Eternity Wall

Agenda

- Timestamping
- OpenTimestamps

Timestamping

- **What's timestamping?**
- How we can use the Blockchain for timestamping?
- Why Blockchain?

What's timestamping?

- Giving a certain date to a document
  - Eg. postmark of the postal office
  - It doesn't help if the stamp is on the envelope
- Civil law requires dates on important document must be made by public official
  - Eg. from the notary if we are buying a house
- What about digital documents?

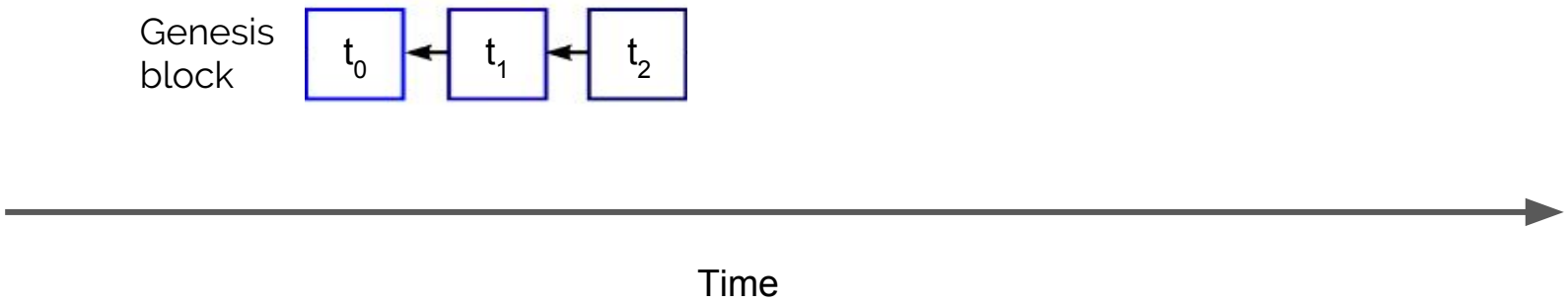
What's digital timestamping?

- Based on digital signature of a third party
- Based on certification authority
    - Eg. Italian PEC

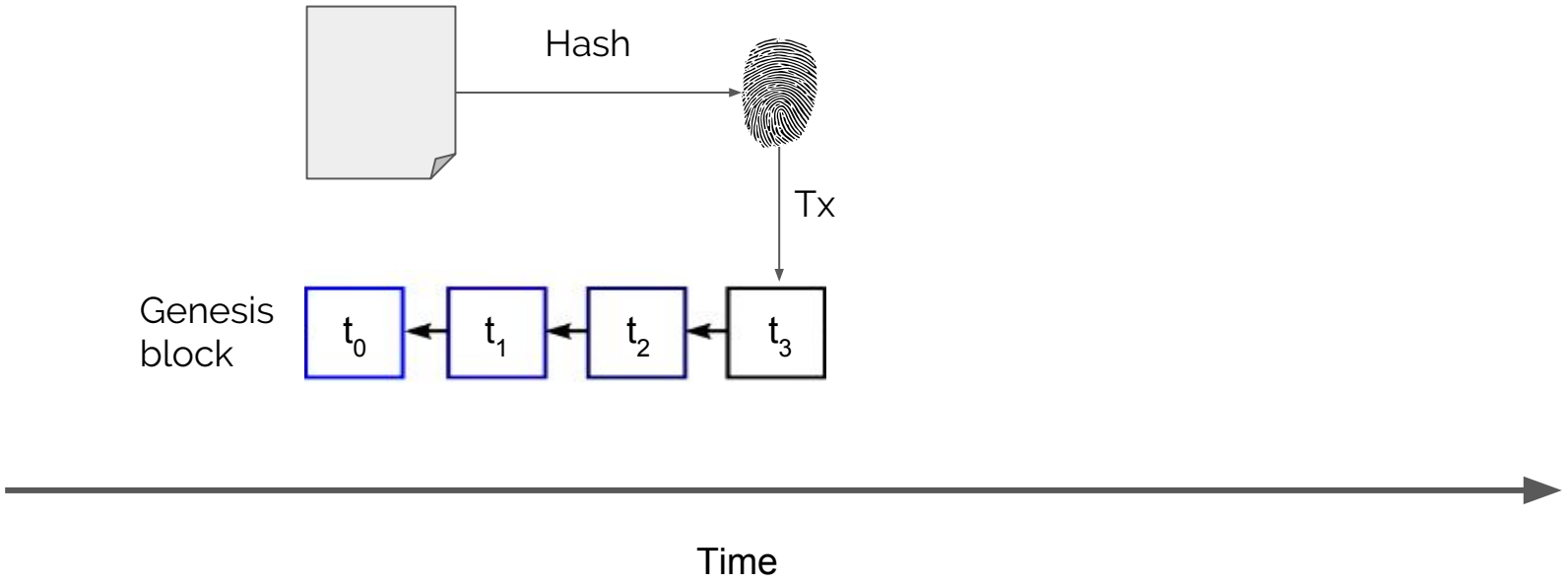
Timestamping

- What's timestamping?
- **How we can use the Blockchain for timestamping?**
- Why Blockchain?

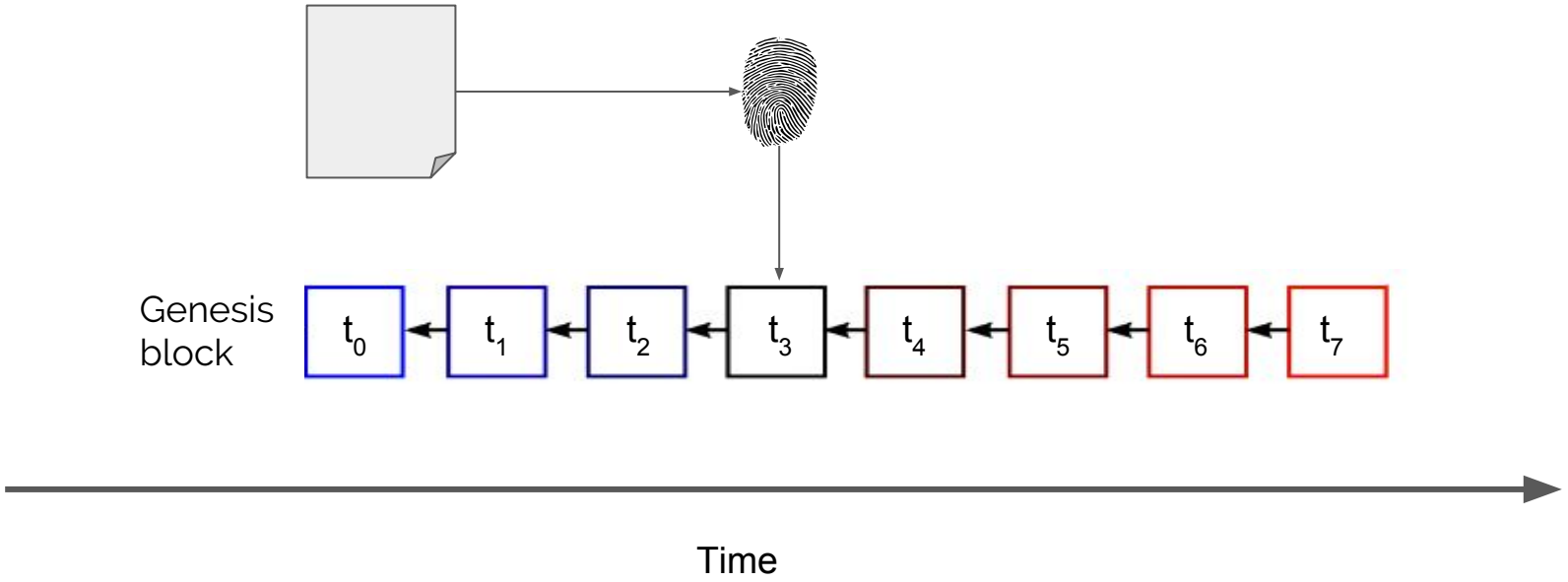
How we can use Blockchain for timestamping?



How we can use Blockchain for timestamping?



How we can use Blockchain for timestamping?



Timestamping

- What's timestamping?
- How we can use the Blockchain for timestamping?
- **Why Blockchain?**

Why Blockchain?

- Digital timestamping
  - Require third party (trusted timestamping)
    - Increase costs
  - Requires digital signature which requires to store a secret
    - Increase risks

Timestamping with digital signature

What if the timestamper's private key is stolen?

The key revocation certificate is issued and timestamps after the theft are considered invalid

Timestamping with digital signature

What if the timestamper's private key is stolen?

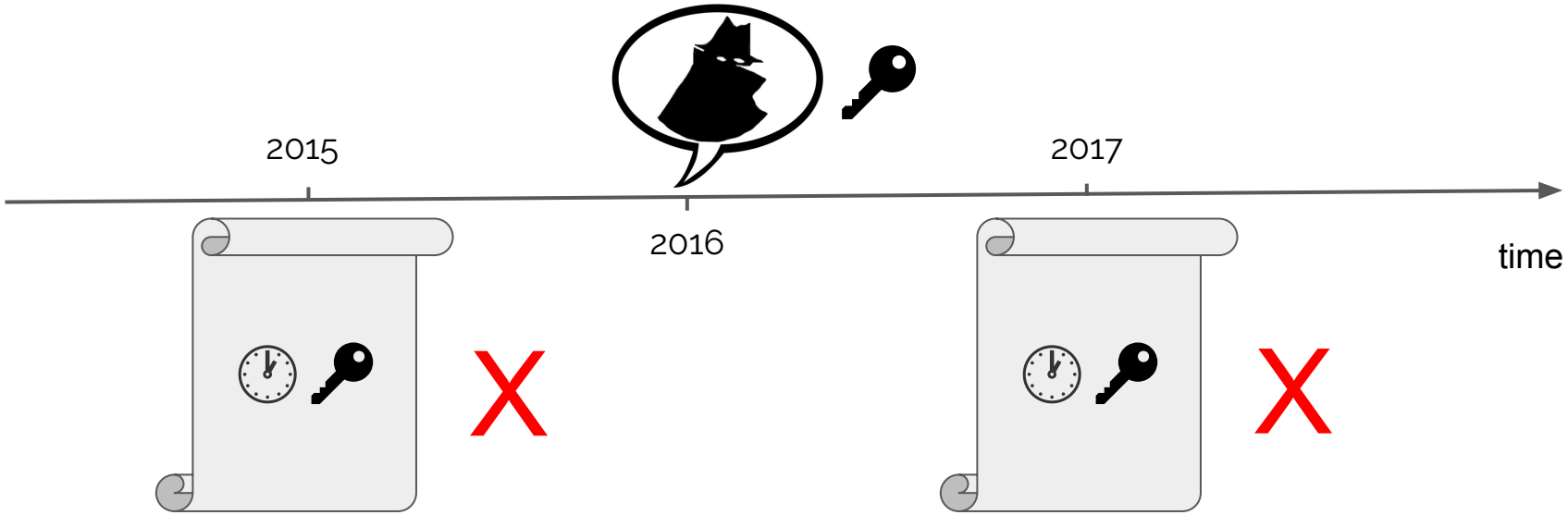
The key revocation certificate is issued and timestamps after the theft are considered invalid

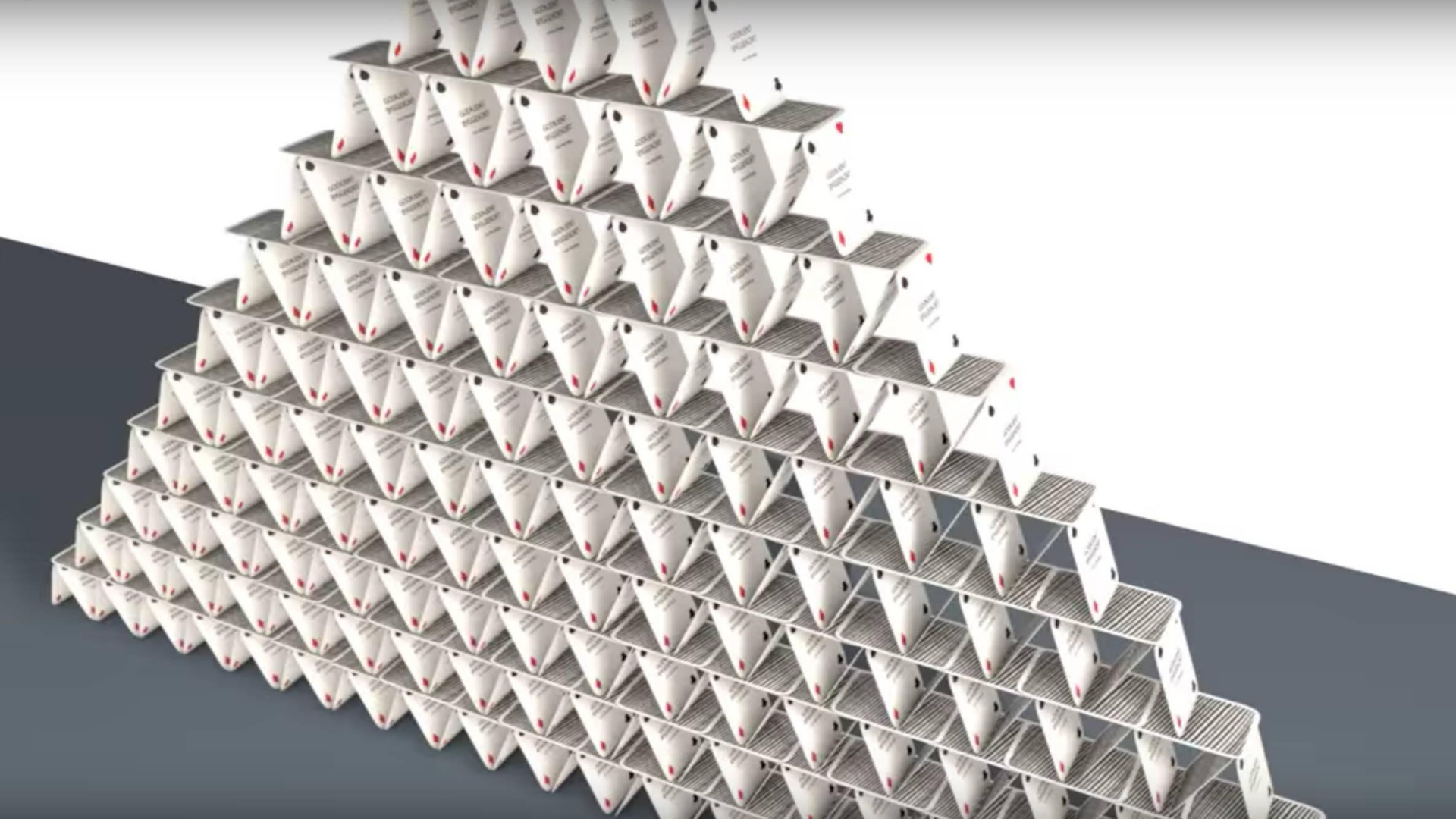
WRONG

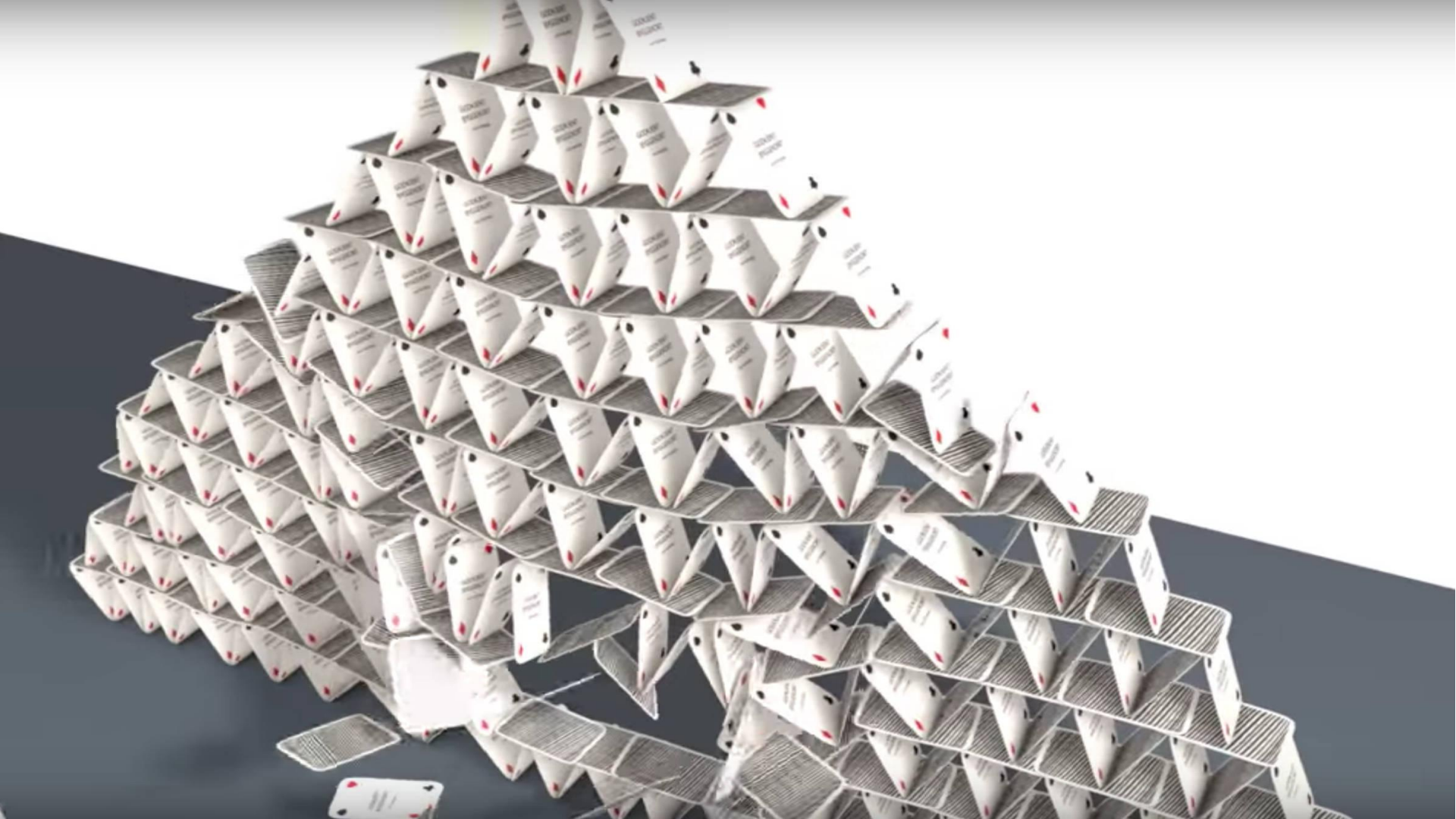
Every timestamp created by that key has to be considered invalid because the thief can backdate timestamps

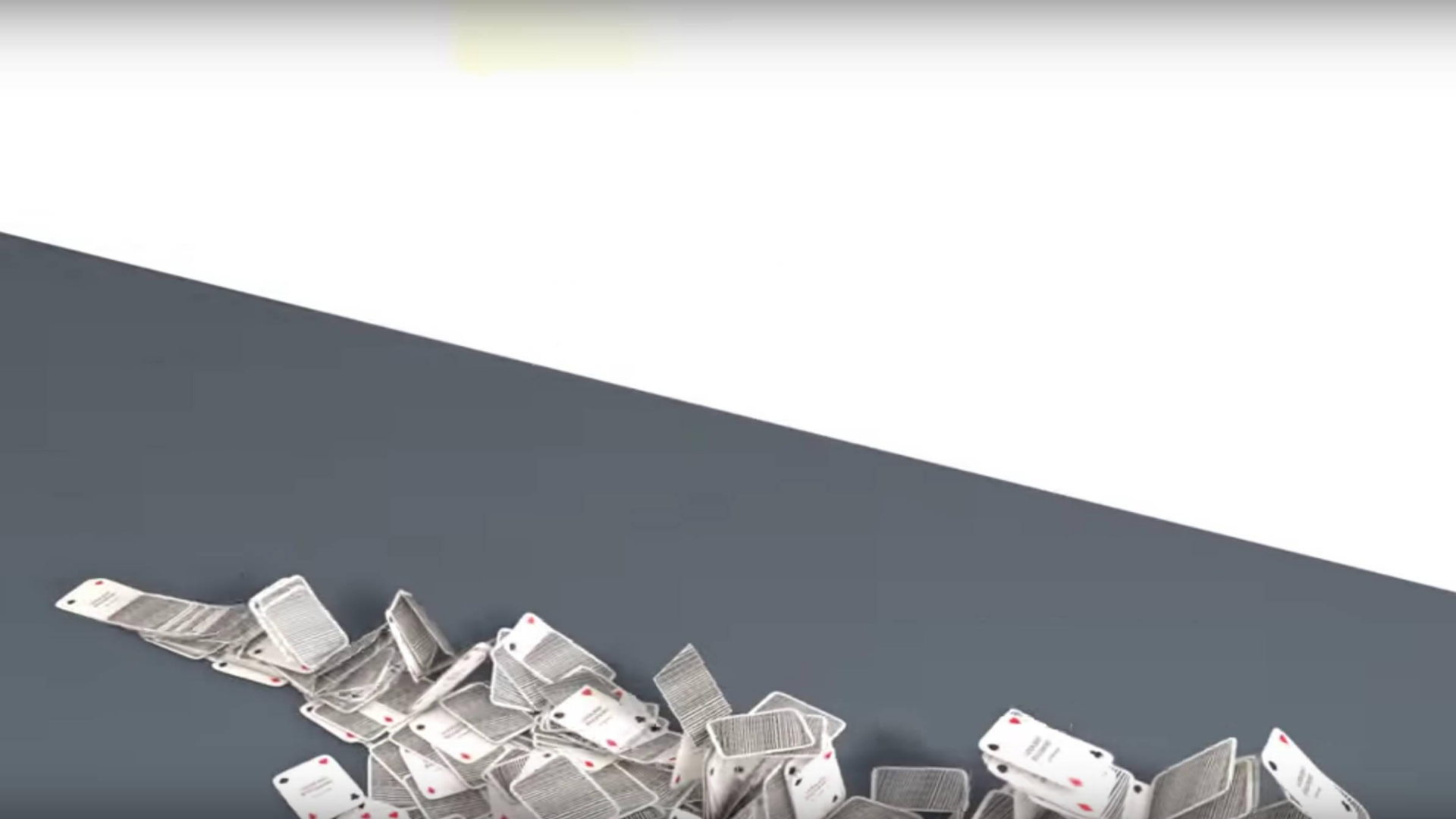
Digitally signed timestamps are as safe as the signing key

Timestamping with digital signature









Trustless timestamping

- Does not require trust in the stamper because client could verify by himself and prove timestamp to others
- Does not require a secret
- If you look closely, a lot of problems could be solved by Timestamping:
  - Improving Digital Signature
  - Supply chain, Healthcare
  - InfoSec, Legal, Insurance, Safe storage
  - ...
  - RegTech, we already worked on this

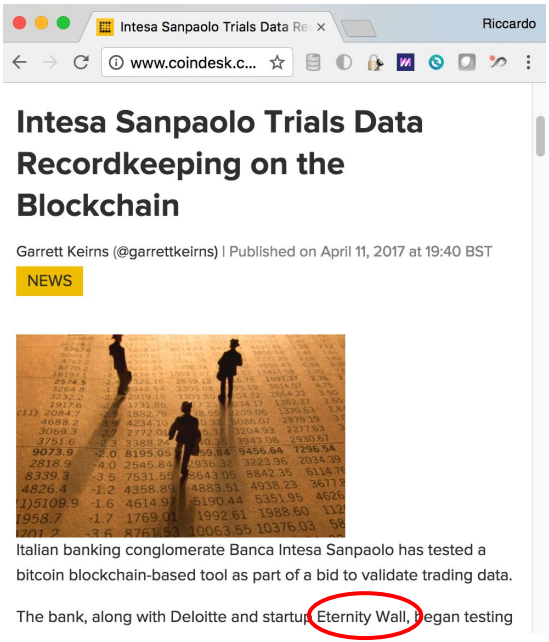
Regulators use case

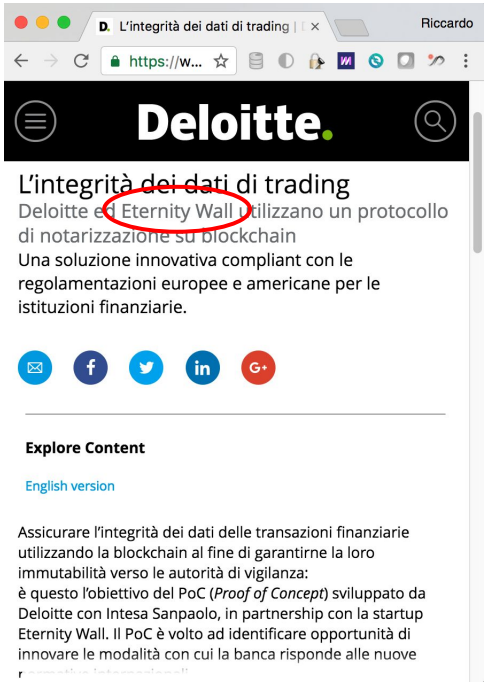
- Dodd-Frank requires trade reconstruction data to be stored on supports satisfying some properties
  - WORM Write Once Read Many
  - Anti tamper

- Today, regulated entities use third party services relying on security by certification authority and digital signature
  - NB Does not solve double spend

Regulators use case

By trustless timestamping we achieve the same anti-tamper and WORM property with less operational costs and more security





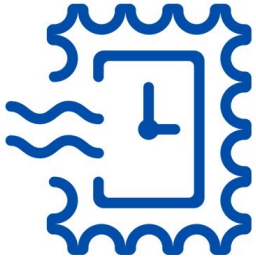
Trustless timestamping

- To answer all this use cases...
- We are working to propose a standard in timestamping:

Agenda

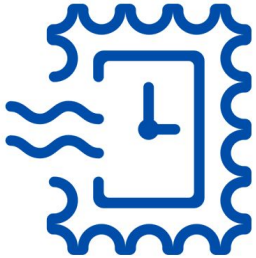
- Timestamping
- **OpenTimestamps**

OpenTimestamps



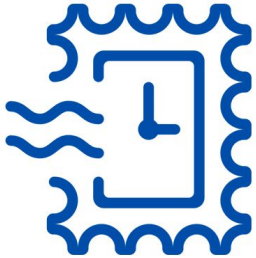
- **What's OpenTimestamps?**
- From one-tx-one-timestamp to Aggregating timestamp (merkle tree)
- Architecture: Blockchain, receipts, clients, calendar servers & backups

OpenTimestamps in a nutshell



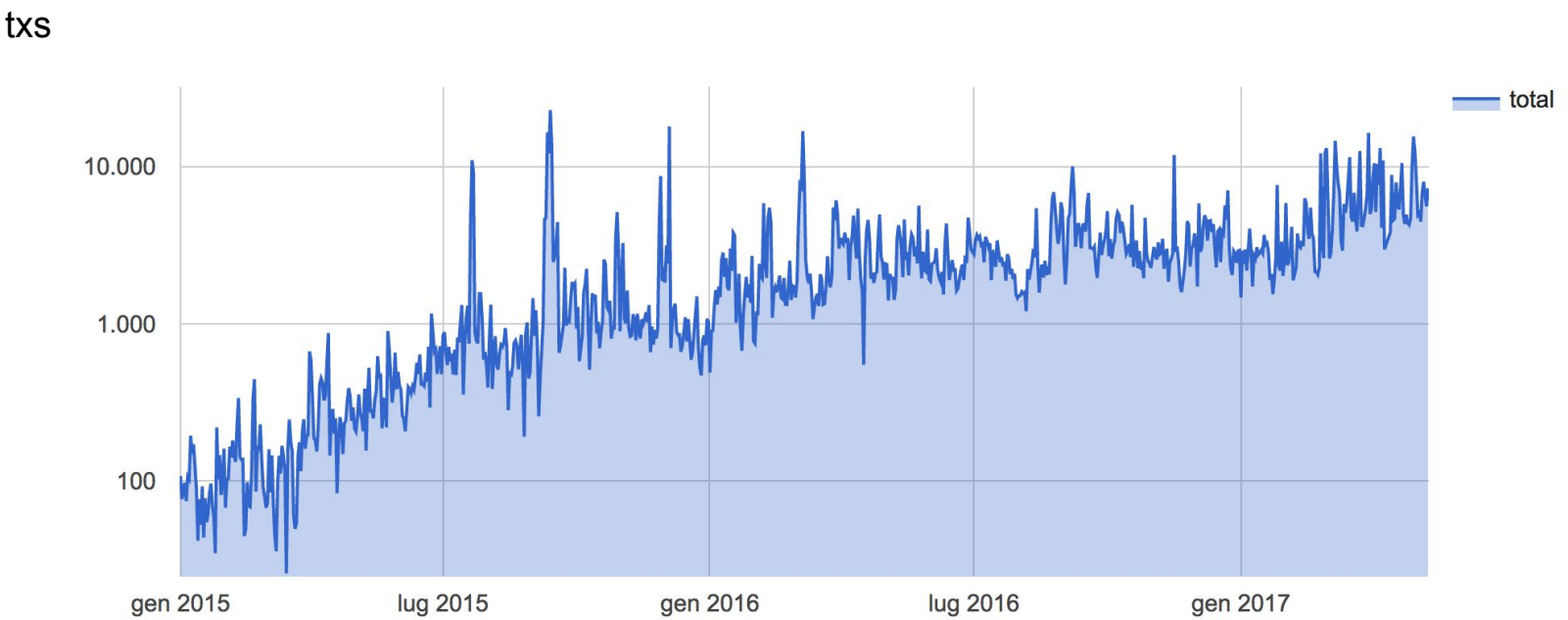
- Blockchain is permissionless
  - Anyone with bitcoin could timestamp something, but:
    - Costs while aggregation
    - Banks have compliance problems
    - Heterogeneous formats lead to tools fragmentations
- OpenTimestamps is a standard way of doing trustless timestamping
  - Proposed by Peter Todd, I am the main contributor, lately Andrew Poelstra and Luca Vaccaro
  - Supports different blockchains
  - Increase startup credibility and reliability as a service provider
- One of the biggest italian bank is using it for Dodd-Frank compliance

OpenTimestamps



- What's OpenTimestamps?
- **From one-tx-one-timestamp to Aggregating timestamp (Merkle tree)**
- Architecture: Blockchain, receipts, clients, calendar servers & backups

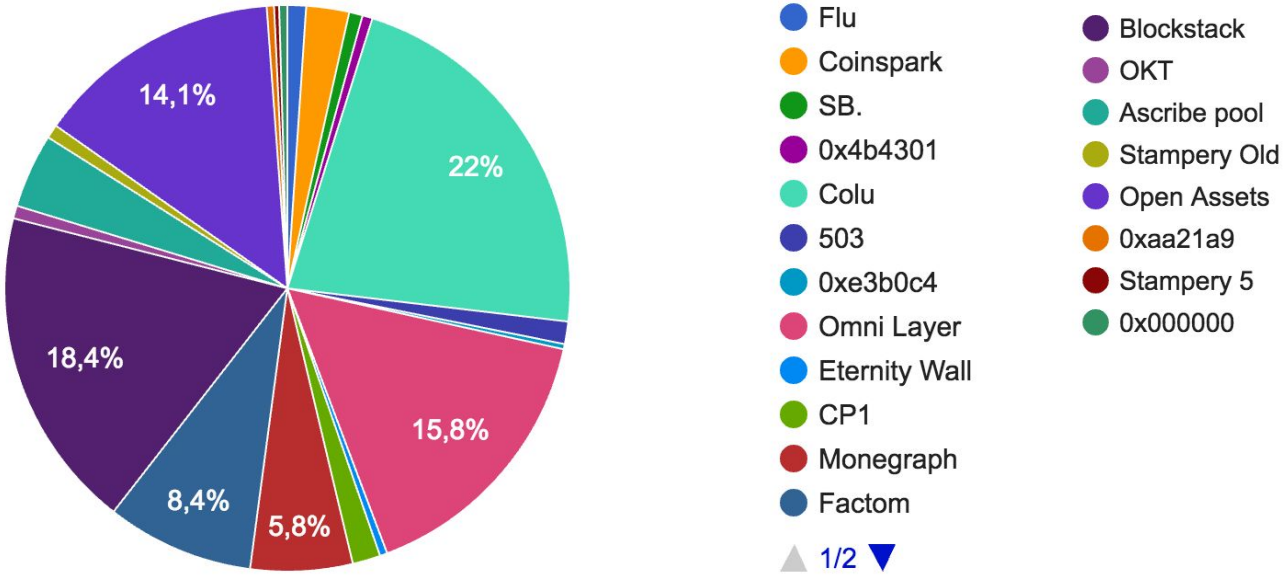
OP_RETURN tx per day



5000
txs/day

http://opreturn.org/

OP_RETURN utilization



http://opreturn.org/

OP_RETURN utilization

~30% for timestamping

http://opreturn.org/

OP_RETURN utilization

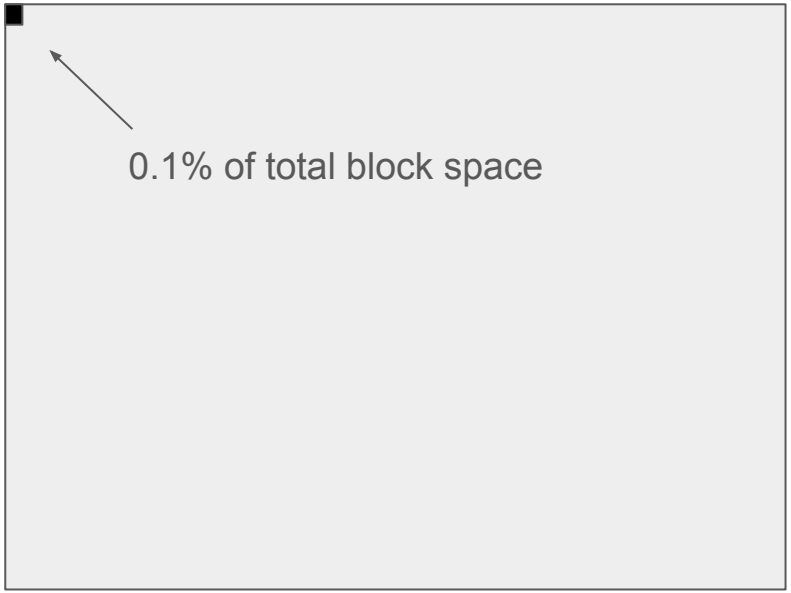
~2000 tx/day
~1000 $/day

http://opreturn.org/

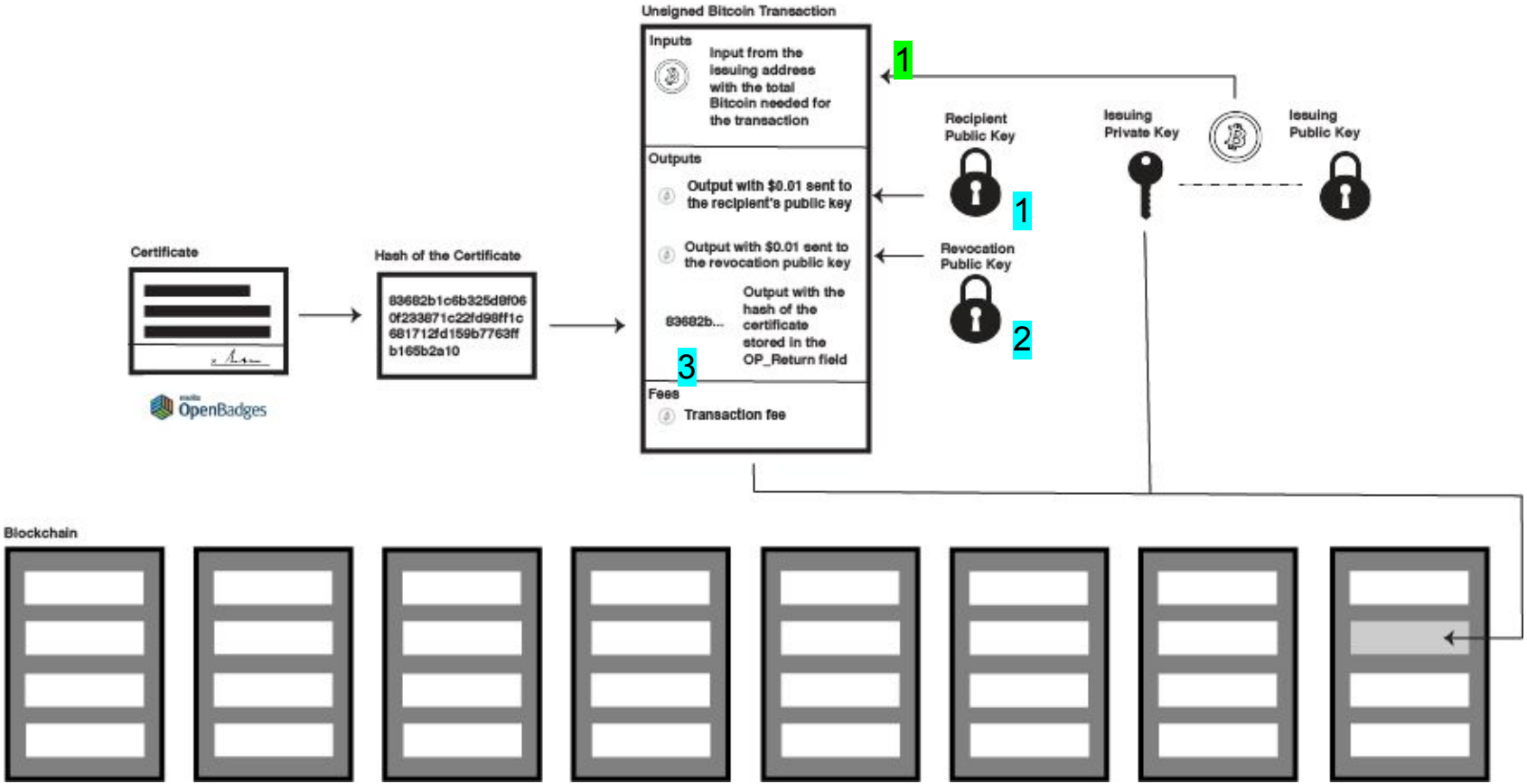
Claim

≈ 200 tx/day for global timestamping needs

- For maximum precision
- Less cost, 1/10 than now
- 0.1% of block

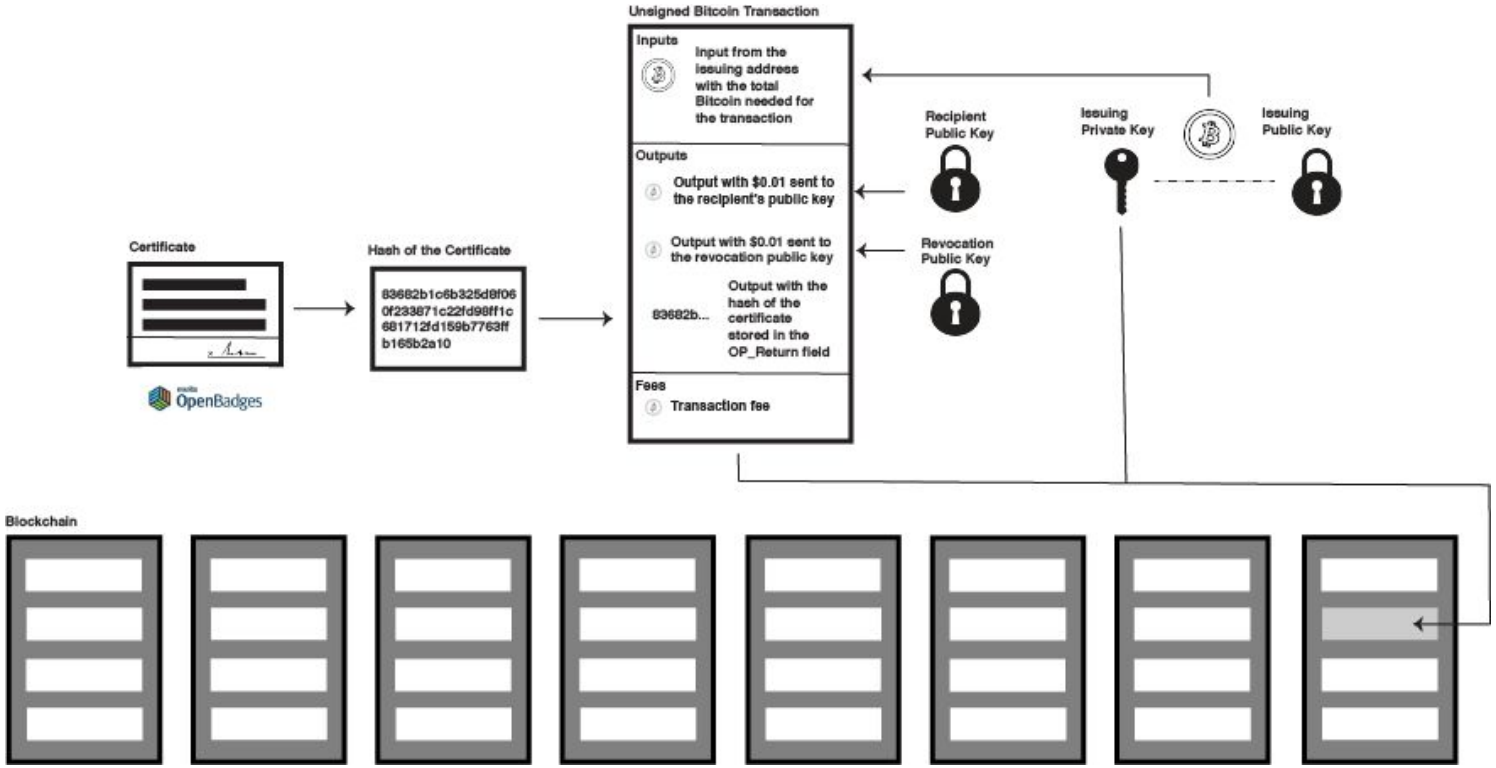


One-certificate-one-transaction



https://medium.com/mit-media-lab/what-we-learned-from-designing-an-academic-certificates-system-on-the-blockchain-34ba5874f196#.xsf1s8hwx

One-certificate-one-transaction

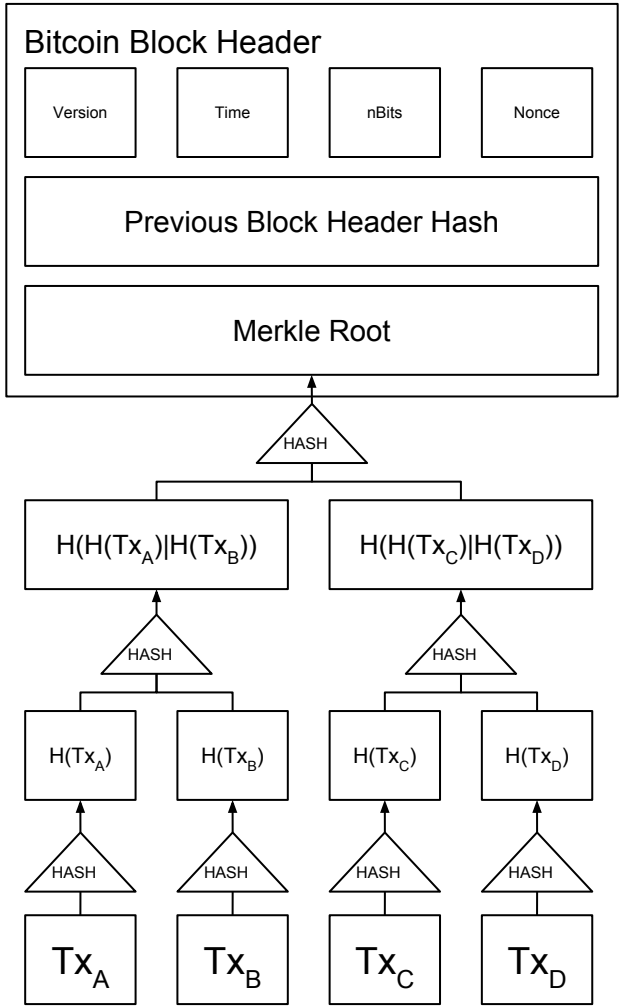


3000 degrees/year * 40 exam/year * 40000 universities ≈ ...

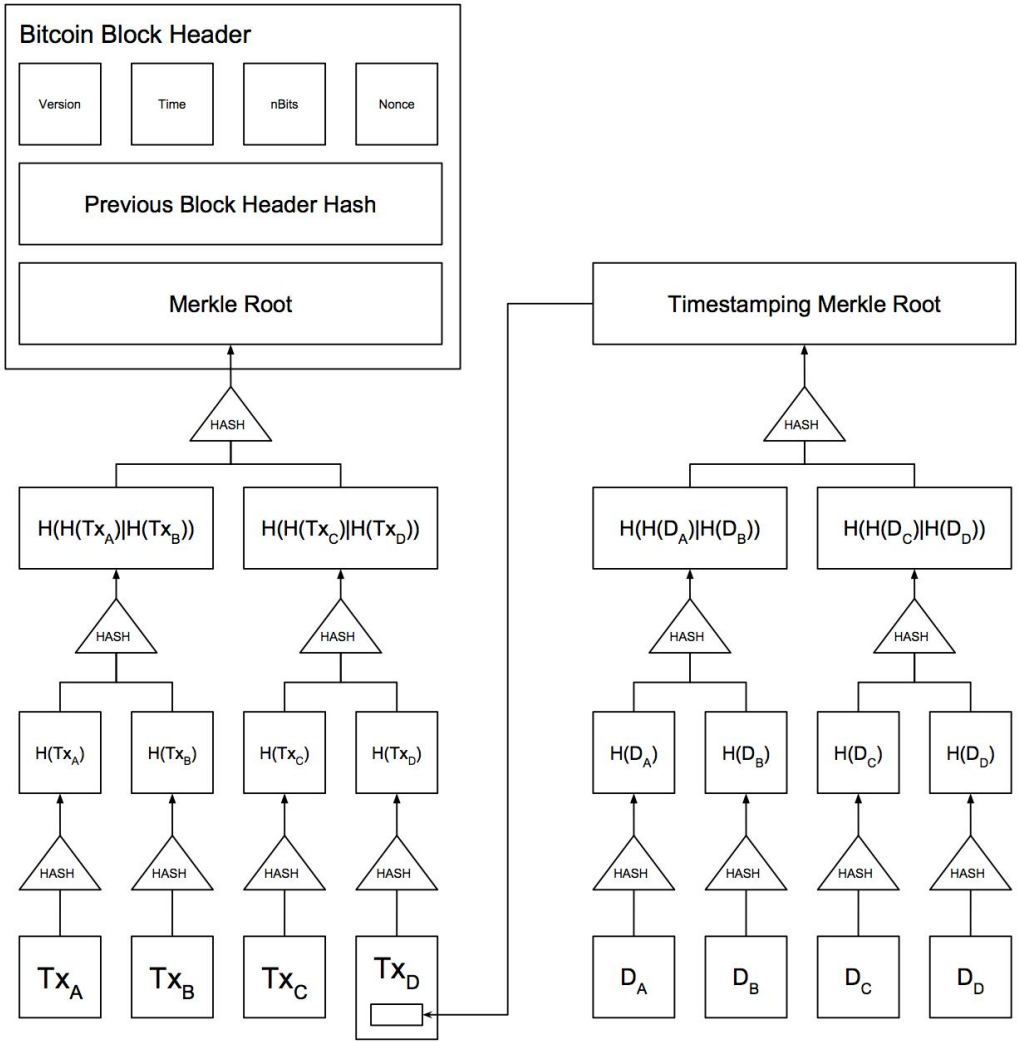
80MB blocks!

We need a Merkle Tree!

Aggregating Timestamps

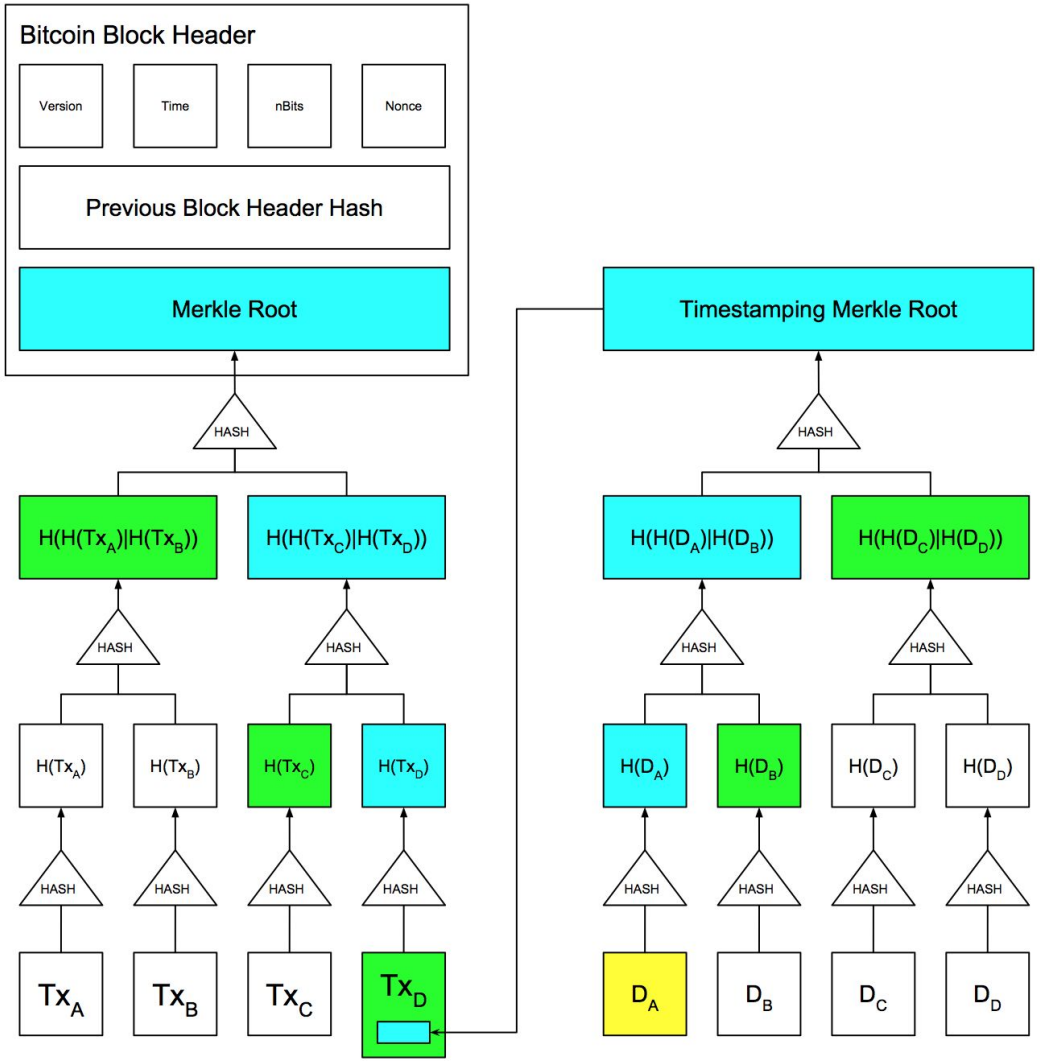


Aggregating Timestamps

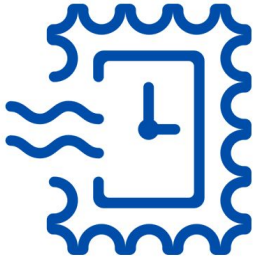


Aggregating Timestamps

✓ scalability

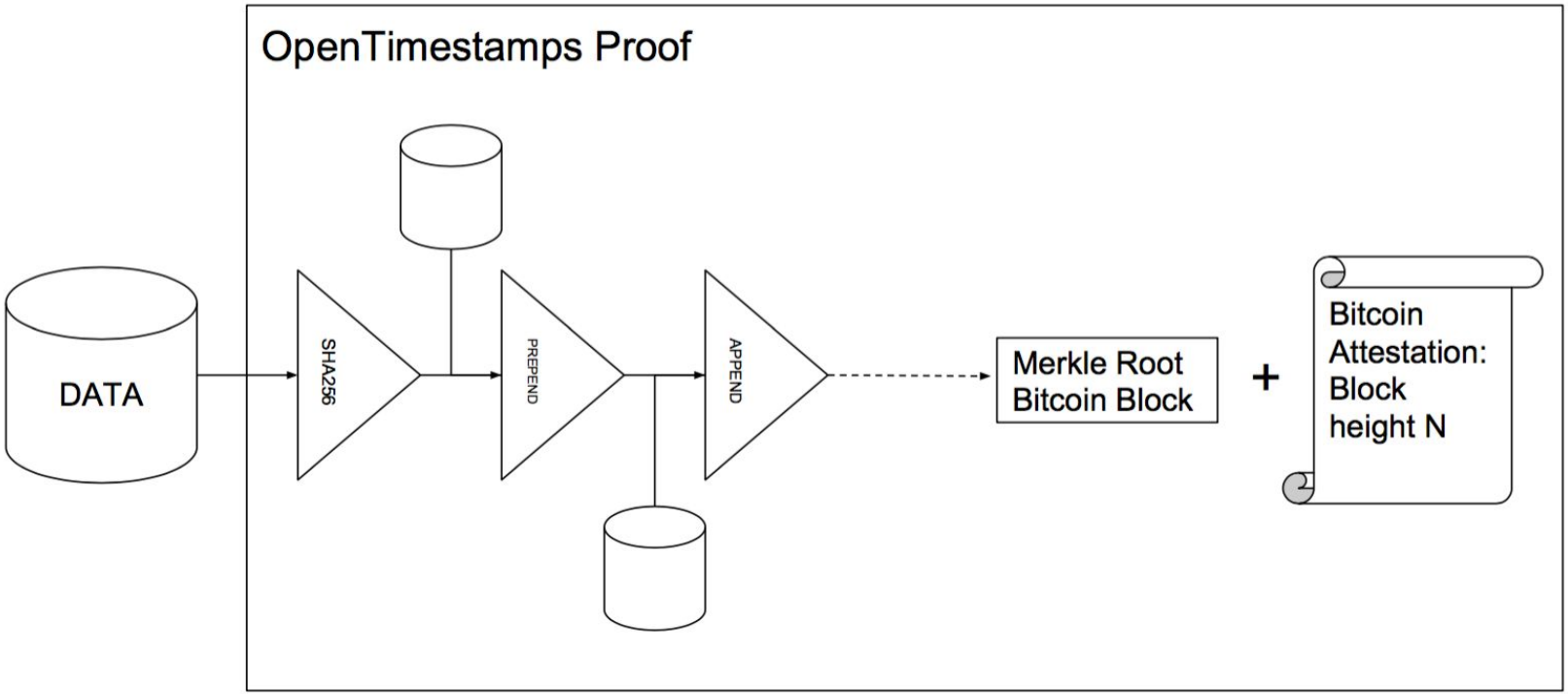


OpenTimestamps



- What's OpenTimestamps?
- From one-tx-one-timestamp to Aggregating timestamp (merkle tree)
- **Architecture: Blockchain, receipts, clients, calendar servers & backups**

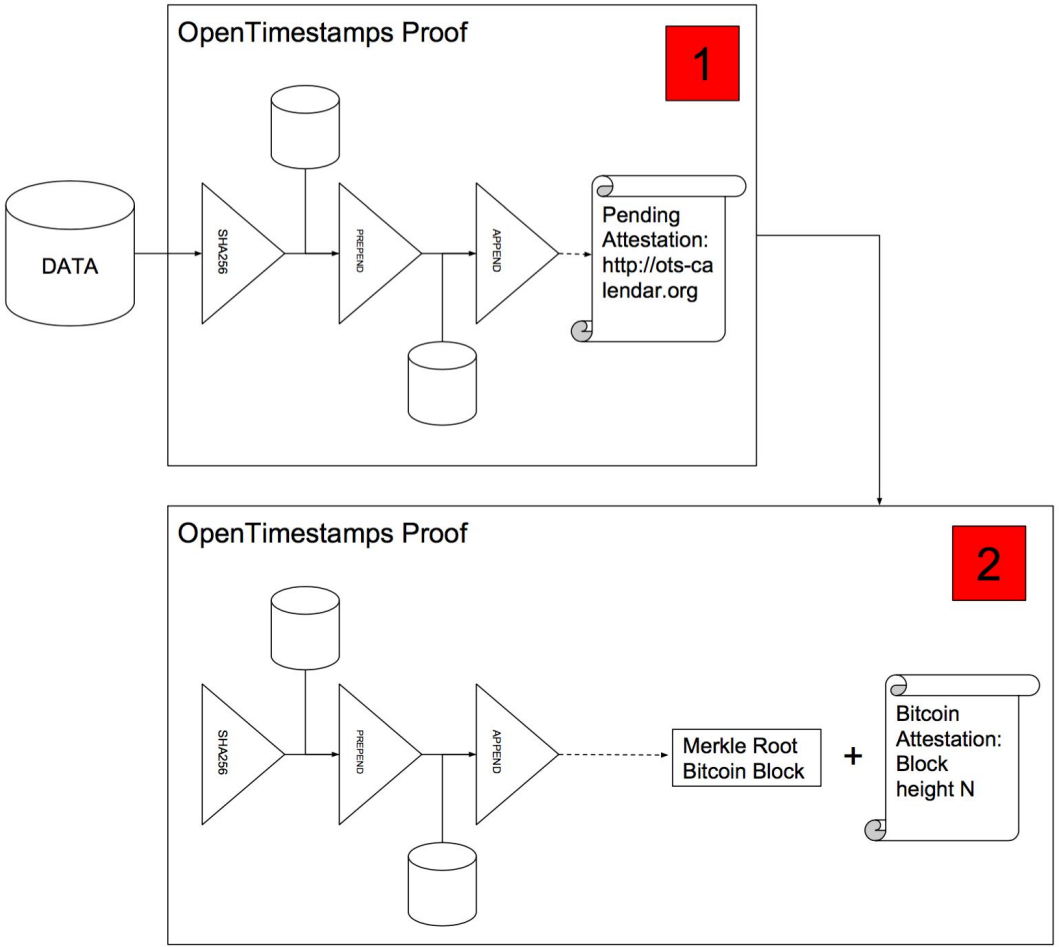
OpenTimestamps



https://opentimestamps.org

OpenTimestamps

Incomplete proof



https://opentimestamps.org

1 - stamp [Doc]

2 - [hash]

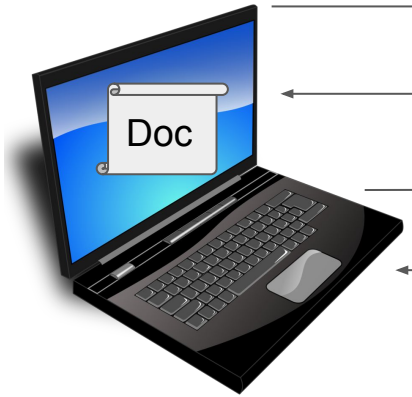
3 - “1 sec merkle tree”

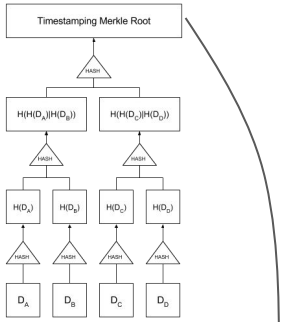
4 - [receipt]

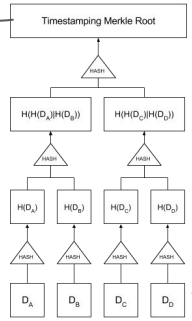
6 - upgrade [receipt]

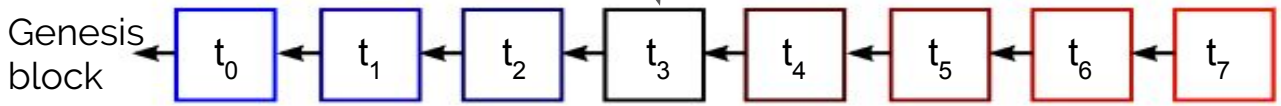
7 - [upgraded receipt]

5 - “merkle root of merkle roots”

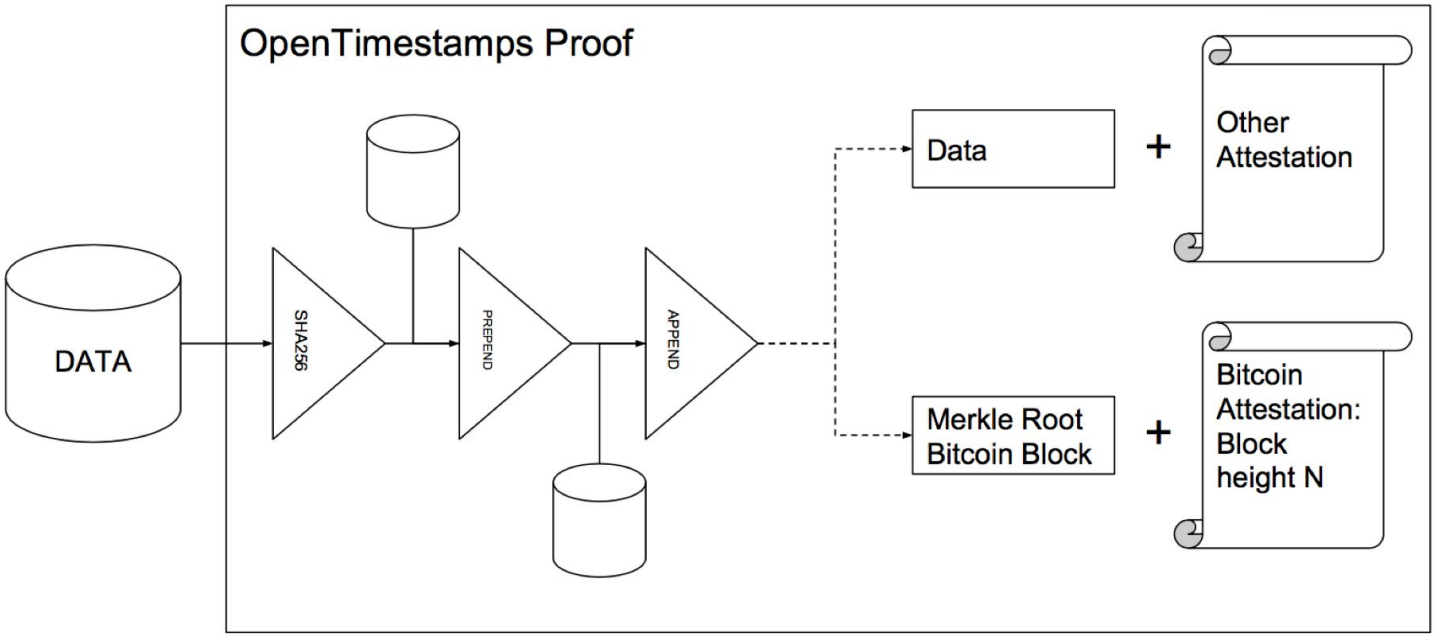








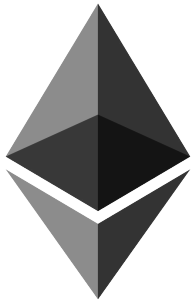
OpenTimestamps branch

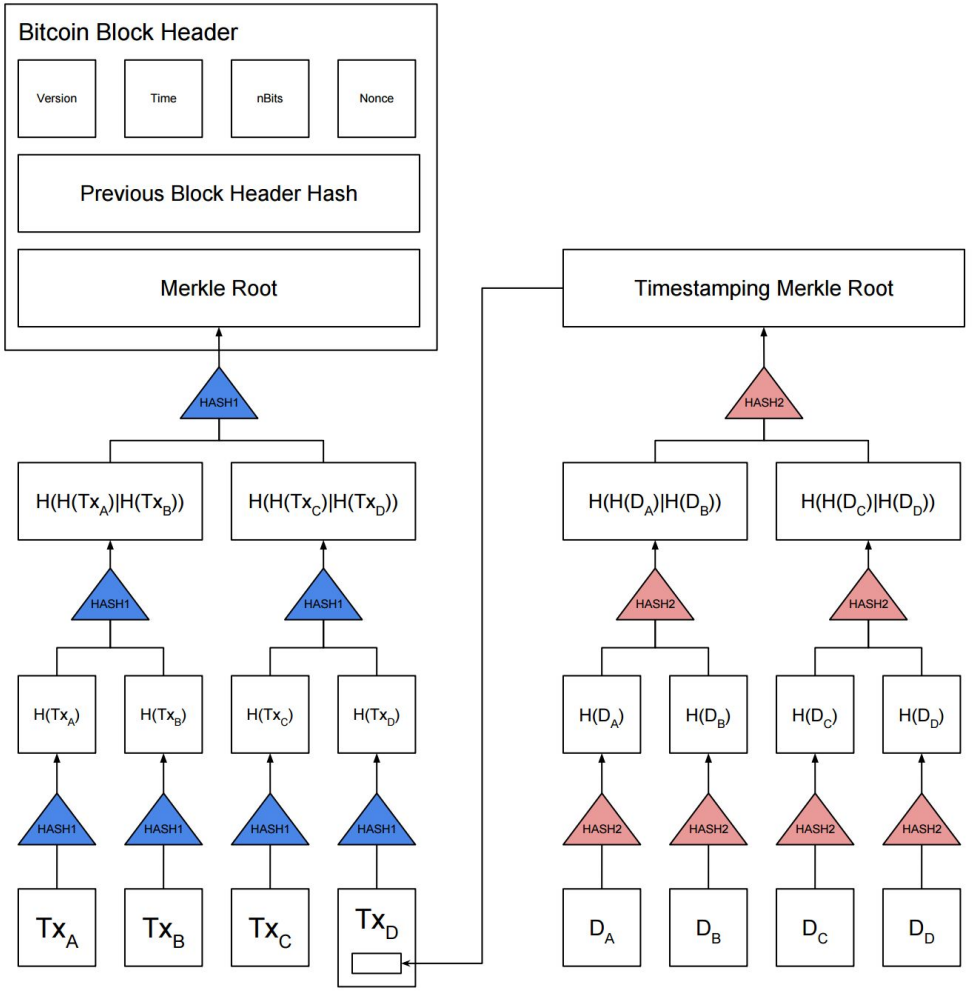


https://opentimestamps.org

OpenTimestamps

Different hash function





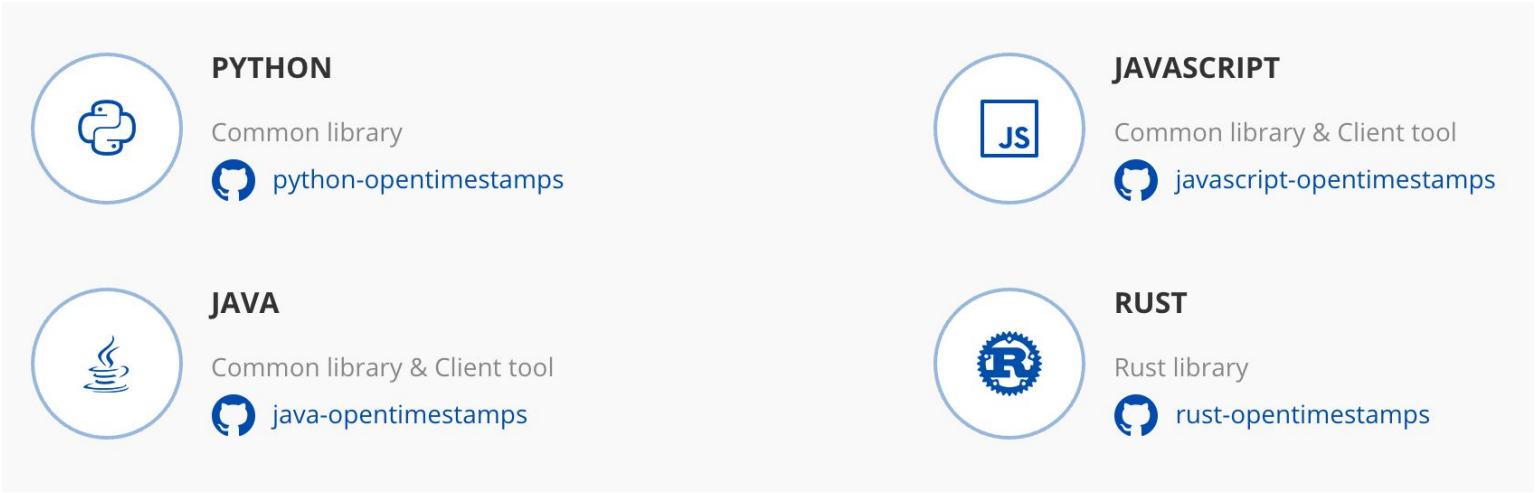
.ots Receipt

Binary format

```
$ ./ots info examples/hello-world.txt.ots
File sha256 hash: 03ba204e50d126e4674c005e04d82e84c21366780af1f43bd54a37816b6ab340
Timestamp:
ripemd160
prepend 0100000001e482f9d32ecc3ba657b69d898010857b54457a90497982ff56f97c4ec58e6f98010000006b48
append 88ac00000000
sha256
sha256
prepend a987f716c533913c314c78e35d35884cac943fa42cac49d2b2c69f4003f85f88
sha256
sha256
prepend dec55b3487e1e3f722a49b55a7783215862785f4a3acb392846019f71dc64a9d
sha256
sha256
prepend b2ca18f485e080478e025dab3d464b416c0e1ecb6629c9aefce8c8214d042432
sha256
sha256
append 11b0e90661196ff4b0813c3eda141bab5e91604837bdf7a0c9df37db0e3a1198
sha256
sha256
append c34bc1a4a1093ffd148c016b1e664742914e939efabe4d3d356515914b26d9e2
sha256
sha256
append c3e6e7c38c69f6af24c2be34ebac48257ede61ec0a21b9535e4443277be30646
sha256
sha256
prepend 0798bf8606e00024e5d5d54bf0c960f629dfb9dad69157455b6f2652c0e8de81
sha256
sha256
append 3f9ada6d60baa244006bb0aad51448ad2fafb9d4b6487a0999cff26b91f0f536
sha256
sha256
prepend c703019e959a8dd3faef7489bb328ba485574758e7091f01464eb65872c975c8
sha256
sha256
append cbfefff513ff84b915e3fed6f9d799676630f8364ea2a6c7557fad94a5b5d788
sha256
sha256
prepend 0be23709859913babd4460bbddf8ed213e7c8773a4b1face30f8acfdf093b705
sha256
sha256
verify BitcoinBlockHeaderAttestation(358391)
```

```
0000000 00 4F 70 65 6E 54 69 6D 65 73 74 61 6D 70 73 00   .OpenTimestamps.
0000010 00 50 72 6F 6F 66 00 BF 89 E2 E8 84 E8 92 94 01   .Proof.........
0000020 08 03 BA 20 4E 50 D1 26 E4 67 4C 00 5E 04 D8 2E   .... NP.&.gL.^...
0000030 84 C2 13 66 78 0A F1 F4 3B D5 4A 37 81 6B 6A B3   ...fx...;.J7.kj.
0000040 40 03 F1 C8 01 01 00 00 00 01 E4 82 F9 D3 2E CC   @.....  ..........
0000050 3B A6 57 B6 9D 89 80 10 85 7B 54 45 7A 90 49 79   ;.W......{TEz.Iy
0000060 82 FF 56 F9 7C 4E C5 8E 6F 98 01 00 00 00 6B 48   ..V.|N..o.....kH
0000070 30 45 02 21 00 B2 53 AD D1 D1 CF 90 84 43 38 A4   0E.!..S......C8.
0000080 75 A0 4F F1 3F C9 E7 BD 24 2B 07 76 2D EA 07 F5   u.O.?...$+.v-...
0000090 60 8B 2D E3 67 02 20 00 B2 68 CA 9C 33 42 B3 76   `.-.g. ....h..3B.v
00000A0 9C DD 06 28 91 31 7C DC EF 87 AA C3 10 B6 85 5E   ...(.1|........^
00000B0 9D 93 89 8E BB E8 EC 01 21 02 0D 8E 4D 10 7D 2B   ........!...M.}+
00000C0 33 9B 00 50 EF DD 4B 4A 09 24 5A A0 56 04 8F 12   3..P..KJ.$Z.V...
00000D0 53 96 37 4E A6 A2 AB 07 09 C6 FF FF FF FF 02 65   S.7N...........e
00000E0 33 E6 05 00 00 00 00 19 76 A9 14 0B F0 57 D4 0F   3.......v....W..
00000F0 BB A6 74 48 62 51 5F 5B 55 A2 31 0D E5 77 2F 88   ..tHbQ_[U.1..w/.
0000100 AC A0 86 01 00 00 00 00 00 19 76 A9 14 F0 06 88   ..........v.....
0000110 AC 00 00 00 00 08 08 F1 20 A9 87 F7 16 C5 33 91   ........ .....3.
0000120 3C 31 4C 78 E3 5D 35 88 4C AC 94 3F A4 2C AC 49   <1Lx.]5.L..?.,.I
0000130 D2 B2 C6 9F 40 03 F8 5F 88 08 08 F1 20 DE C5 5B   ....@.._.... ..[
0000140 34 87 E1 E3 F7 22 A4 9B 55 A7 78 32 15 86 27 85   4....".. U.x2..'.
0000150 F4 A3 AC B3 92 84 60 19 F7 1D C6 4A 9D 08 08 F1   ......`....J.....
0000160 20 B2 CA 18 F4 85 E0 80 47 8E 02 5D AB 3D 46 4B   . .......G..].=FK
0000170 41 6C 0E 1E CB 66 29 C9 AE FC E8 C8 21 4D 04 24   Al...f).....!M.$
0000180 32 08 08 F0 20 11 B0 E9 06 61 19 6F F4 B0 81 3C   2... ....a.o...<
0000190 3E DA 14 1B AB 5E 91 60 48 37 BD F7 A0 C9 DF 37   >....^.`H7.....7
00001A0 DB 0E 3A 11 98 08 08 F0 20 C3 4B C1 A4 A1 09 3F   ..:..... .K....?
00001B0 FD 14 8C 01 6B 1E 66 47 42 91 4E 93 9E FA BE 4D   ....k.fGB.N....M
00001C0 3D 35 65 15 91 4B 26 D9 E2 08 08 F0 20 C3 E6 E7   =5e..K&..... ....
00001D0 C3 8C 69 F6 AF 24 C2 BE 34 EB AC 48 25 7E DE 61   ..i..$..4..H%~.a
00001E0 EC 0A 21 B9 53 5E 44 43 27 7B E3 06 46 08 08 F1   ..!.S^DC'{..F....
00001F0 20 07 98 BF 86 06 E0 00 24 E5 D5 D5 4B F0 C9 60   . .......$...K..`
0000200 F6 29 DF B9 DA D6 91 57 45 5B 6F 26 52 C0 E8 DE   .).....WE[o&R....
0000210 81 08 08 F0 20 3F 9A DA 6D 60 BA A2 44 00 6B B0   .... ?..m`..D.k.
0000220 AA D5 14 48 AD 2F AF B9 D4 B6 48 7A 09 99 CF F2   ...H./....Hz....
0000230 6B 91 F0 F5 36 08 08 F1 20 C7 03 01 9E 95 9A 8D   k...6... ........
0000240 D3 FA EF 74 89 BB 32 8B A4 85 57 47 58 E7 09 1F   ...t..2...WGX...
0000250 01 46 4E B6 58 72 C9 75 C8 08 08 F0 20 CB FE FF   .FN.Xr.u.... ....
0000260 F5 13 FF 84 B9 15 E3 FE D6 F9 D7 99 67 66 30 F8   ............gf0.
0000270 36 4E A2 A6 C7 55 7F AD 94 A5 B5 D7 88 08 08 F1   6N...U........ ..
0000280 20 0B E2 37 09 85 99 13 BA BD 44 60 BB DD F8 ED   ...7......D`....
0000290 21 3E 7C 87 73 A4 B1 FA CE 30 F8 AC FD F0 93 B7   !>|.s.....0......
00002A0 05 08 08 00 05 88 96 0D 73 D7 19 01 03 F7 EF 15   .... ....s.......
```

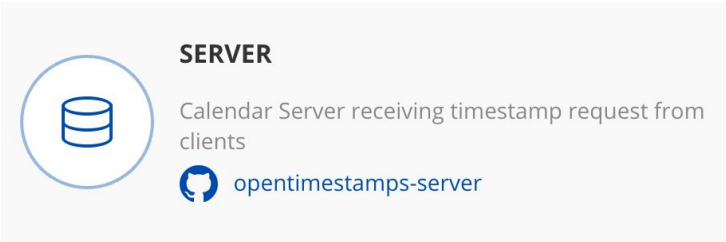
Libraries



https://github.com/opentimestamps

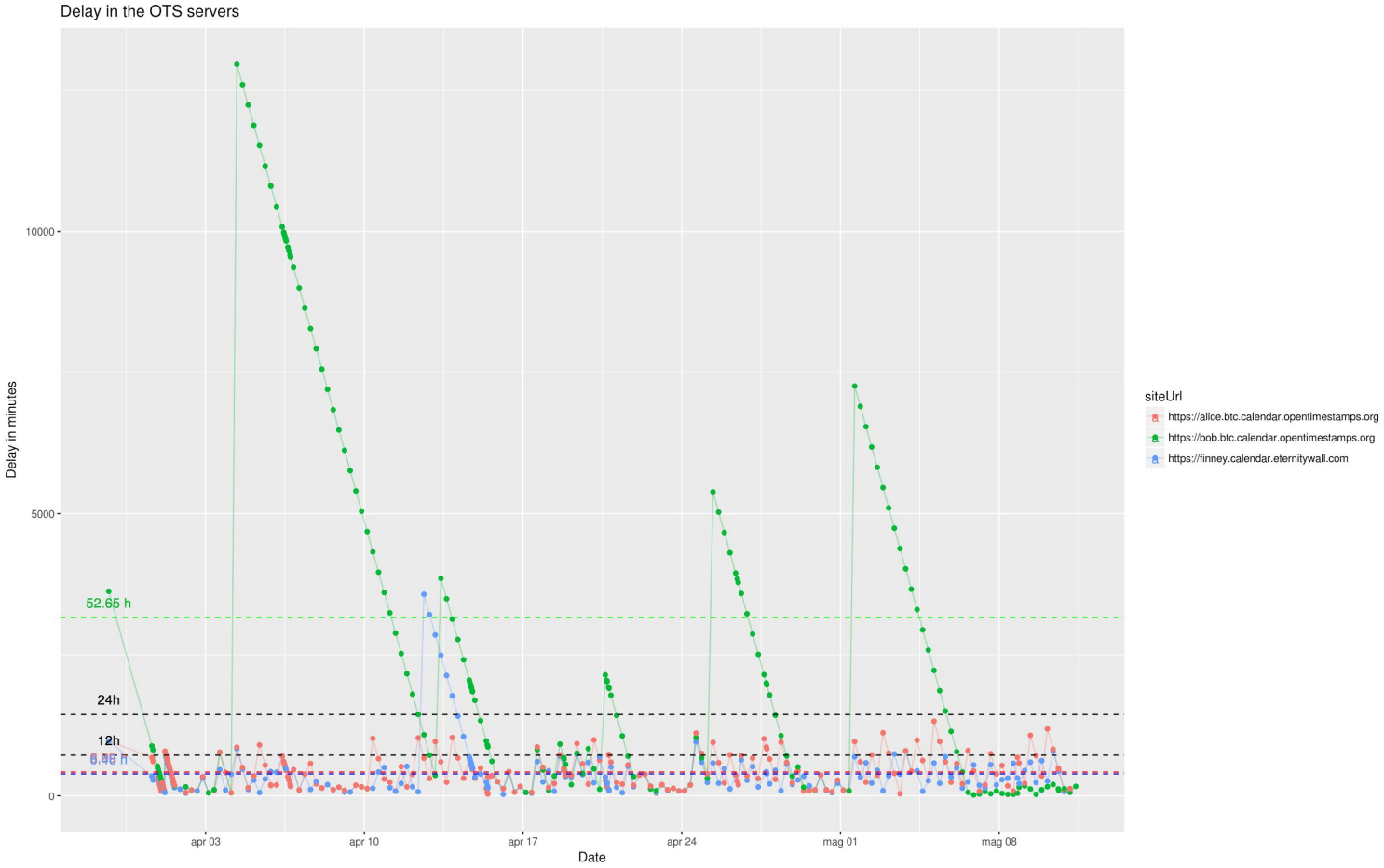
Calendar Servers

- Maintained by different entities
  - https://alice.btc.calendar.opentimestamps.org/
  - https://bob.btc.calendar.opentimestamps.org/
  - https://finney.calendar.eternitywall.com/
- Offering their state publicly (all performed timestamp)
  - Through the /calendar URI

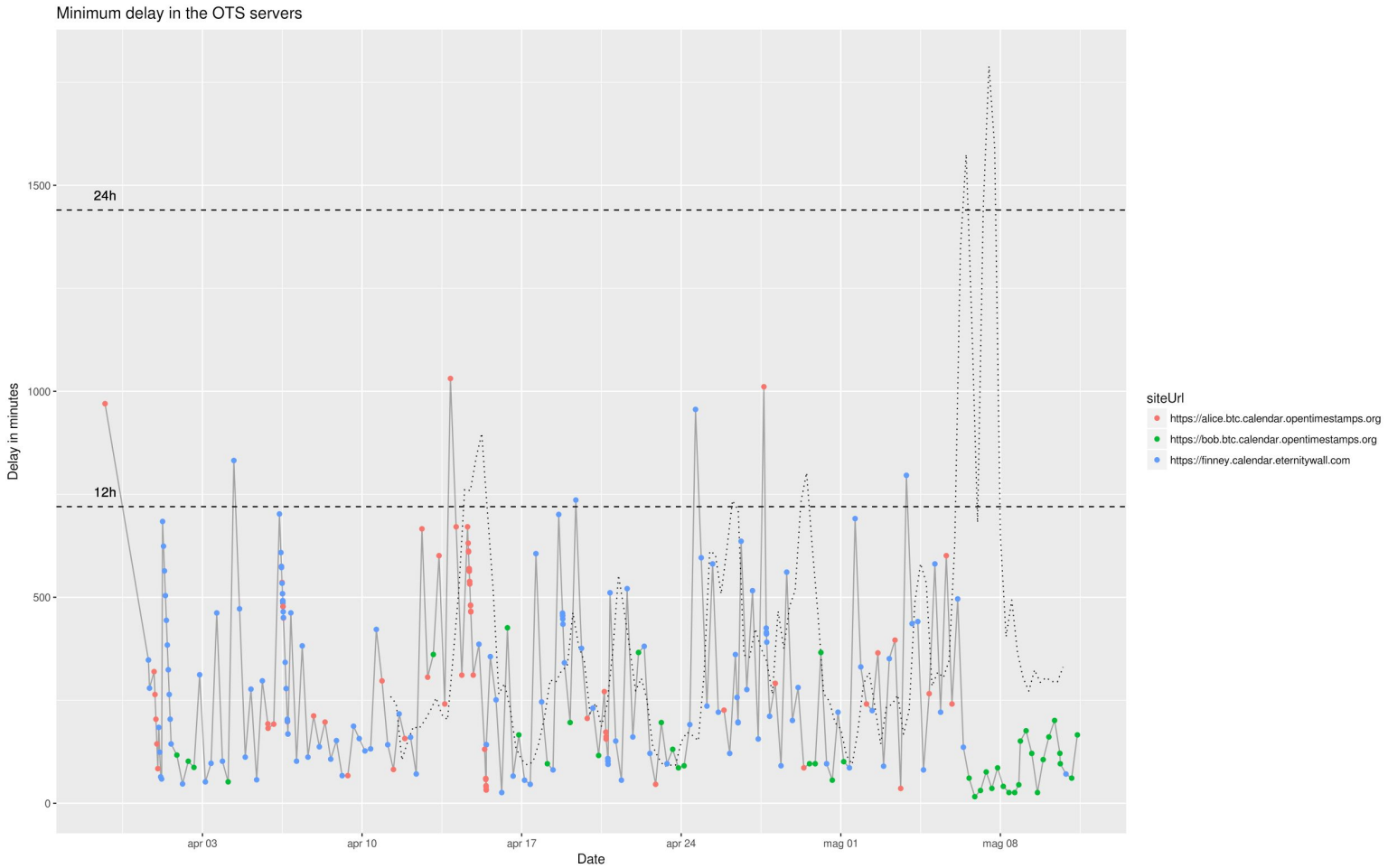


https://github.com/opentimestamps

Reliability and execution time



Reliability and execution time



Eternity Wall

Timestamping and proof of publication

- Timestamping
  - An external viewer **could not** see all the element of the set
    - If someone timestamp two different version of a document, the rest of the world cannot see it
- Proof of publication
  - An external viewer **could** see all the the element of the set
    - Prevent double spend!
    - Bitcoin UTXO (Unspent Transaction Output)