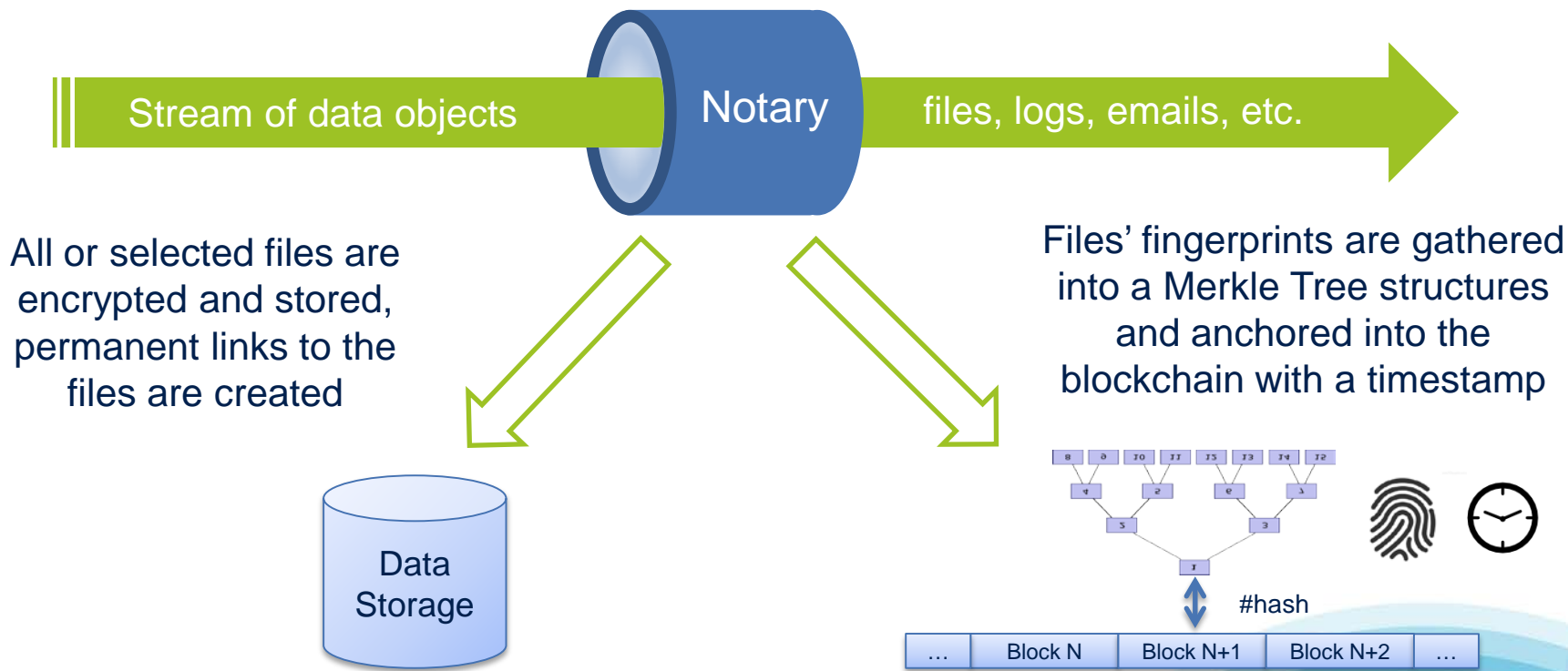
## Traditional contracts

a court, the court would look at you like you were who could look at you like you were  
**Smart contracts**  
 iration."

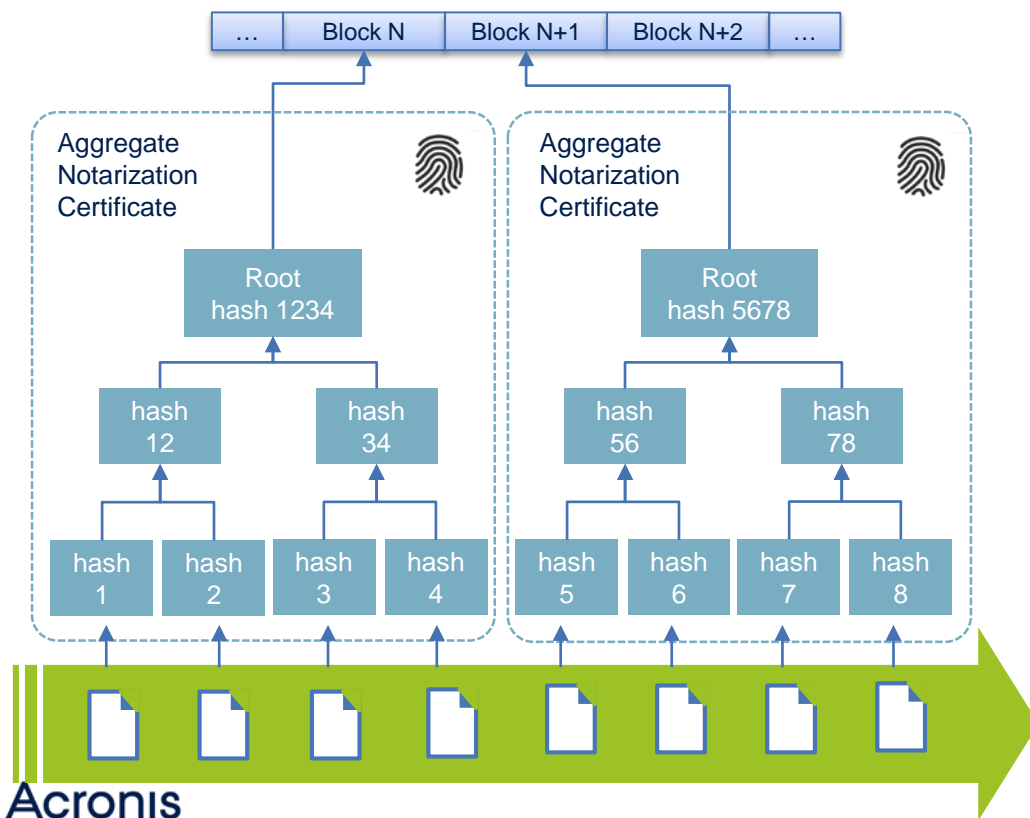
 1-3 Days	 Minutes
 Manual remittance	 Automatic remittance
 Escrow necessary	 Escrow may not be necessary
 Expensive	 Fraction of the cost
 Physical presence (wet signature)	 Virtual presence (digital signature)
 Lawyers necessary	 Lawyers may not be necessary



# Data Notarization



# Trusted Timestamping



Acronis

In cryptography and computer science, a hash tree or Merkle tree is a tree in which every non-leaf node is labelled with the hash of the labels or values of its child nodes. Hash trees are useful because they allow efficient and secure verification of the contents of large data structures.

Notary computes Aggregate Notarization Certificate (ANC) for a batch of files. Each ANC contains a Merkle tree built using hashes of the files in the batch. The root hash of the tree is recorded into the blockchain.

Having the ANC and the corresponding record in the blockchain one can prove the authenticity of the files from the batch.

Number of files per batch depends on the application requirements and features.

# Digital Notarization Market Landscape



Apostille

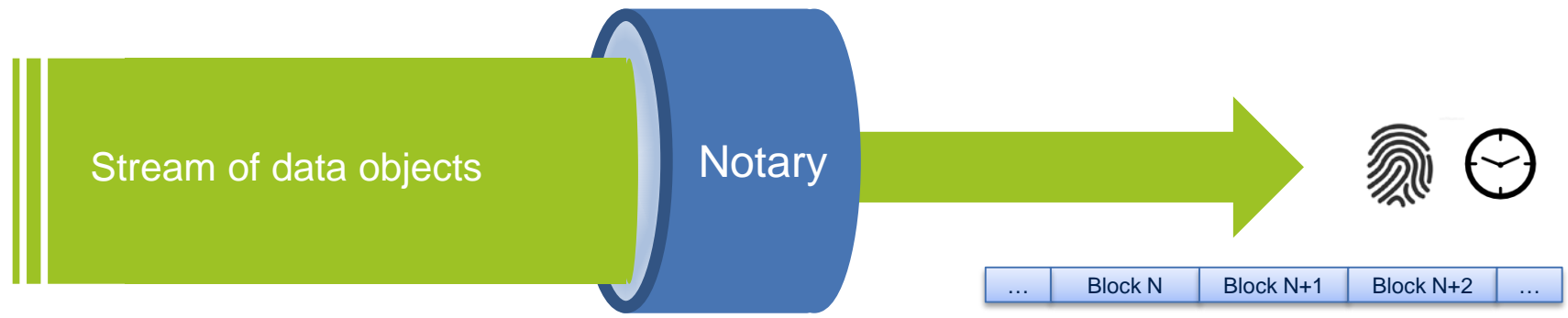


Emercoin

Acronis

# Challenges with Blockchain

Balance high volume data stream at the input with low recording rate of a blockchain: achieve recording rate x10,000 data objects per second



Scalable industrial solutions must be able to process huge streams of data

Low recording rate is the intrinsic property of blockchains

# Innovating in Conventional Market

Software-defined storage **with data verification**

Backup solution **with data verification**

Electronic signing **with trusted timestamping**



PROTECTION AGAINST INSIDER  
ATTACKS



REGULATORY TRANSPARENCY



PORTABILITY OF EVIDENCE

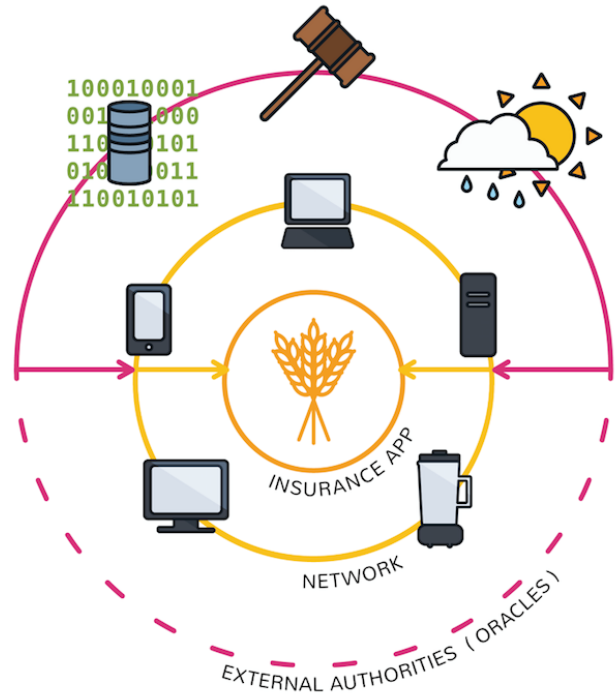


INDEPENDENT VERIFICATION

# Digital Notary Legislation

- **Uniform Electronic Transactions Act ('UETA')** is an Act adopted by 47 states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands
- **Electronic Signatures in Global and National Commerce Act ('ESIGN')** was passed at the federal level in 2000
- **Vermont Blockchain law – Act No. 157 (H.868):** *“Blockchain Technology (effective July 1, 2016) creates rebuttable statutory presumptions of authenticity for records using blockchain technology”*
- **Arizona Blockchain Bill HB 2417:** *“A signature that is secured through blockchain technology is considered to be in an electronic form and to be an electronic signature”*
- **Delaware Senate Bill 69:** *“The bill includes a series of amendments to the Delaware General Corporation Law, specifically to Sections 219, 224, and 232, that legally recognize any number of records being stored on networks of electronic databases – e.g., blockchain – for the creation and maintenance of corporate records, including the corporation’s stock ledger”*

# Blockchain 3.0: Decentralized Web



# Decentralized Data Protection



STORJ.IO



Filecoin



MaidSafe

Acronis



# Opportunities and Challenges

## Opportunities

- Unique marketplace
- Secure data fragmentation and distribution
- Availability and resilience
- Combination of legacy and modern systems

## Challenges

- Performance and stability
- Vulnerabilities in smart contracts
- Trust for alternative currencies
- Auditability

# Apply What You Have Learned Today

- Next week you should:
  - Read couple of articles explaining blockchain as a technology
- In the first three months following this presentation you should:
  - Read several materials about potential blockchain applications. Identify applications solving real-world problems, and those coming out of the thin air and blockchain buzz
- Within six months you should:
  - Build a simple Decentralized App on Ethereum platform solving small yet real-world problem

# RSA<sup>®</sup>Conference2017

Singapore | 26–28 July | Marina Bay Sands

SESSION ID: SDS-R02

## Thank you!



**Eugene Aseev**

Head of Singapore R&D Centre  
Acronis  
@toxizique

POWER OF  
OPPORTUNITY