EnigioTime

is it possible to maintain integrity and authenticity without certificates?

Hans Almgren, Mats Stengård

EnigioTime

hans.almgren@enigio.com
mats.stengard@enigio.com

presentators

- Hans Almgren, CTO Enigio Time AB
  M.Sc. Industrial Engineering Linköping University
  Computer Science, Polytech Lausanne

- Mats Stengård, COO Enigio Time AB
  M.Sc. Computer Science and Engineering Linköping University
  Computer Science, Polytech Nice-Sophia

enigio time

- Innovation driven company founded in Stockholm 2012
  - Swedish patents, approved PCT applications and international patents pending
- Background & Competence
  - Computer science, cryptography, e-archive systems, realtime trading systems…
- Main focus
  - Qualified electronic timestamps and E-archives
- Services
  - Consulting, development and maintenance of e-archive solutions
  - Platform with API for qualified electronic timestamping
  - Web and mobile applications built on the platform
- Research association
  - Collaborator members in InterPARES Trust

EnigioTime

the mission

EnigioTime

- Protect ”Data at Rest” from manipulation, secure existence in time with **integrity** and **authenticity**

  - The world creates vast amounts of data that is continuously in the process of becoming and changing
  - Data location is ”in the cloud” and the actual physical location will probably be a less relevant attribute
  - Long term preservation of data

EnigioTime

the challenge

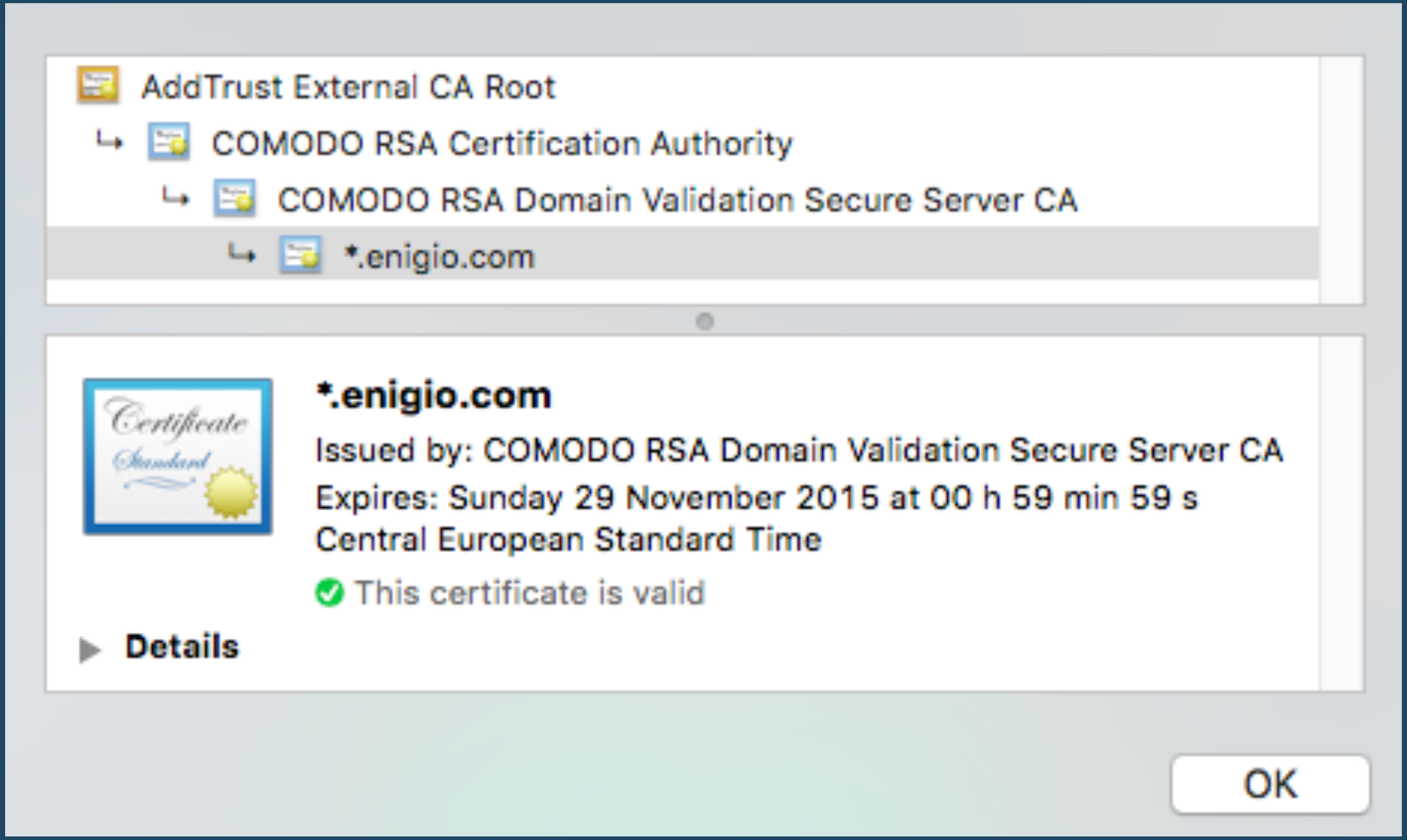
cryptographic keys

- Cryptographic keys are introduced mainly for secure communication, encryption/decryption and authenticity

- However, the protection of sensitive information in an archive does not really need this.

  Access control and reliable traceability will often be a more convenient strategy.
  e.g. Medical records.

Keys need certificates



AddTrust External CA Root
↳ COMODO RSA Certification Authority
↳ COMODO RSA Domain Validation Secure Server CA
↳ *.enigio.com

***.enigio.com**
Issued by: COMODO RSA Domain Validation Secure Server CA
Expires: Sunday 29 November 2015 at 00 h 59 min 59 s Central European Standard Time
✓ This certificate is valid

EnigioTime

traditional PKI

PKI introduces some problems for long term preservation:

- Certificate expiry
  - Adds complexity and cost for the records keeper
  - Should the signature be re-signed or re-validated?
- Key management
- Single point of failure
- Trust is required for the certificate infastructure

certificate chains are sensitive structures

- Certificates chains are the foundation for key distribution (PKI).

- Strong but not stronger than their weakest link

- If any link expires, or becomes compromised, the entire structure will be compromised

- One line of trust. No redundancy. No proof.

EnigioTime

could certificates live forever?

- Technologic advances (cryptos, hardware…)
- Human factors (maintaining the private key etc.)
- Changes in the real world need to be reflected. Nothing lasts forever.
- Revocation strategy needed. Current implementations are CRLs and OCSP.
- After expiration, the certificate is not included in revocation procedures
- Without expiration, CRLs would grow forever

EnigioTime

Can we find a way to preserve **integrity** and **authenticity** without introducing the issues of expired certificates and key management?

blockchain technology for maintaining integrity and authenticity?

EnigioTime

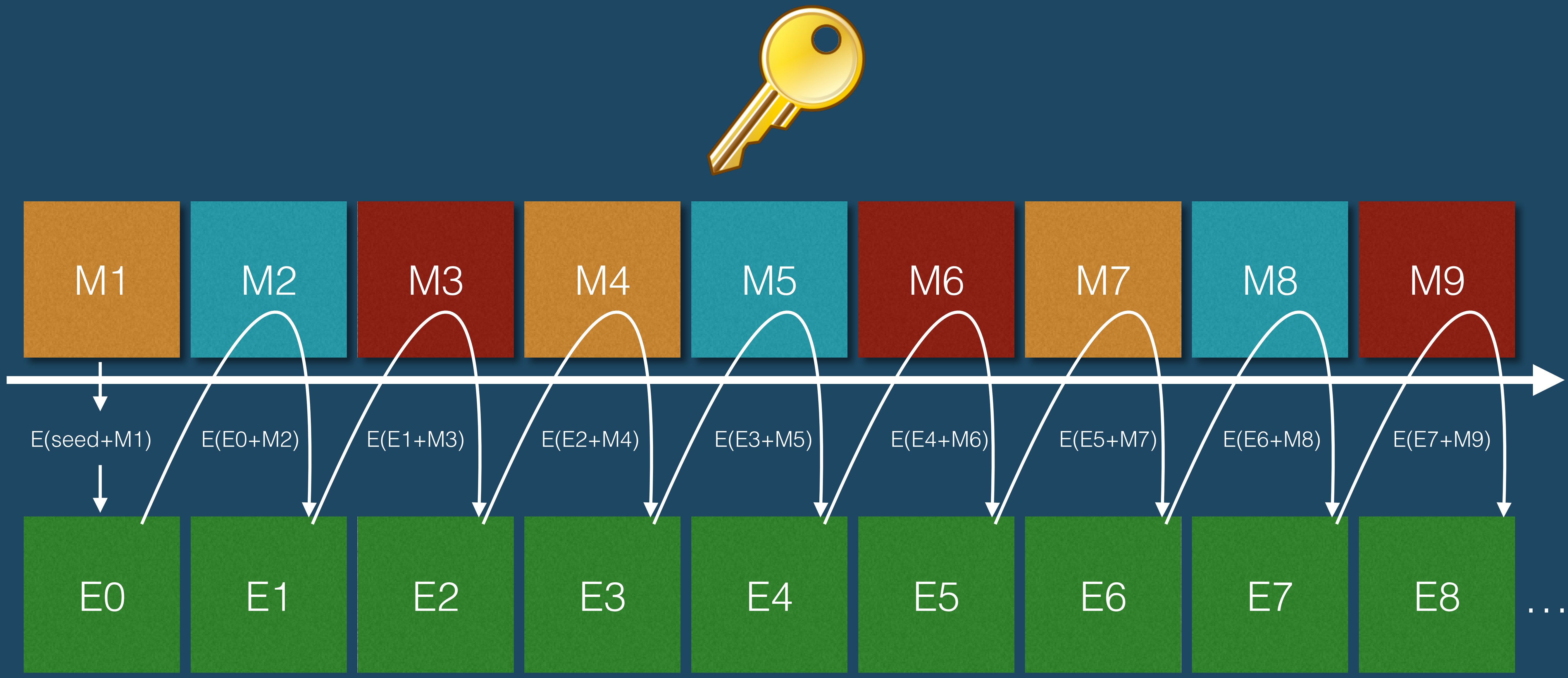
integrity of data

- To secure integrity of data and make sure manipulation has not occurred we usually use cryptographic checksums (via one-way hash functions)

- This is used in many different applications and certainly in electronic archives

cipher block chaining

- Another well-established concept in cryptography is CBC (cipher block chaining)
- Encrypting each block of a message by making it dependent on all previous blocks in the message creates an unbreakable chain
- Any change in a single bit of the encrypted message invalidates the possibility of retrieving it.



M1 M2 M3 M4 M5 M6 M7 M8 M9

E(seed+M1) E(E0+M2) E(E1+M3) E(E2+M4) E(E3+M5) E(E4+M6) E(E5+M7) E(E6+M8) E(E7+M9)

E0 E1 E2 E3 E4 E5 E6 E7 E8 …

EnigioTime

block chain technology

- Block chain technology resembles CBC. However, it does not require any key.

- Bitcoin has paved the way for a considerable wider adoption of block chain technology.

- By using block chaining or a ”linked scheme” we can arrange a sequence of cryptographic checksums from data, securing integrity of the series

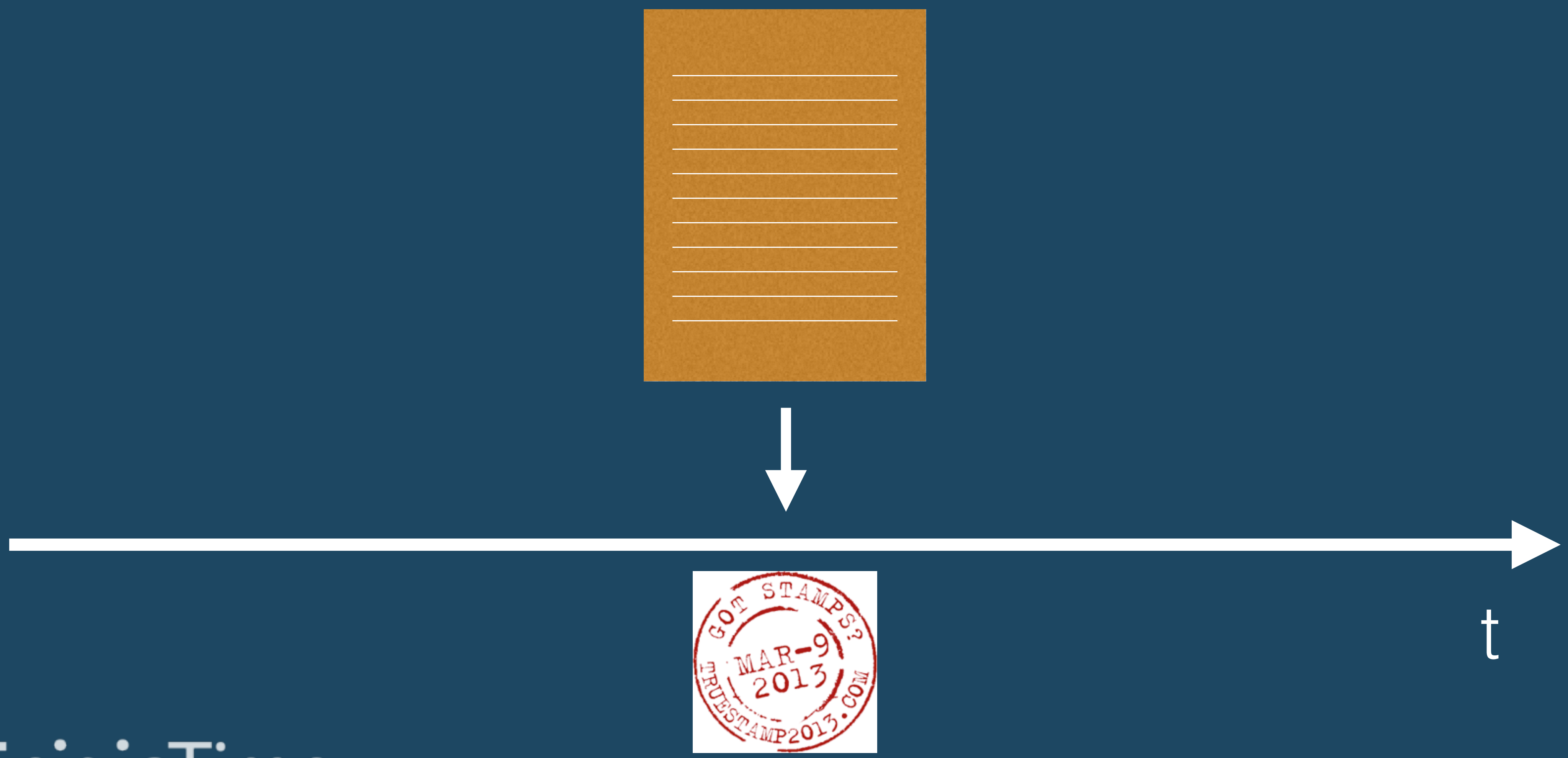
how to build a block chain?

- One way hash functions are used to create cryptographic checksums
- Blocks of similar sizes are populated with specific business data and sealed at regular intervals
- Each block contains a link to the previous block by means of including it’s checksum
- To lock each block in time, an irrevocable ”public ledger” is used.

EnigioTime

timestamp

- A timestamp is used for proving **existence** of data in time and preservation of **integrity**



integrity of data in time

- By using block chain technology we can guarantee existence, integrity and sequence in time

★ **It is thus possible to create a qualified timestamp without using a certificate**

- Data integrity is mathematically ”carved in stone” by means of the publicly verifiable cryptographic checksums that verify the entire chain

bitcoin

”Bitcoin… I used to think it would never fly.

Now I think, not only will it fly as a currency, but the underlying **Block Chain technology** of crypto currencies is a core part of the next generation of the internet that is radically going to transform not just commerce and the nature of the corporation, but many of our institutions in society,
and everyone needs to pay attention to this.”

– Don Tapscott (dec 2014)

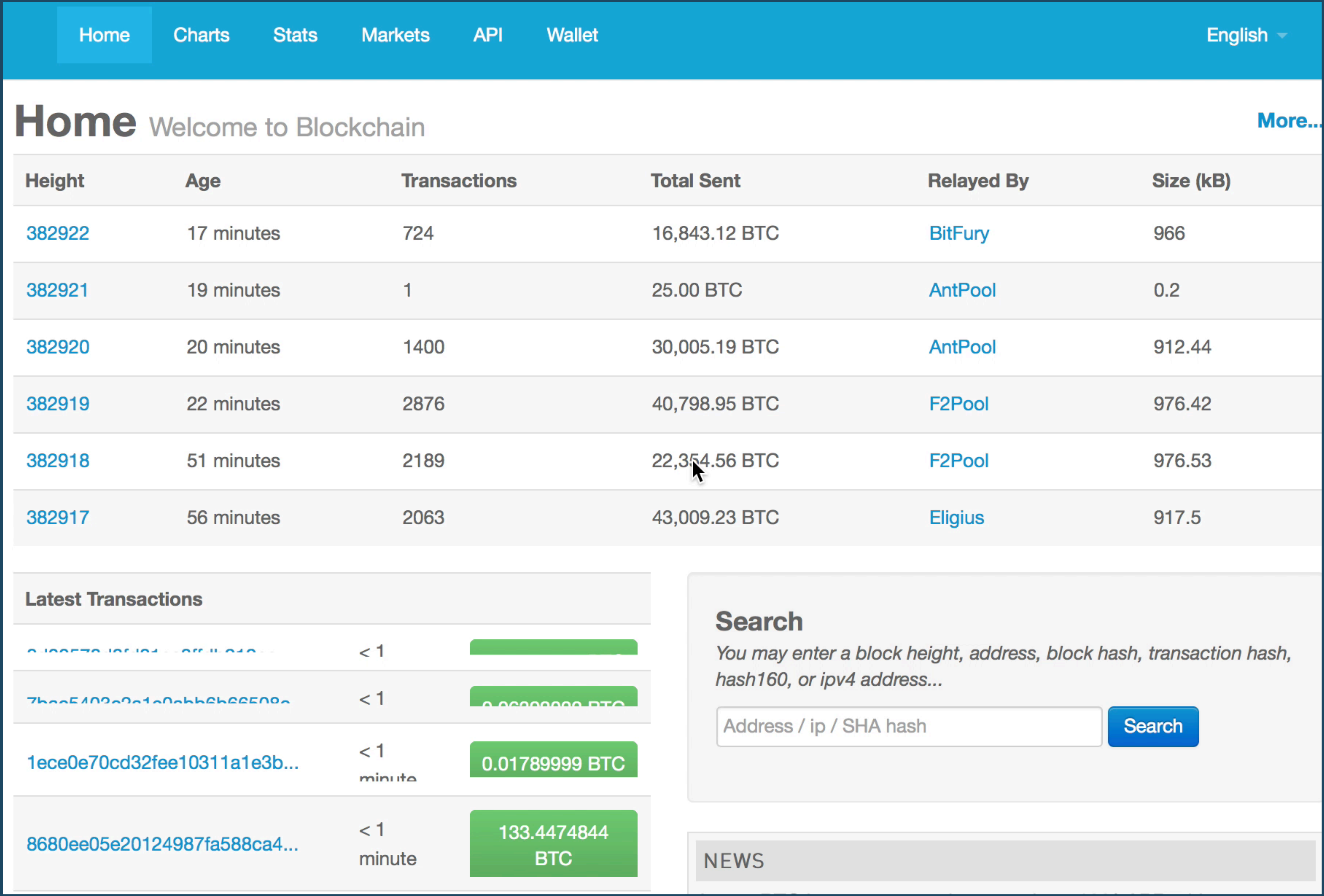
EnigioTime

bitcoin

- Crypto currency with no central authority
- All proof of integrity and authenticity is managed within the massively replicated open transaction ledger that can be validated and verified via mathematics, by anyone
- A bitcoin block is sealed approx. each 10 min

bitcoin miners

- At the end of each block a competition is held for the ”best” hash value in order to seal the block
- A bitcoin block’s hash value is considered better the more leading zeroes it has
  - Ex) 00000000000000000182712fe519775227b06a15459b846c15b6115e0284b25d
- In order to win a contest, massive amounts of computing power is required
- The winning ”miner” receives 25 BTC + transaction fees



Home Welcome to Blockchain

More...

Height	Age	Transactions	Total Sent	Relayed By	Size (kB)
382922	17 minutes	724	16,843.12 BTC	BitFury	966
382921	19 minutes	1	25.00 BTC	AntPool	0.2
382920	20 minutes	1400	30,005.19 BTC	AntPool	912.44
382919	22 minutes	2876	40,798.95 BTC	F2Pool	976.42
382918	51 minutes	2189	22,354.56 BTC	F2Pool	976.53
382917	56 minutes	2063	43,009.23 BTC	Eligius	917.5

Latest Transactions

[illegible]	< 1	[illegible]
7bae5403e2a1e0abb6b66508e	< 1	0.06299999 BTC
1ece0e70cd32fee10311a1e3b...	< 1 minute	0.01789999 BTC
8680ee05e20124987fa588ca4...	< 1 minute	133.4474844 BTC

Search

You may enter a block height, address, block hash, transaction hash, hash160, or ipv4 address...

the solution?

how to maintain integrity of digital data with a block chain?

- The existens of records and its metadata could be timestamped via block chain technology during the whole process of ”becoming” or more traditionally during the whole ”life-cycle”

- More specifically for archiving at the moment of ingestion

- Records and metadata will in this way always maintain integrity in time.

- Data access and modifications will also be secured in time without keys, certificates or reliance on trust. Anyone can always validate the integrity of the chain.

- Full integrity and traceability can be maintained no matter where the data itself is stored

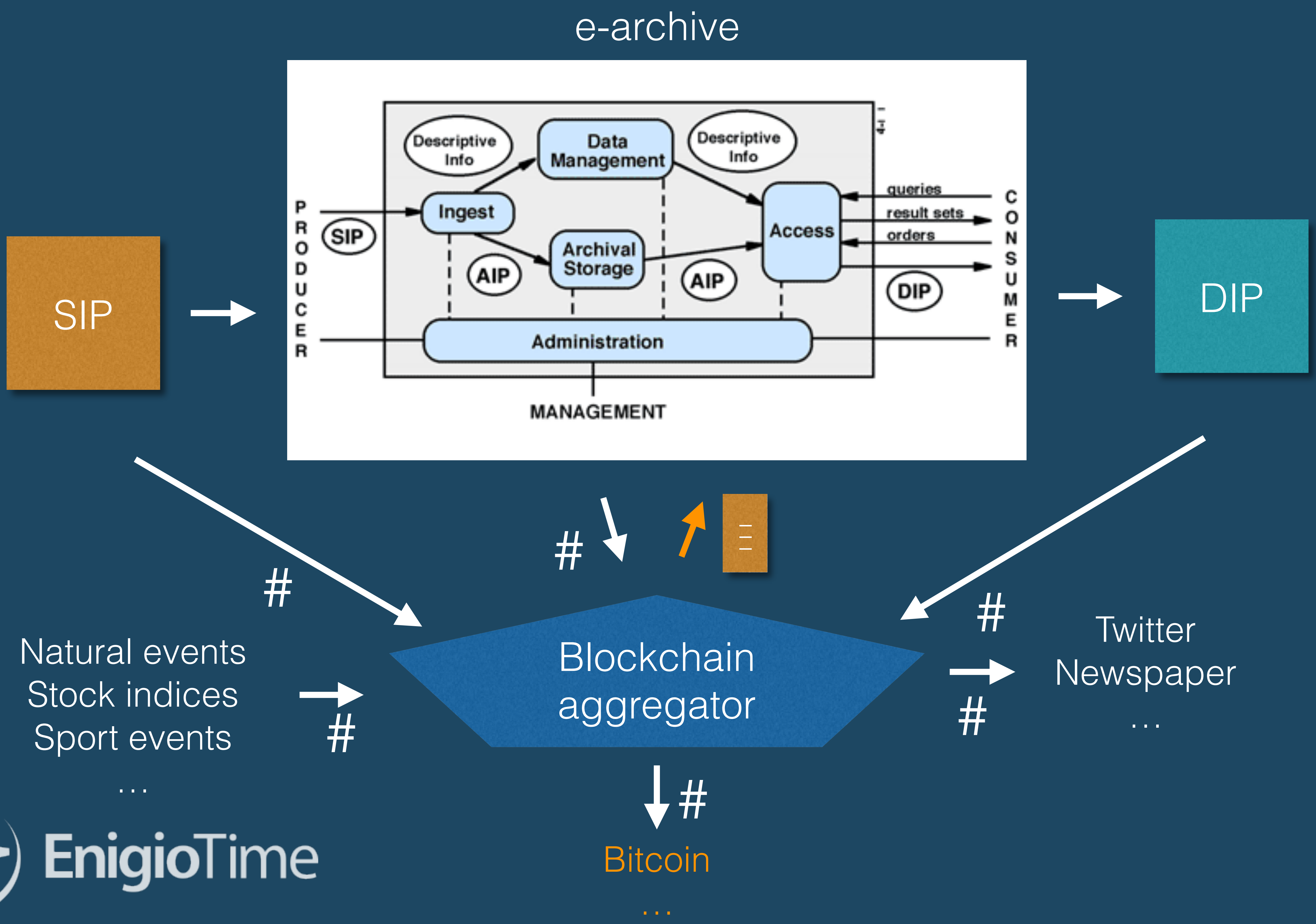
EnigioTime

the data and time

- A timestamp via a ”linked scheme” is not something that needs to be stored with the data. It is not necessarily ”archived”.
- We can save a ”timestamp” as metadata within the data set being ”stamped” but the proof is not with the data, the ”linked scheme” contains the proof.
  - You may archive ”the chain” from your data to the ”public ledger”
- The ”integrity in time” of the data becomes a ”fact” of the data that can not be altered! The linked scheme will be ingrained in the ”Cloud” and other physical publication channels.

EnigioTime

OAIS e-archive solutions integrated with a blockchain aggregator



e-archive

SIP

DIP

#

#

Natural events
Stock indices
Sport events
…

#

Blockchain aggregator

#

#

Twitter
Newspaper
…

#

Bitcoin
…

EnigioTime

why a block chain aggregator?

More redundancy	several channels and references
More conveniency	easier than to build blockchain publication ”in-house”
Higher granularity	the proof can be more precise
Powerful traceability	easier to verify proof
Monitoring	continuously validating the chain of proof and alert if integrity would be compromised

local block chain aggregation

- If frequent updates and additions (e.g. in a business system or middle archive) need a timestamp, communication to external block chain aggregator might be extensive and induce too large data traffic

- By using local block chain aggregation within the system, the granularity of timestamps at the external block chain could be reduced while still keeping an intact integrity and traceability

how about authenticity?

- Timestamping should be used as early as possible! Preferably at data creation, modification and preservation.
- Timestamping ties metadata to their records
- Making sure provenance is secured as metadata at data creation

→ Thus, we add a chain of proof and traceability that helps solving and securing both authenticity and integrity for the record.

EnigioTime

- but isn’t the blockchain aggregator really a trusted third party, similar to the CA?

- The output of the blockchain aggregator is always verifiable
- Verification and proof of integrity of the data is independent of the blockchain aggregator
- Only cryptographic checksums are sent to the blockchain aggregator, no sensitive data
- The blockchain aggregator is only required for aggregation and distribution of cryptographic checksums
- A receipt, representing the ”chain of proof”, is returned from the blockchain aggregator

is this established?

- Bit Coin is completely depending on blockchain technology and isn’t ruled by any authority or trusted institution. All currency transactions are secured within the blockchain itself.

- Linked schemes are covered in some existing standards and regulations but not yet widely adopted

  - e.g. ISO 18014-3 and X9.95

  - eIDAS regulations will accept linked schemes as qualified (will be in force July 1, 2016)

- Block chain aggregators might help to facilitate a wider adoptions to those modern standards for use in records management

can we forget about certificates in records keeping?

- We do not need certificates for securing integrity of data connected to a specific time, i.e. for creating qualified electronic timestamps

- However, a significant amount of documents are still digitally signed using certificates which means that we still have a preservation challenge for expiring certificates

how about LTV?

- Long Term Validation (LTV) is a concept originating from the PDF standard ISO 32000-1.
- Included in the European PAdES standard as well as Adobe products and some others
- ”LTV enabled” means that all information necessary to validate the file (minus root certs) is embedded.
- It is achieved by storing all certificates as well as up-to-date CRLs inside the DSS (Document Security Store), secured with a qualified timestamp that protects the authenticity of all data.
- Is it possible to verify the validity of the LTV signature later in time or do you have to Trust the original validation from when the LTV signature was created?

EnigioTime

can we preserve the valid signature without the certificate?

- One of the problems with preserving the signature is the practice of revalidating it continuously before the certificate expires with a new seal using a new certificate that will expire.

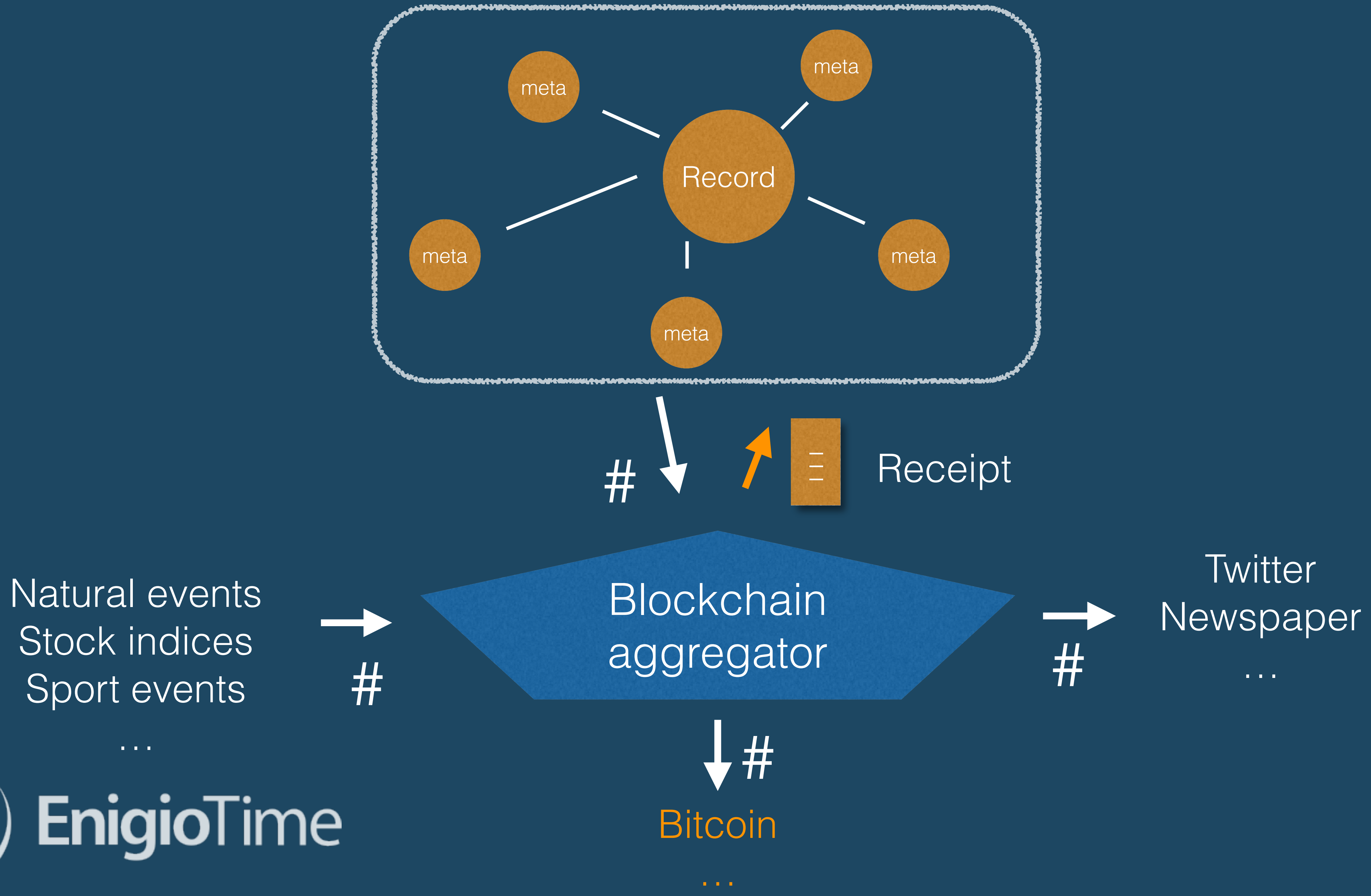
- With a timestamp based on a ”linked scheme” we prolong the issue of revalidation to the point where the cryptographics of the hash-function used might be compromised.

- Even if the hash-function would no longer be considered strong, the possibility to ”back-date” anything would still be considered impossible, as the linked scheme has created a network of dependencies that strongly secures the integrity of the chain of proof.

EnigioTime

example of how we create timestamps using a ”linked scheme”

How to timestamp a data set with metadata



meta

meta

Record

meta

meta

meta

#

Receipt

Natural events
Stock indices
Sport events
…

#

Blockchain
aggregator

#

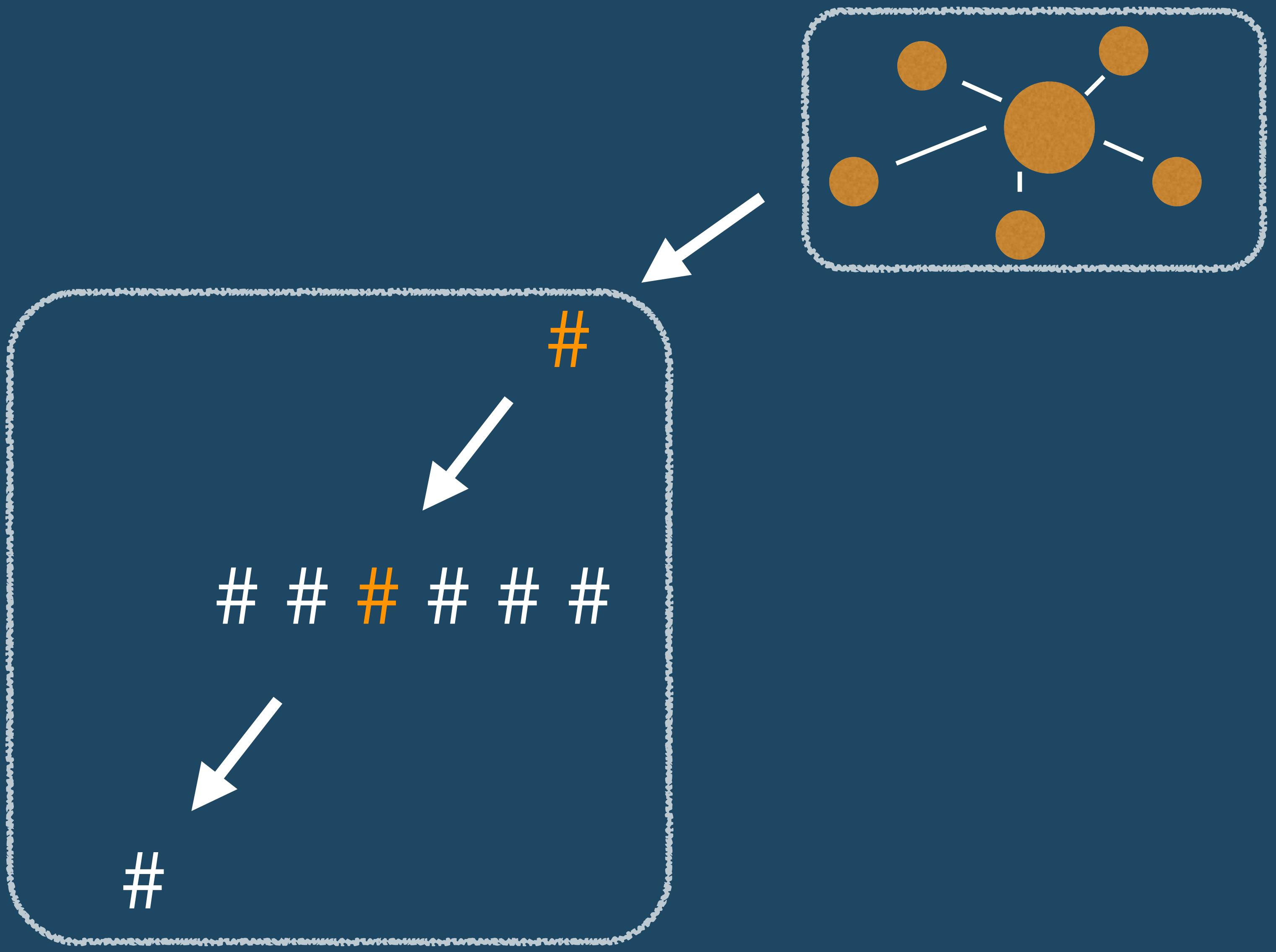
Twitter
Newspaper
…

#

Bitcoin
…

EnigioTime

Chain of proof -”Receipt”



Twitter
Newspaper
…

EnigioTime

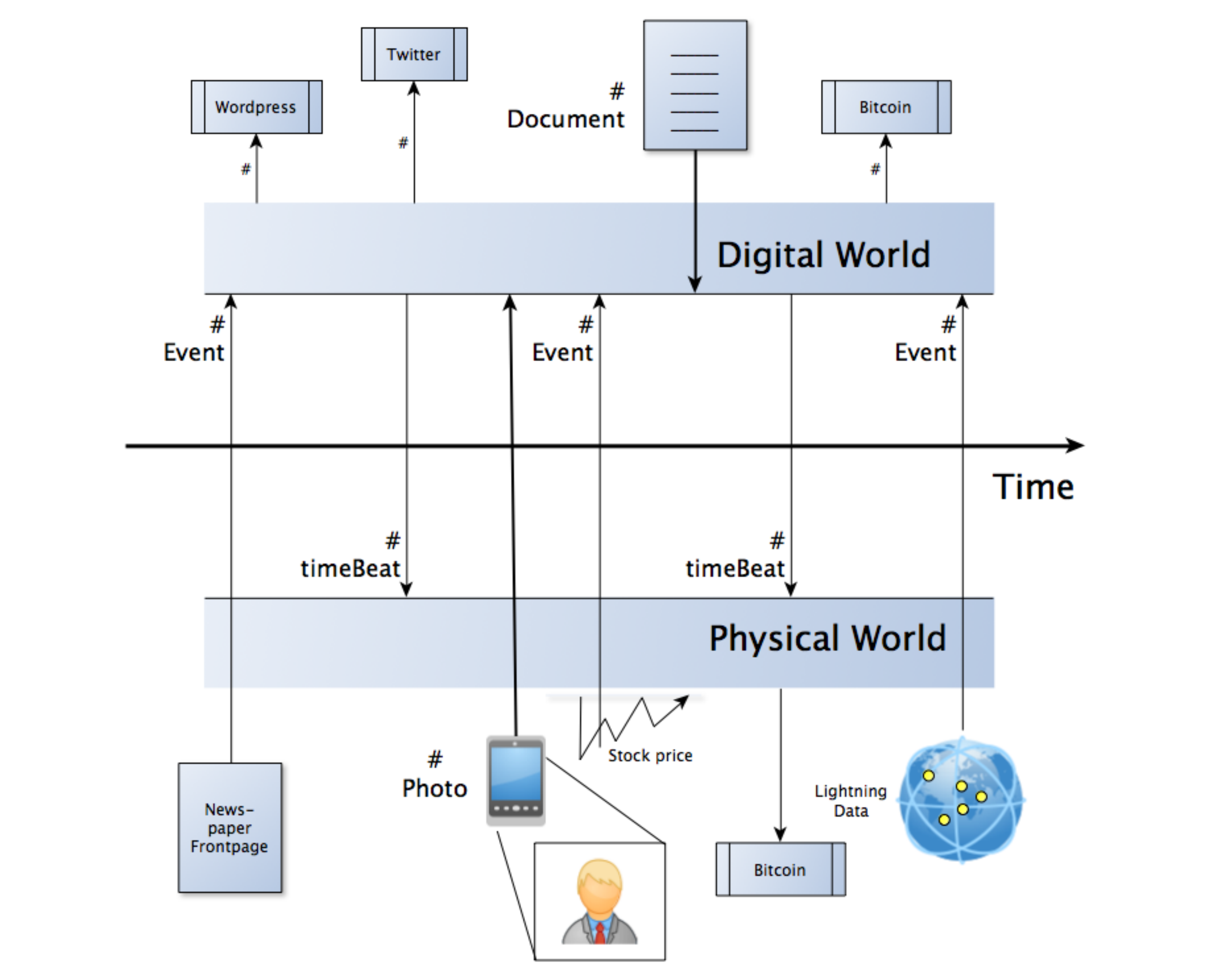
time:beat

- Enigio patent in Sweden, approved PCT application and other national patents pending

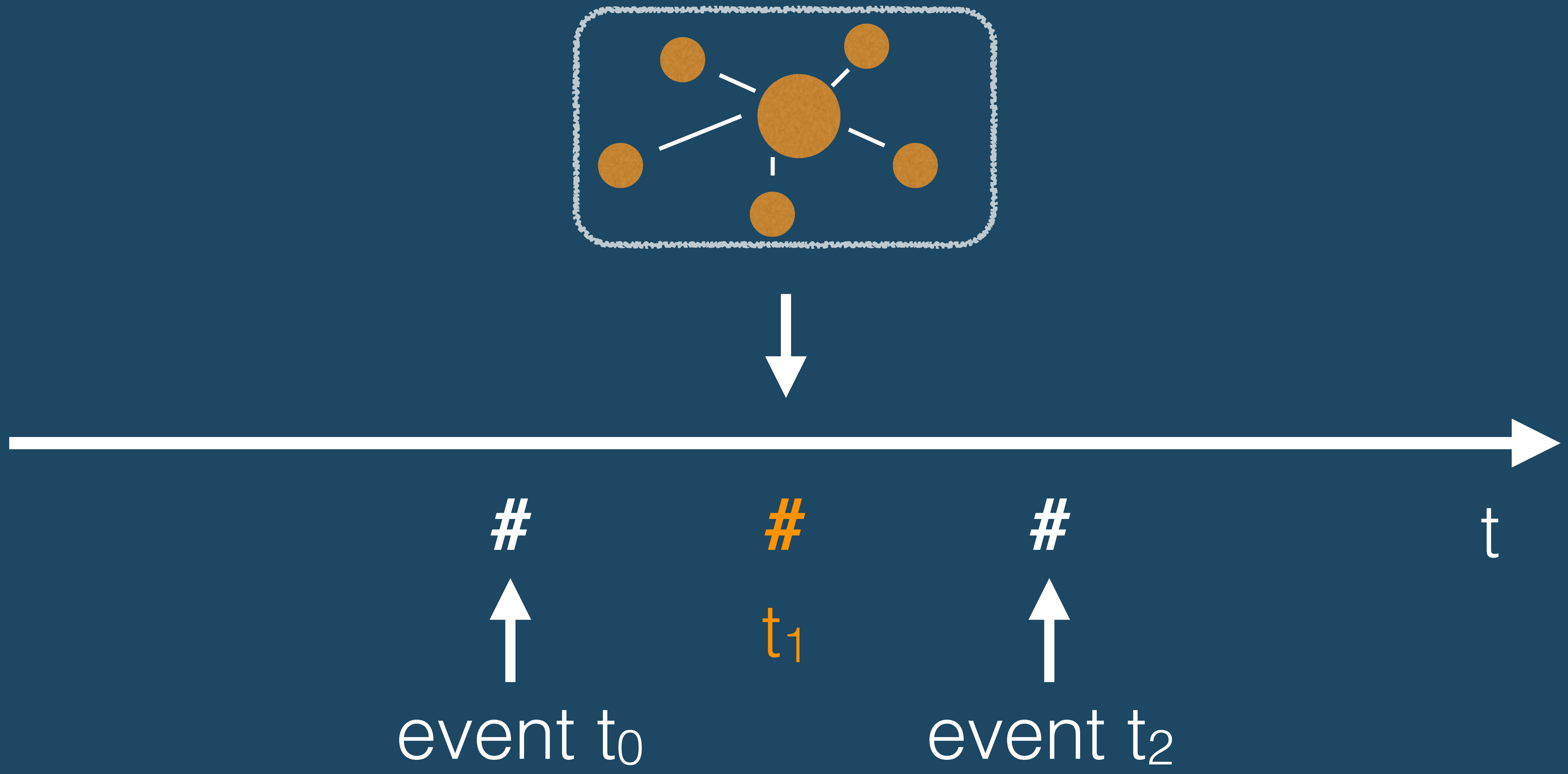
- To further secure the ”public ledger” in a linked scheme or block chain we introduce ”real world” events that have large consensus and cannot be predicted.

- We introduce other input streams to the block chain to secure time; like stock indices, sport results, headline news on top new papers, natural phenomena etc.

time:beat example



ex. timestamp with time:beat



#

#

#

t

t_1

event t_0

event t_2

EnigioTime

time:beat

Teamwork

SWOT analysis in teams

- SWOT on the statement ”The use of block chain technology for long term preservation of data”
    - Discuss and write notes on Strengths, Weaknesses, Opportunities and Threats related to the statement above and the concepts we have described!
    - Mark each note with S, W, O or T
- Teamwork 15 min
- Presentation and discussions

EnigioTime

Summary

EnigioTime

Questions?

EnigioTime