PRESERVATION OF AUTHENTIC DIGITAL RECORDS USING BLOCKCHAIN

Dr. **Hrvoje Stančić**, full professor

Director Team Europe, InterPARES Trust

Department of Information and Communication Sciences

Faculty of Humanities and Social Sciences

University of Zagreb, Croatia

hstancic@ffzg.hr

Havana, 18 February 2019

Contents

1. Introduction
2. eIDAS Regulation
3. ETSI EN 319 102-1
4. The study
5. Blockchain enabling concepts
6. TrustChain model
7. Conclusion

1. Introduction

- Documents and records today – increasingly
  - created, analysed, used, reused

  in the digital form
- Requirements for the (long-term) preservation (LTP) of digital records
  - different for various types of records
    - e.g. 11 years, 70 years, permanently
- Constant change and development of ICT
  - LTP actions = conversion, migration, emulation, virtualization

1. Introduction …

- LTP challenges – how to preserve
  - authenticity
  - integrity
  - reliability
  - usability
  - non-repudiation
  - security
  - confidentiality
- Focus on a particular challenge
  - LTP of digitally signed or sealed records
- **eIDAS Regulation**
  - Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

    http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN

2. eIDAS Regulation

- **eIDAS Regulation**
  - e-Signatures
  - e-Timestamps
  - e-Seals
  - Qualified Trust Services
  - …

2. eIDAS Regulation ...

- **Advanced e-signature**
  - an e-signature that:
    - (a) it is uniquely linked to the signatory
    - (b) it is capable of identifying the signatory
    - (c) it is created using means that the signatory can maintain under his sole control, and
    - (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable
- Advanced e-signatures rely on **qualified certificates**
  - guarantee the authenticity and the identity of the signatory

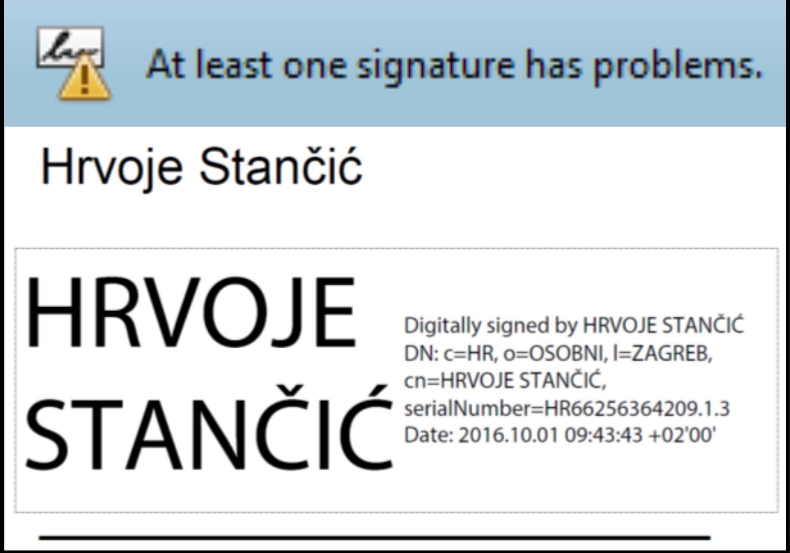
2. eIDAS Regulation ...

eIDAS

- **Challenges** with e-signatures
  - short expiration period
  - possibilities of certificate revocation
  - the need for resigning
  - dependence on the certification authority(-ies), i.e. qualified trust service providers ("trusted third party")

2. eIDAS Regulation ...

eIDAS

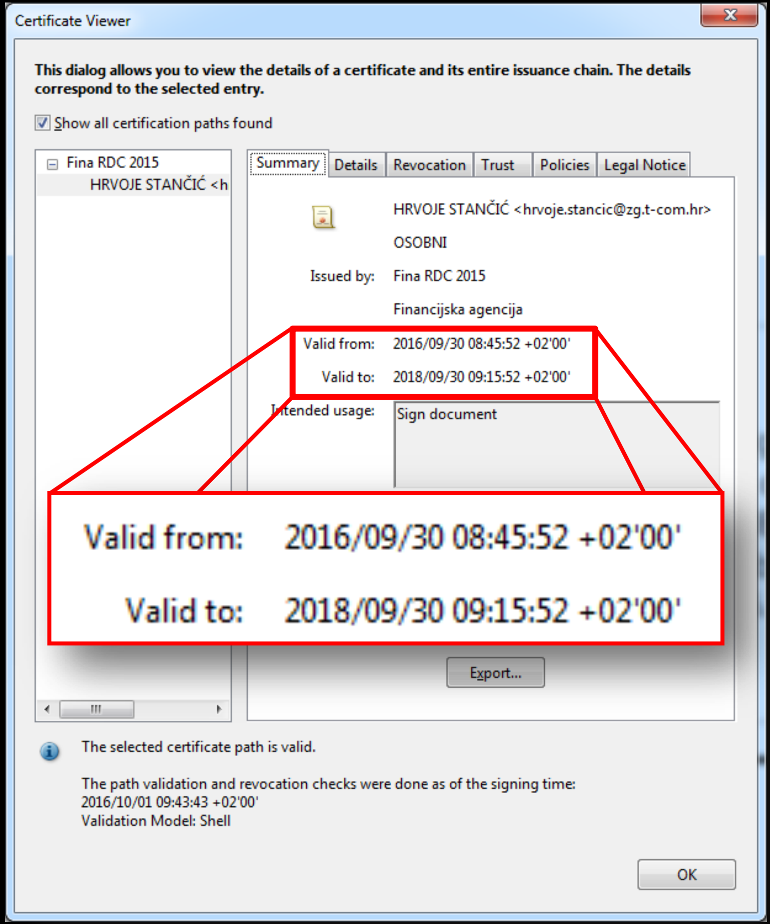


At least one signature has problems.

Hrvoje Stančić

HRVOJE STANČIĆ

Digitally signed by HRVOJE STANČIĆ
DN: c=HR, o=OSOBNI, l=ZAGREB, cn=HRVOJE STANČIĆ, serialNumber=HR66256364209.1.3
Date: 2016.10.01 09:43:43 +02'00'



Certificate Viewer

This dialog allows you to view the details of a certificate and its entire issuance chain. The details correspond to the selected entry.

☑ Show all certification paths found

HRVOJE STANČIĆ <hrvoje.stancic@zg.t-com.hr>

OSOBNI

Issued by: Fina RDC 2015

Financijska agencija

Valid from: 2016/09/30 08:45:52 +02'00'

Valid to: 2018/09/30 09:15:52 +02'00'

Intended usage: Sign document

Valid from: 2016/09/30 08:45:52 +02'00'

Valid to: 2018/09/30 09:15:52 +02'00'

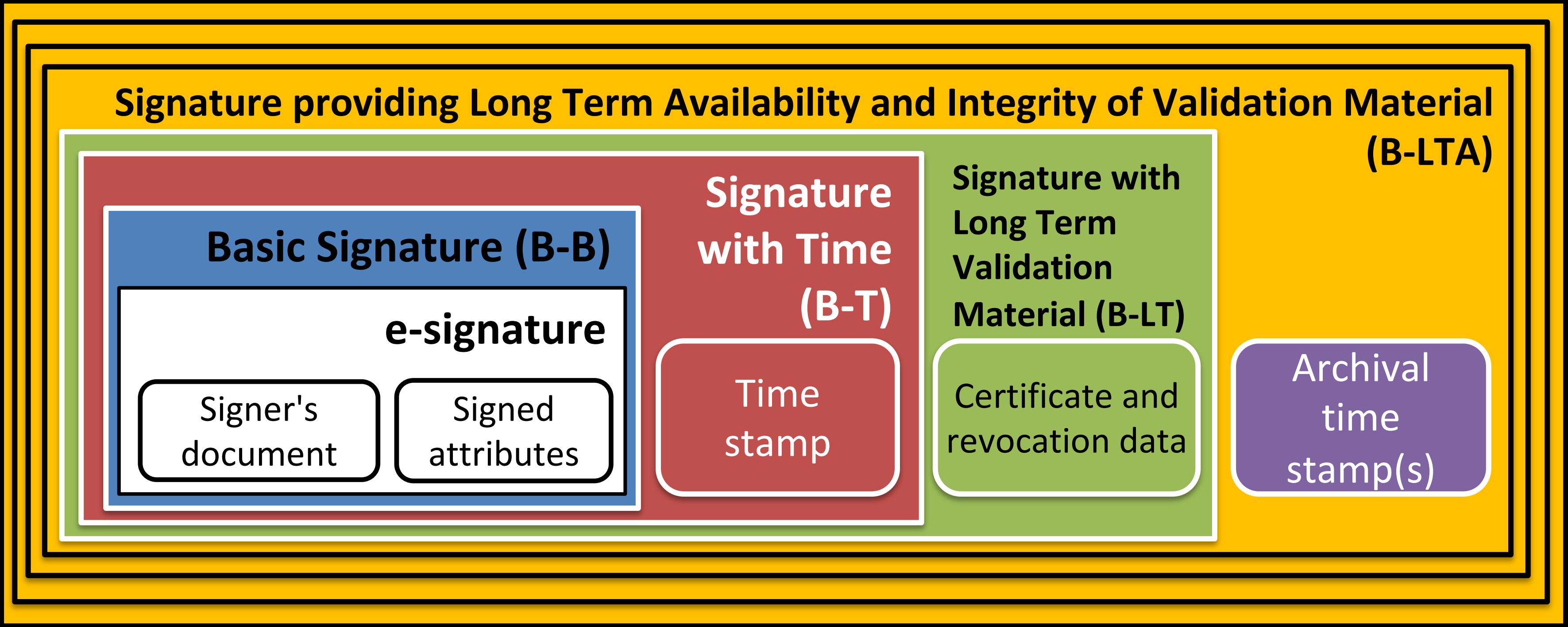
The selected certificate path is valid.

The path validation and revocation checks were done as of the signing time:
2016/10/01 09:43:43 +02'00'
Validation Model: Shell

3. ETSI EN 319 102-1

eIDAS

Procedures for Creation and Validation of AdES Digital Signatures (Part one: Creation and Validation)



Signature providing Long Term Availability and Integrity of Validation Material (B-LTA)

Signature with Long Term Validation Material (B-LT)

Signature with Time (B-T)

Basic Signature (B-B)

e-signature

Signer's document

Signed attributes

Time stamp

Certificate and revocation data

Archival time stamp(s)

4. The study

Model for Preservation of Trustworthiness of the Digitally Signed, Timestamped and/or Sealed Digital Records (TRUSTER Preservation Model)

- the Team: Hrvoje Stančić (lead), Victoria Lemieux, Natasha Khramtsovsky, Enigio Time AB, Croatian Financial Agency FINA, FHSS GRAs
- a model for blockchain-based Validity Information Preservation (VIP) solution

TRUSTCHAIN

3. Blockchain enabling concepts

1. Hash algorithm
2. Merkle tree
3. Chaining of top hashes
4. Distributed consensus

1. Hash algorithm

SHA-256 – example of a hash value of a document

7d8c5b62dcb44023
3f7eaac1ec49e4c3
86b8089c37d69ab5
1bc674b8877cb032

Abstract proposal for paper presentation at ICA Conference, October 2016 in Seoul

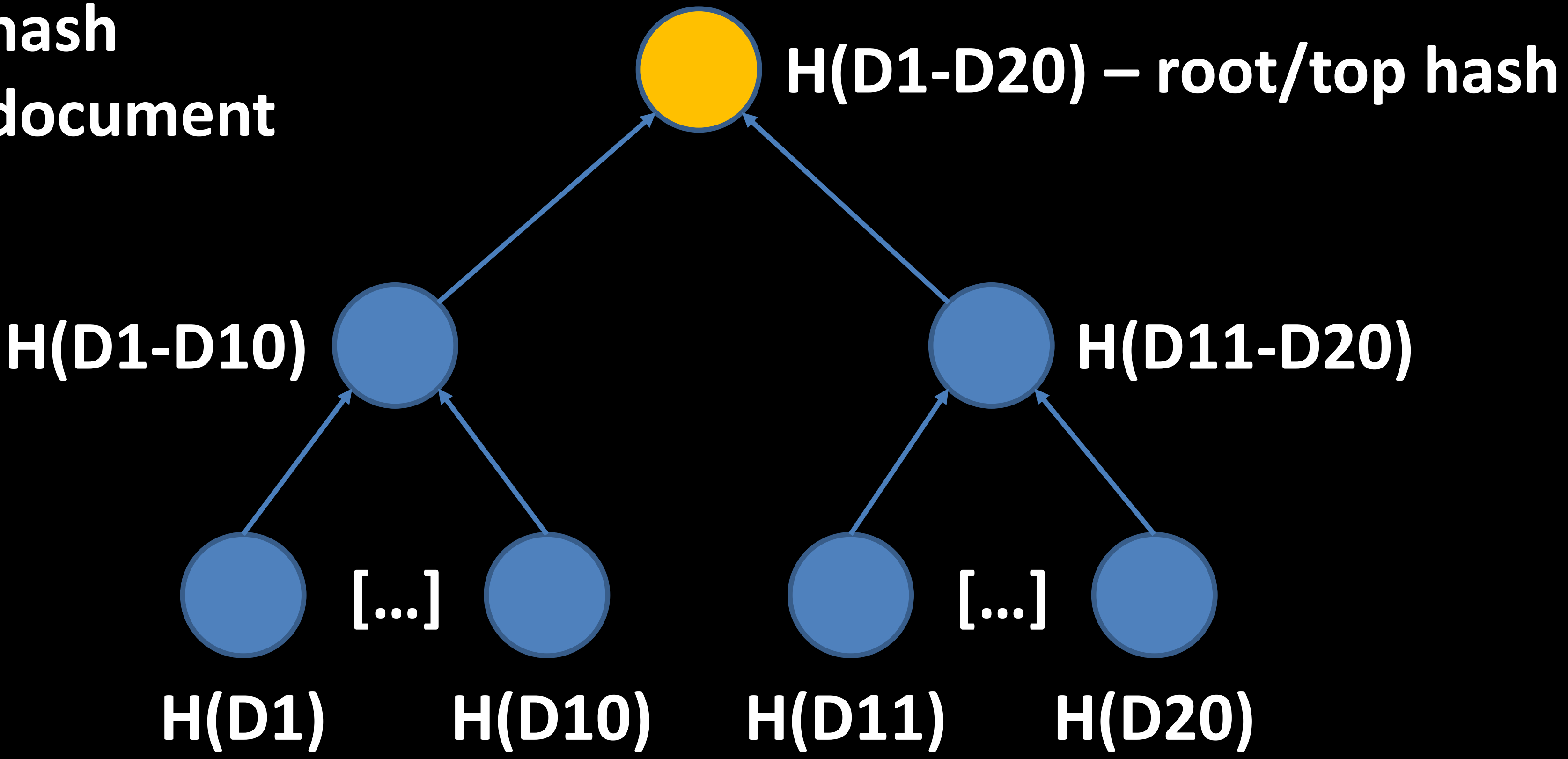
Hrvoje Stancic – Faculty of Humanities and Social Sciences, University of Zagreb, Croatia
Hans Almgren – Empir Time AB, Stockholm, Sweden
Natasha Khramtsovsky – Electronic Office Systems LLC, Moscow, Russia

Recordkeeping in the Digital Age – Possibilities and challenges of using linking based timestamping and blockchain technology to maintain long term integrity and authenticity

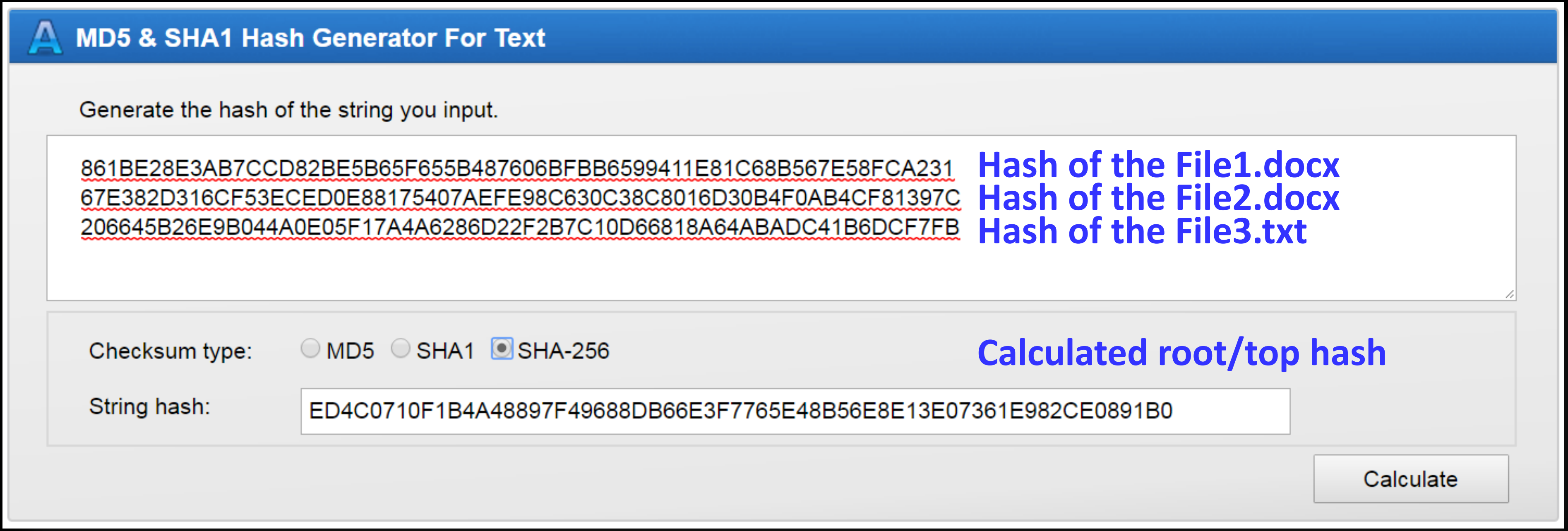
[illegible]

2. Merkle tree

H – hash
D – document



2. Merkle tree



MD5 & SHA1 Hash Generator For Text

Generate the hash of the string you input.

```
861BE28E3AB7CCD82BE5B65F655B487606BFBB6599411E81C68B567E58FCA231
67E382D316CF53ECED0E88175407AEFE98C630C38C8016D30B4F0AB4CF81397C
206645B26E9B044A0E05F17A4A6286D22F2B7C10D66818A64ABADC41B6DCF7FB
```

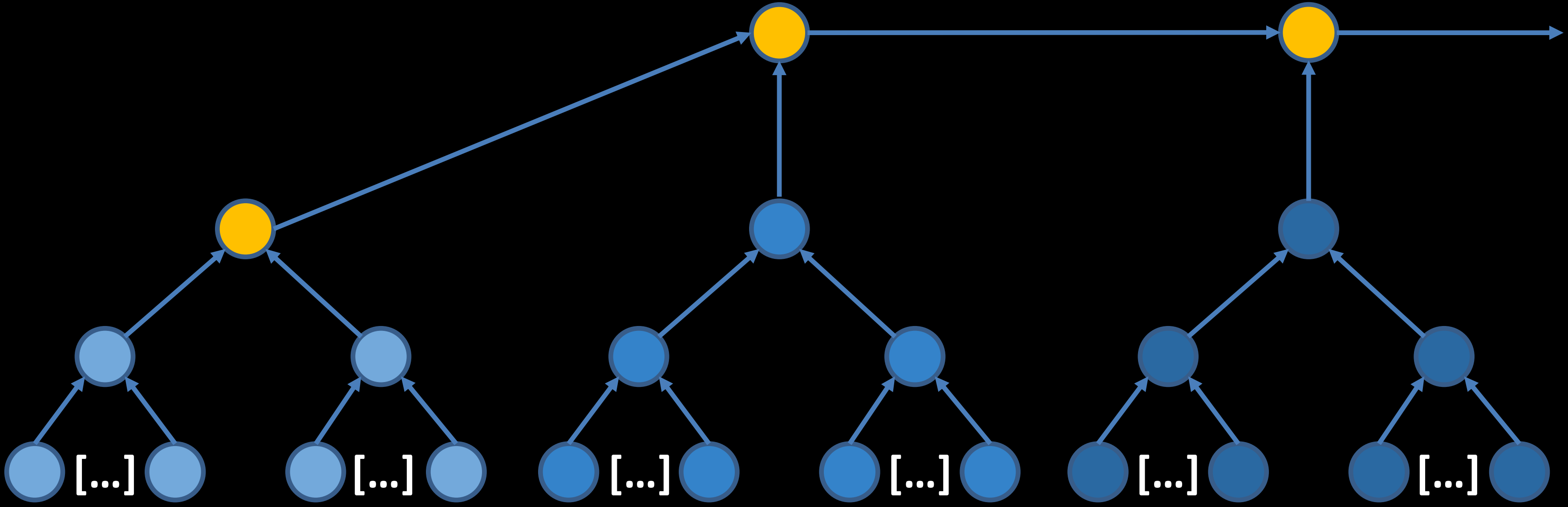
Hash of the File1.docx
Hash of the File2.docx
Hash of the File3.txt

Checksum type: ○ MD5 ○ SHA1 ● SHA-256

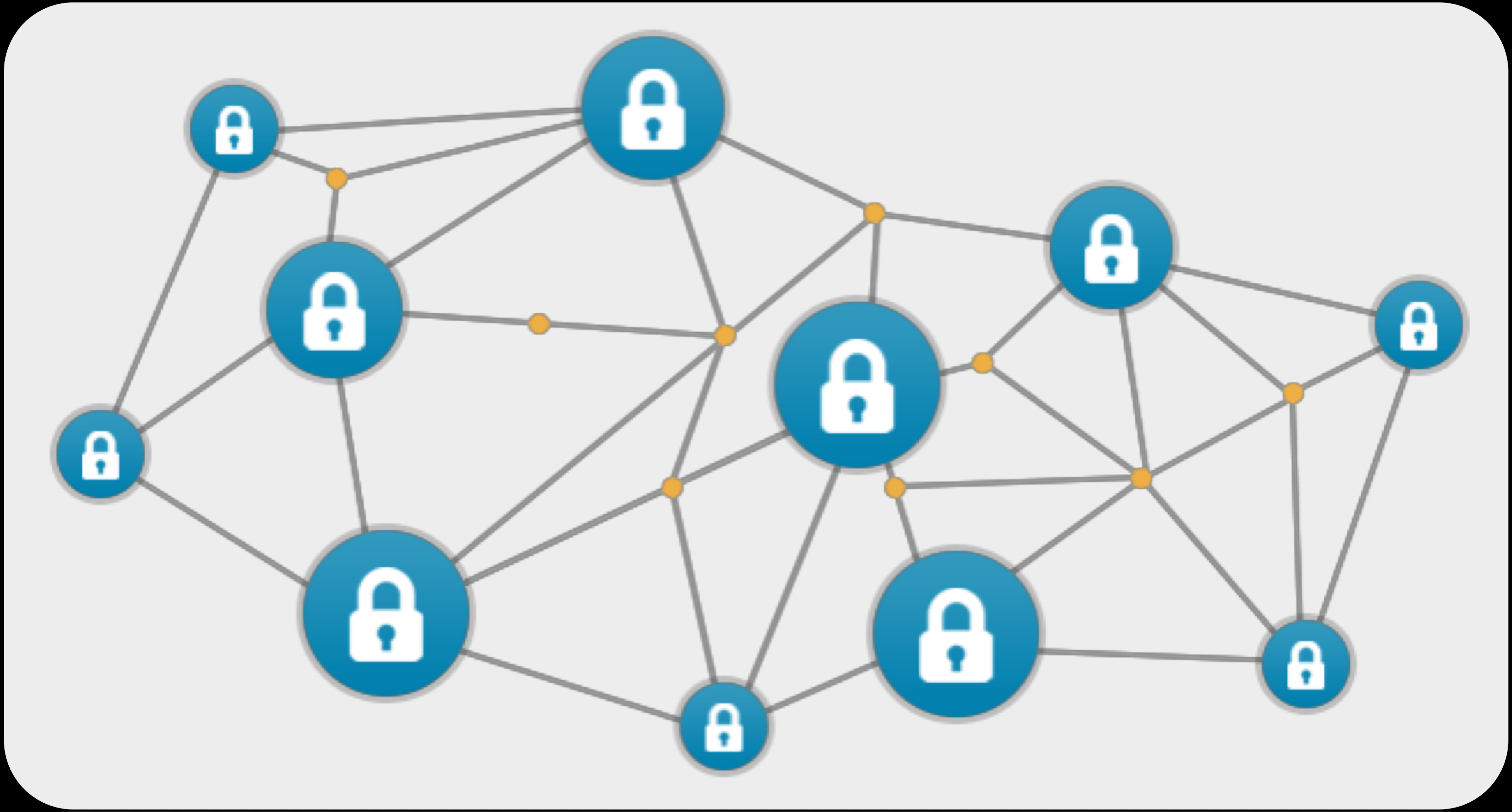
Calculated root/top hash

String hash: ED4C0710F1B4A48897F49688DB66E3F7765E48B56E8E13E07361E982CE0891B0

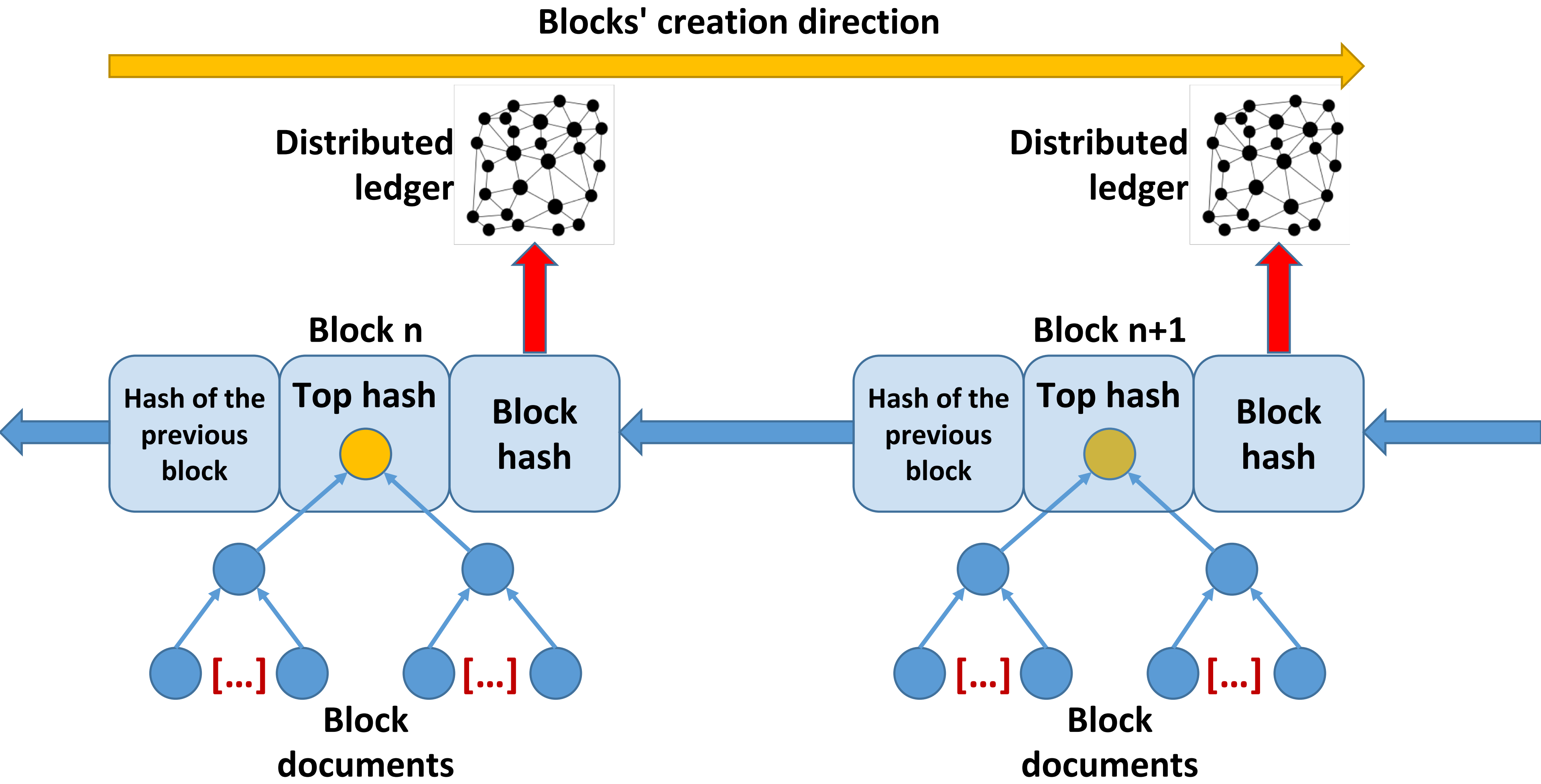
3. Chaining of top hashes



4. Distributed (peer-to-peer) consensus



Blockchain



Blocks' creation direction

Distributed ledger

Block n

Hash of the previous block

Top hash

Block hash

[...] [...]

Block documents

Distributed ledger

Block n+1

Hash of the previous block

Top hash

Block hash

[...] [...]

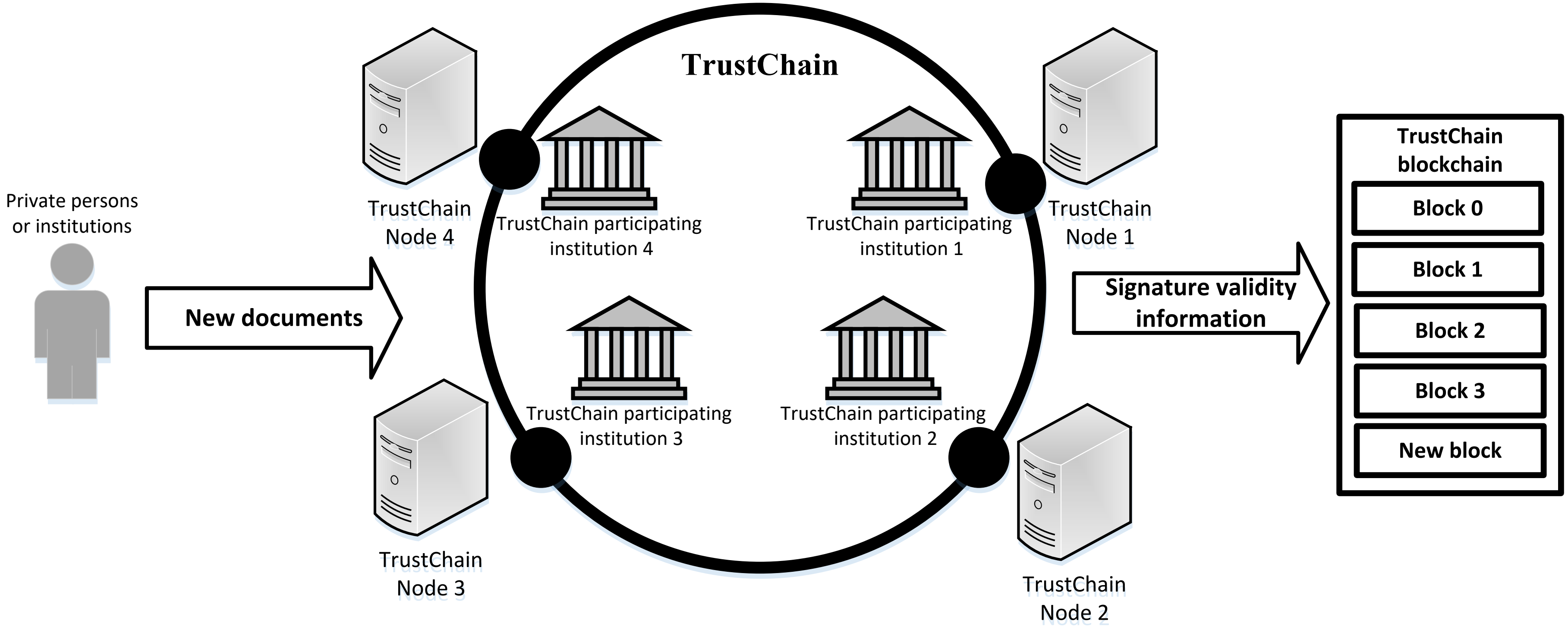
Block documents

4. TrustChain model

1. A request to register new document is started

2. TrustChain instituions check the signature and vote on its validity

3. Documents are registered in the TrustChain blockchain



Private persons or institutions

New documents

TrustChain

TrustChain Node 4

TrustChain participating institution 4

TrustChain participating institution 1

TrustChain Node 1

TrustChain participating institution 3

TrustChain participating institution 2

TrustChain Node 3

TrustChain Node 2

Signature validity information

TrustChain blockchain

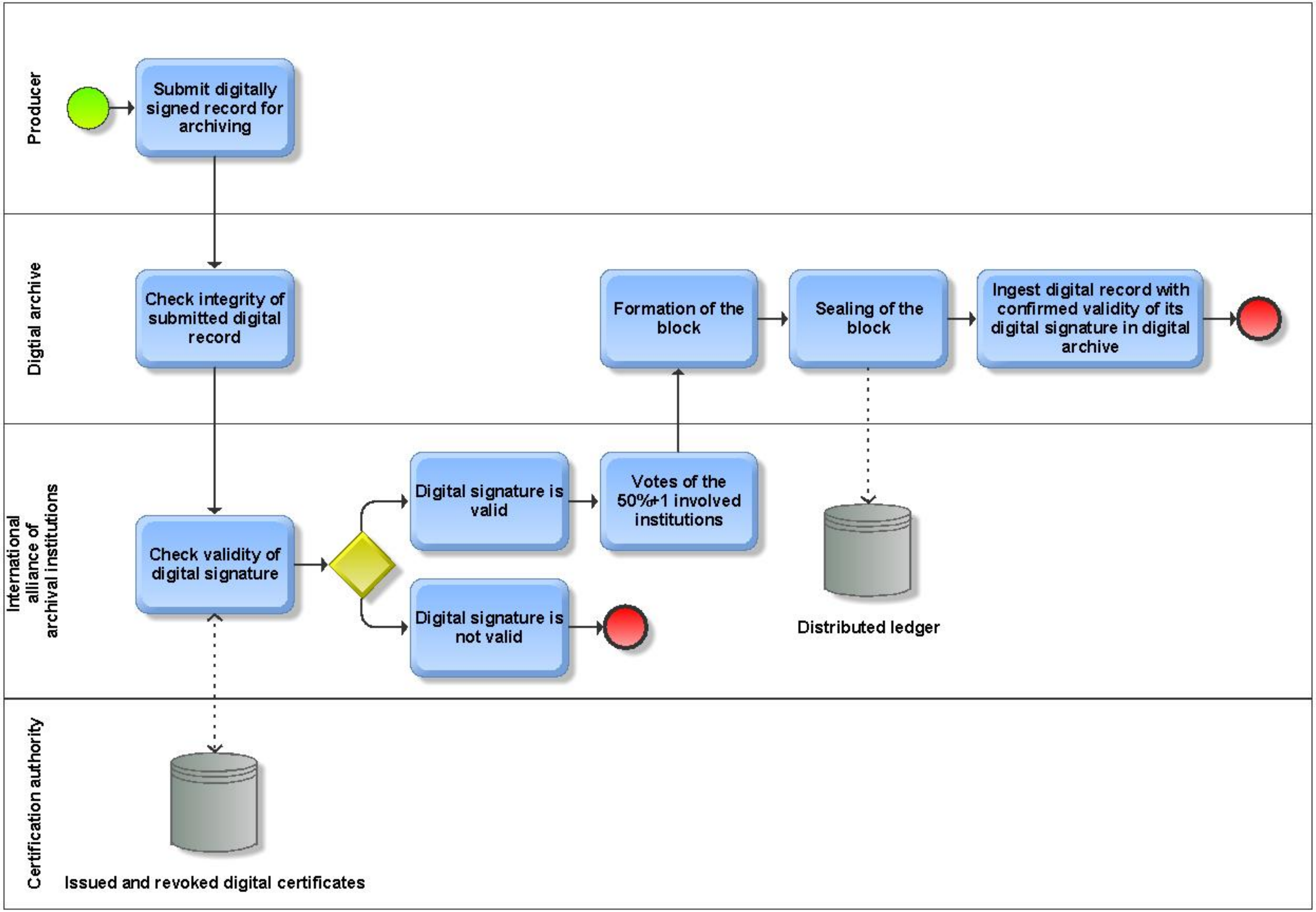
Block 0

Block 1

Block 2

Block 3

New block



Producer

Submit digitally signed record for archiving

Digtial archive

Check integrity of submitted digital record

Formation of the block

Sealing of the block

Ingest digital record with confirmed validity of its digital signature in digital archive

International alliance of archival institutions

Check validity of digital signature

Digital signature is valid

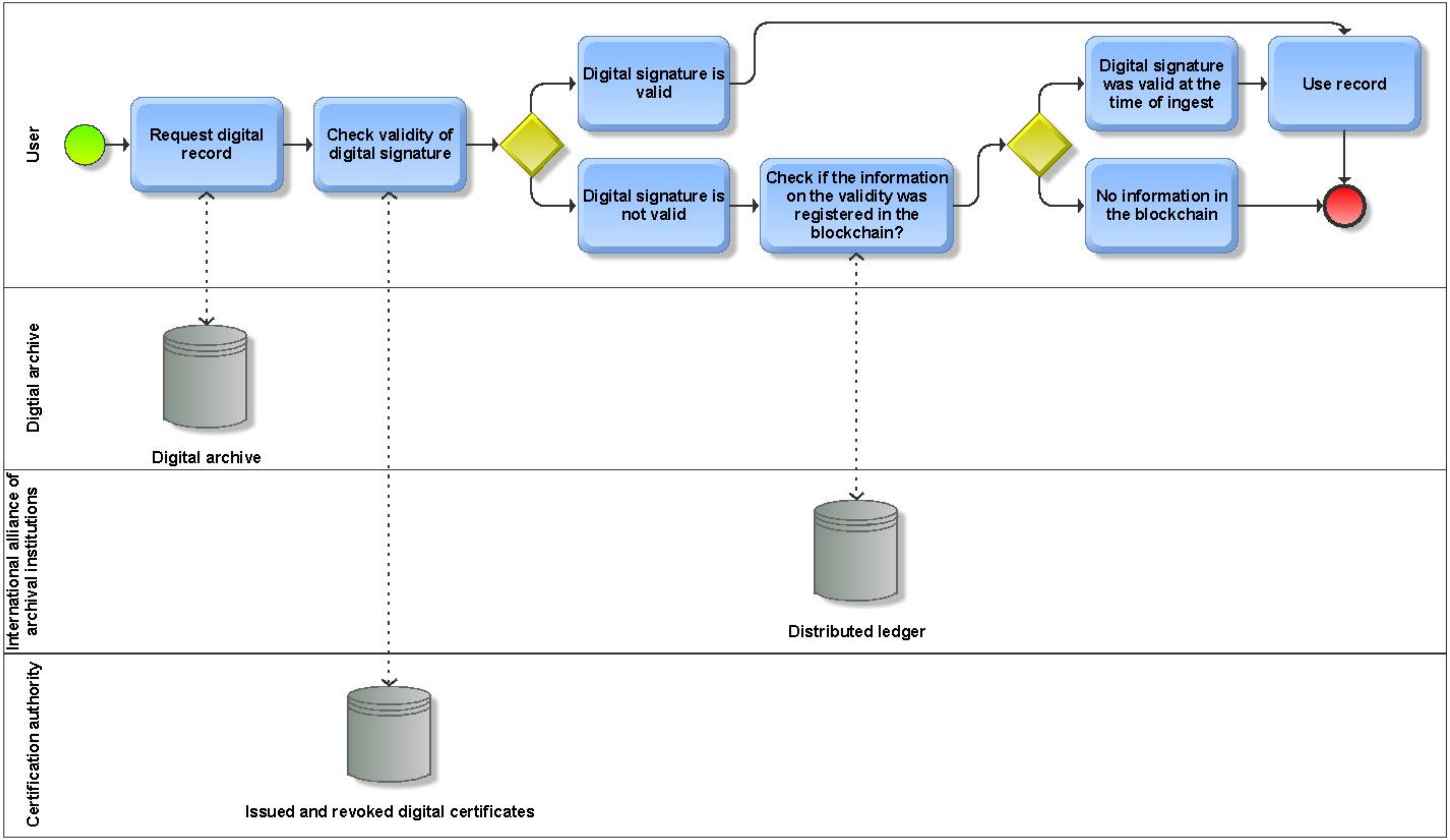
Votes of the 50%+1 involved institutions

Digital signature is not valid

Distributed ledger

Certification authority

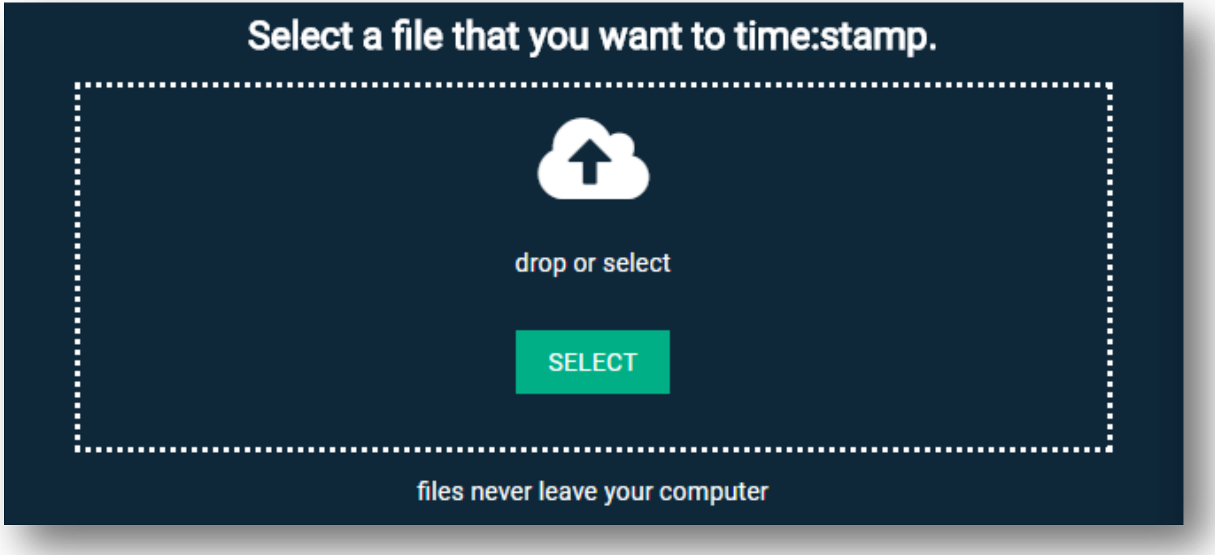
Issued and revoked digital certificates


User
Digtial archive
International alliance of archival institutions
Certification authority
Request digital record
Check validity of digital signature
Digital signature is valid
Digital signature is not valid
Check if the information on the validity was registered in the blockchain?
Digital signature was valid at the time of ingest
No information in the blockchain
Use record
Digital archive
Distributed ledger
Issued and revoked digital certificates

Can you start before we develop TrustChain?

EnigioTime – time:beat solution

https://timebeat.com/



Select a file that you want to time:stamp.

drop or select

SELECT

files never leave your computer

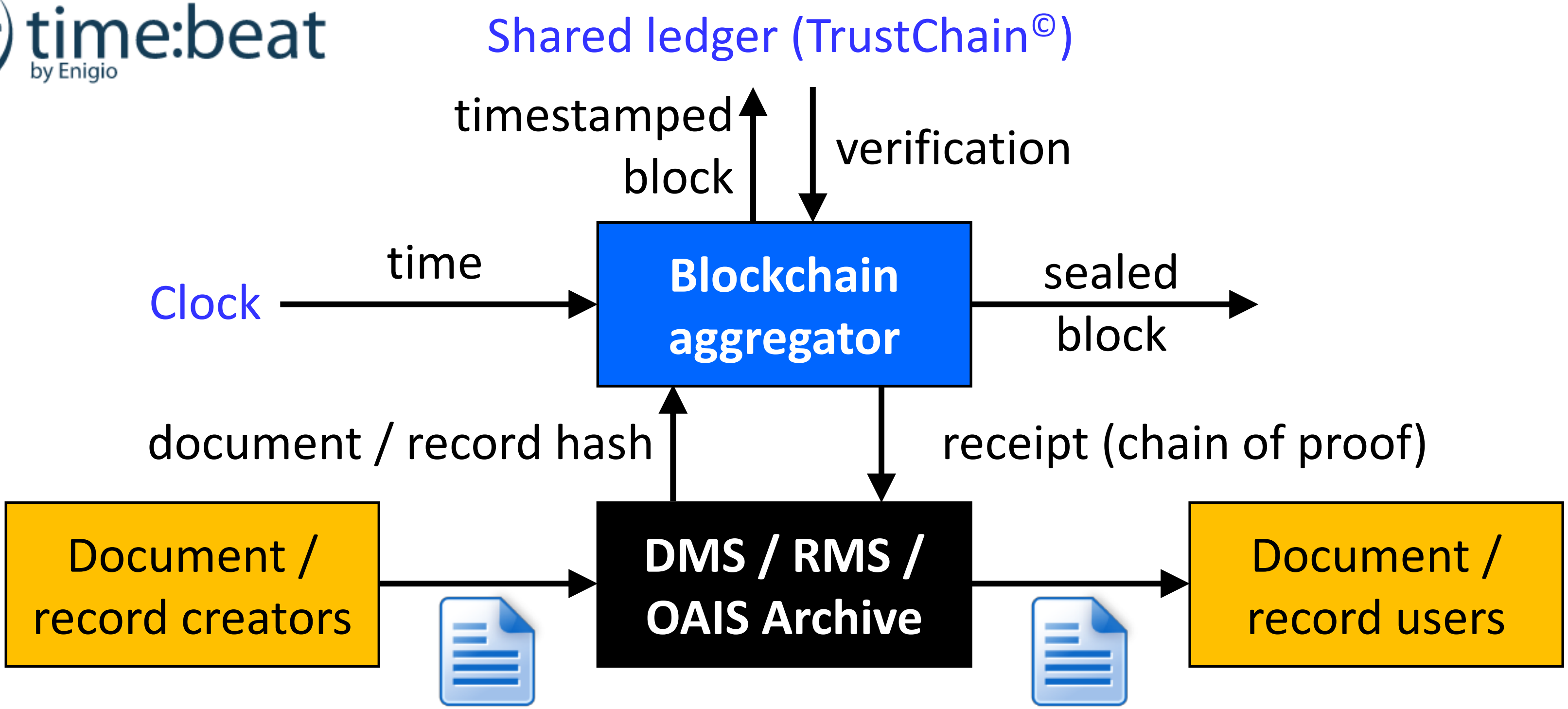
time:beat
by Enigio

Files	Web	Pictures	E-mail
time:stamp	time:grab	time:shot	time:mail

Can you start before we develop TrustChain?

EnigioTime – blockchain aggregator

time:beat by Enigio



Shared ledger (TrustChain©)

timestamped block

verification

Clock

time

Blockchain aggregator

sealed block

document / record hash

receipt (chain of proof)

Document / record creators

DMS / RMS / OAIS Archive

Document / record users

TrustChain

1. Confirm integrity
2. Existence or creation at a point in time
3. Confirm sequence
4. Support/enhance non-repudiation
5. Improve validation

7. Conclusion

- By using blockchain aggregator and TrustChain
  - establish the new generation of archival and business-oriented e-services
  - enable anyone to connect using API
  - preserve authentic digital records with the help of blockchain principles

Resources

- Bralić, V., Kuleš, M., & Stančić, H. (2017).
  A model for long-term preservation of digital signature validity: TrustChain
  In: I. Atanassova, W. Zaghouani, B. Kragić, K. Aas, H. Stančić, & S. Seljan (Eds.), INFuture2017: Integrating ICT in Society, pp. 89-113, https://www.researchgate.net/publication/321171227_A_Model_for_Long-term_Preservation_of_Digital_Signature_Validity_TrustChain

- **InterPARES Trust research dissemination**
  https://interparestrust.org/trust/research_dissemination

THANK YOU!

Preservation of Authentic Digital Records Using Blockchain

Dr. **Hrvoje Stančić**, full professor

Director Team Europe, InterPARES Trust

Department of Information and Communication Sciences

Faculty of Humanities and Social Sciences

University of Zagreb, Croatia

hstancic@ffzg.hr

Havana, 18 February 2019