

Scalable and Accountable Timestamping

Riccardo Casatta - Eternity Wall

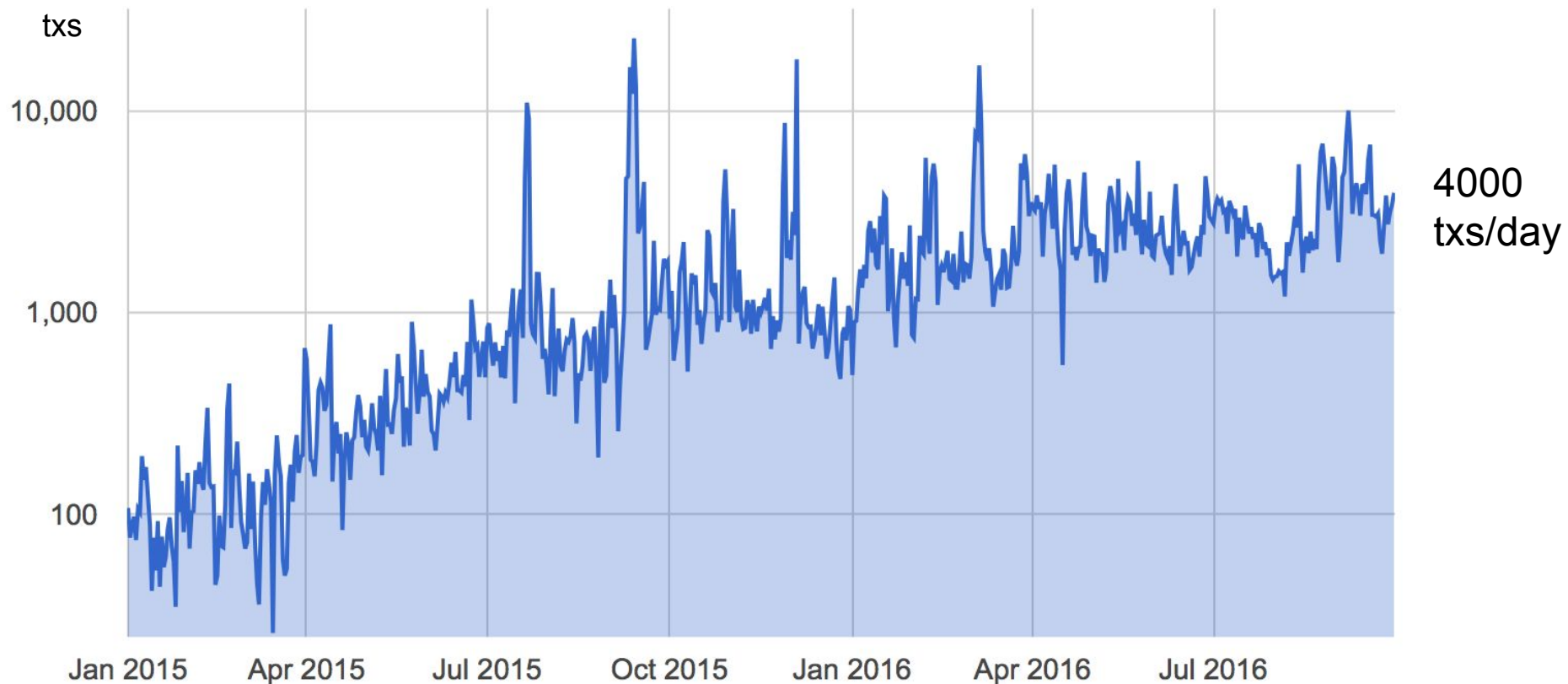
Agenda

- Why Timestamping @ Scaling
- Aggregating timestamps
- Timestamping Proof formats
 - OpenTimestamps
 - Chainpoint

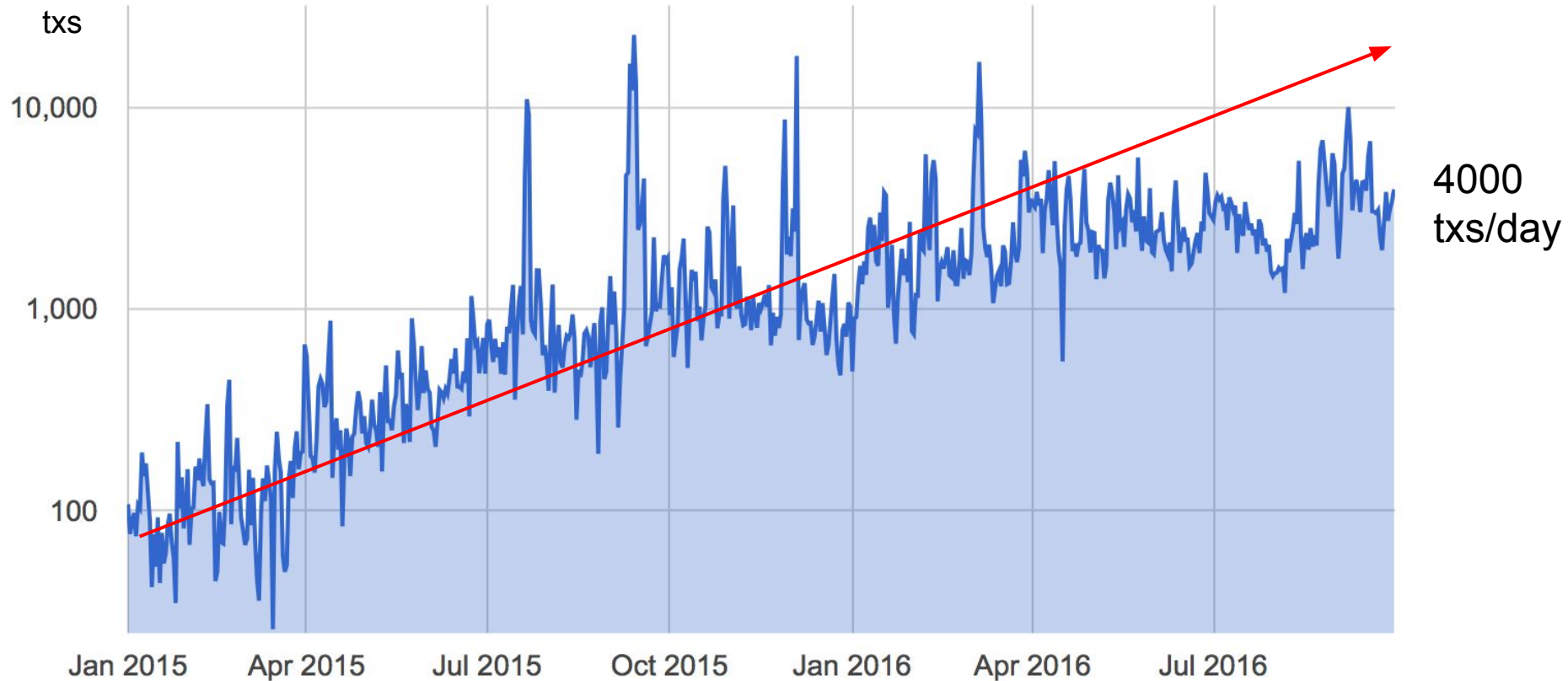
Agenda

- **Why Timestamping @ Scaling**
- Aggregating timestamps
- Timestamping Proof formats
 - OpenTimestamps
 - Chainpoint

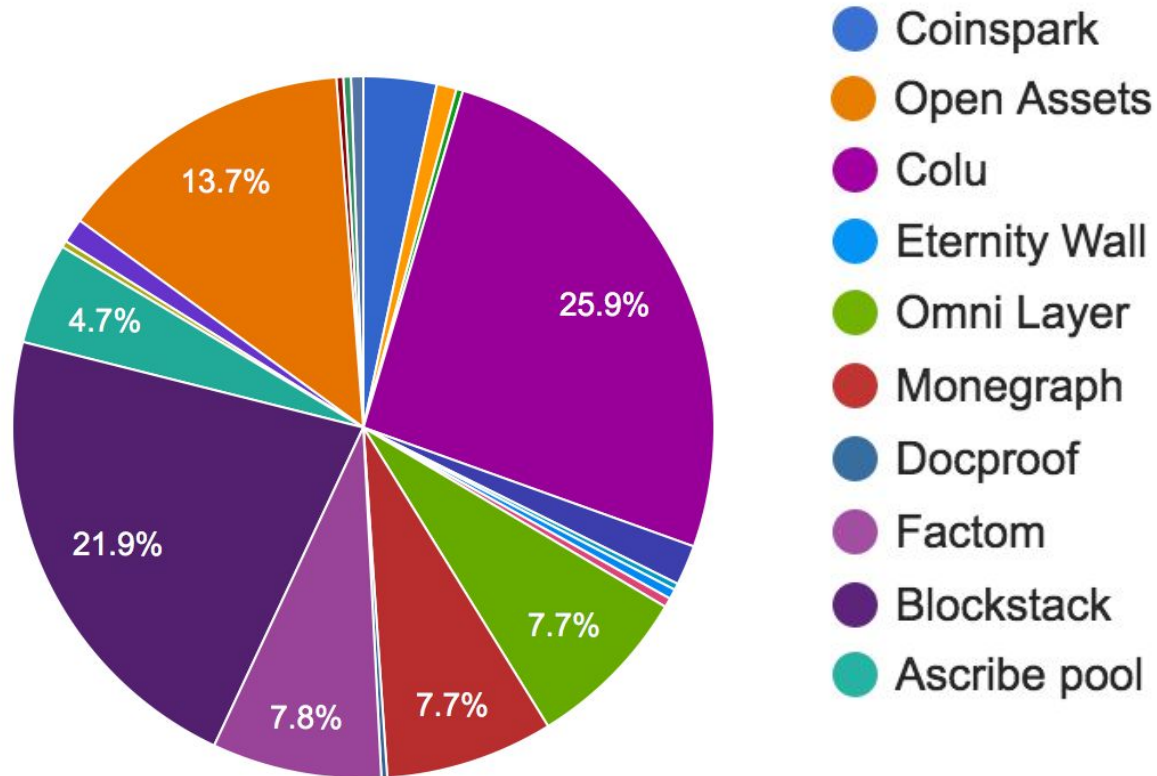
OP_RETURN tx per day



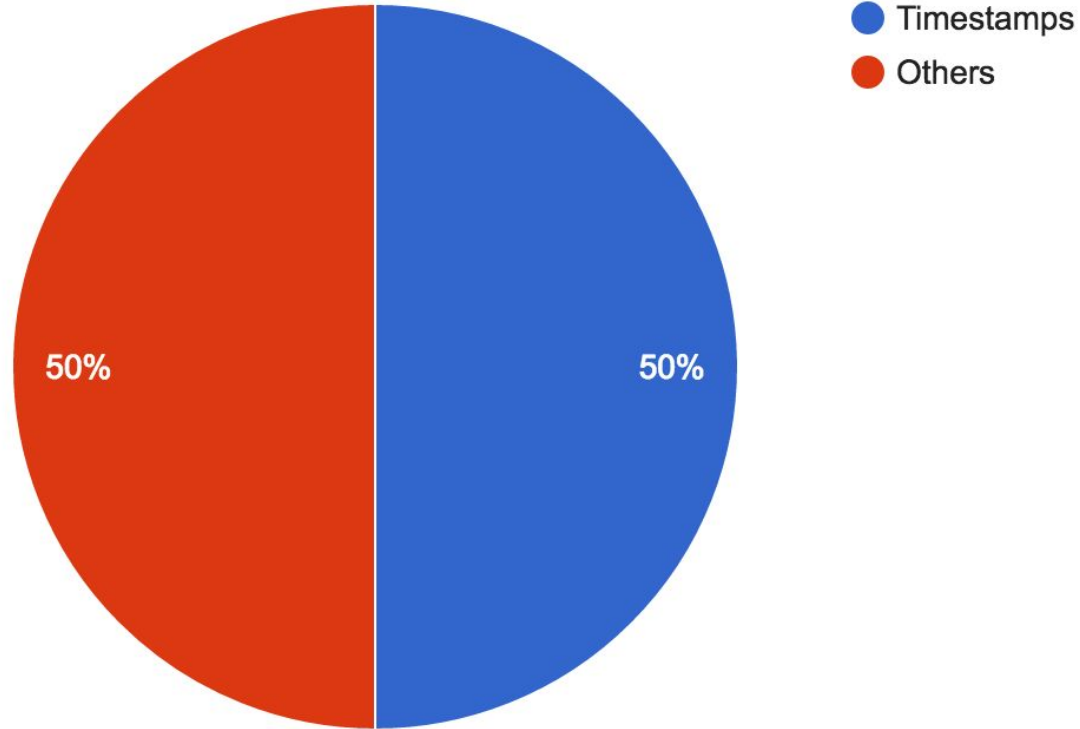
OP_RETURN tx per day



OP_RETURN utilization



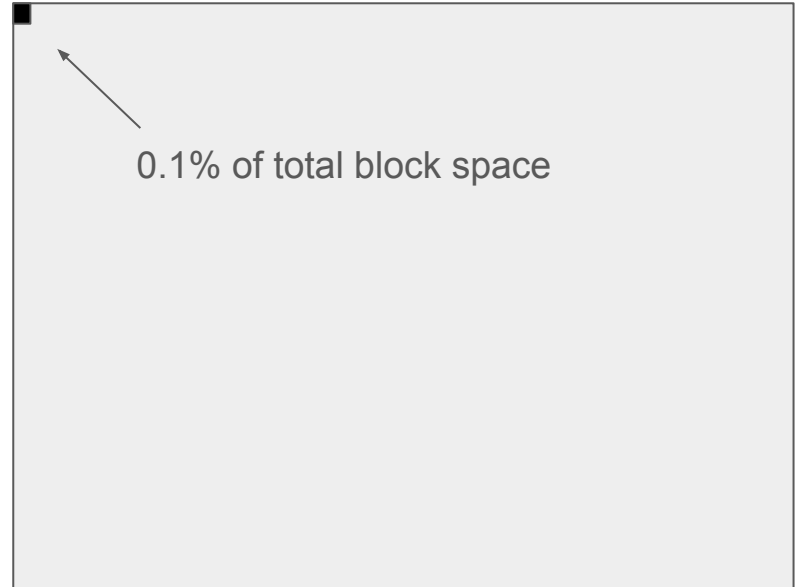
OP_RETURN utilization



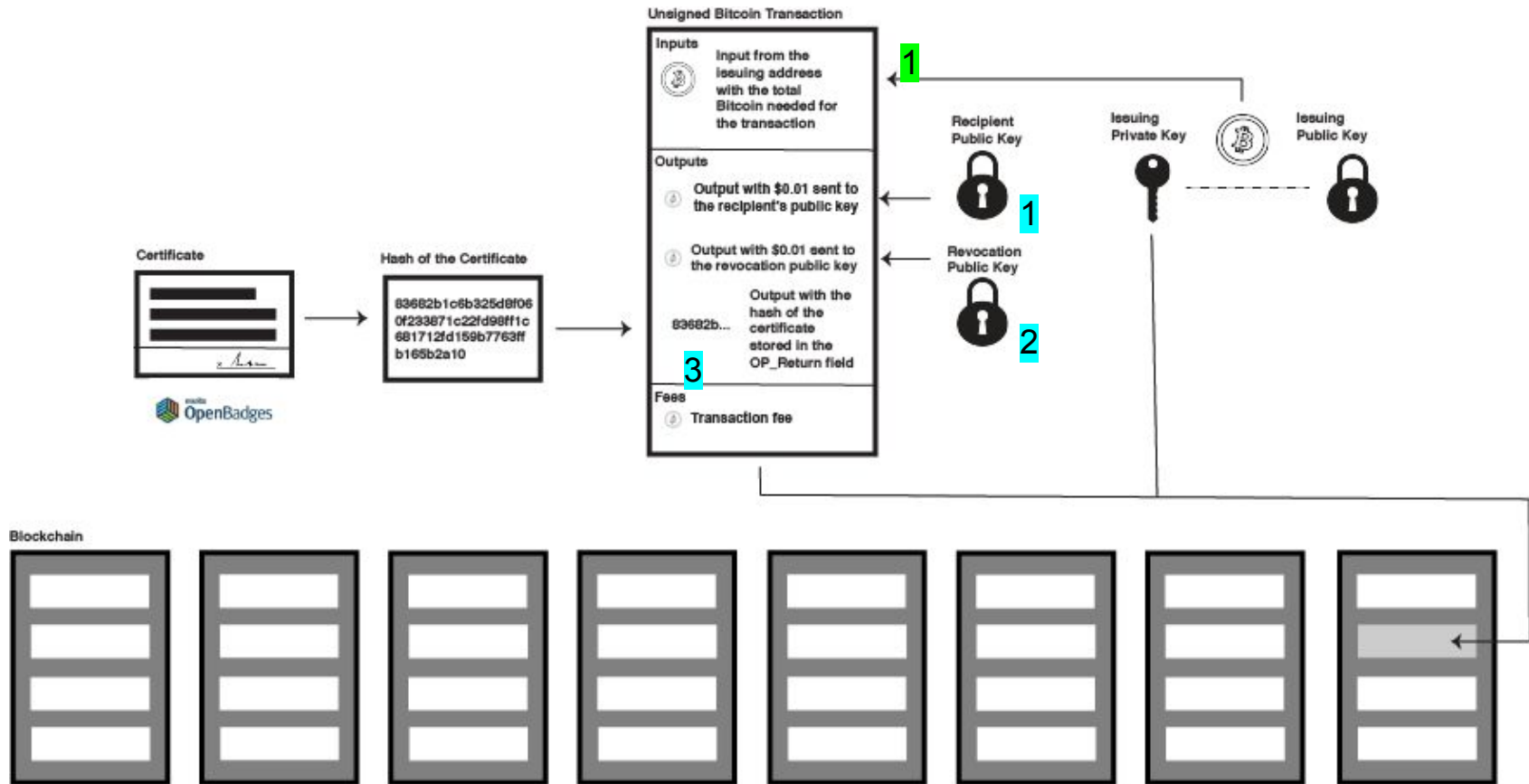
Claim

≈ 200 tx/day for global timestamping needs

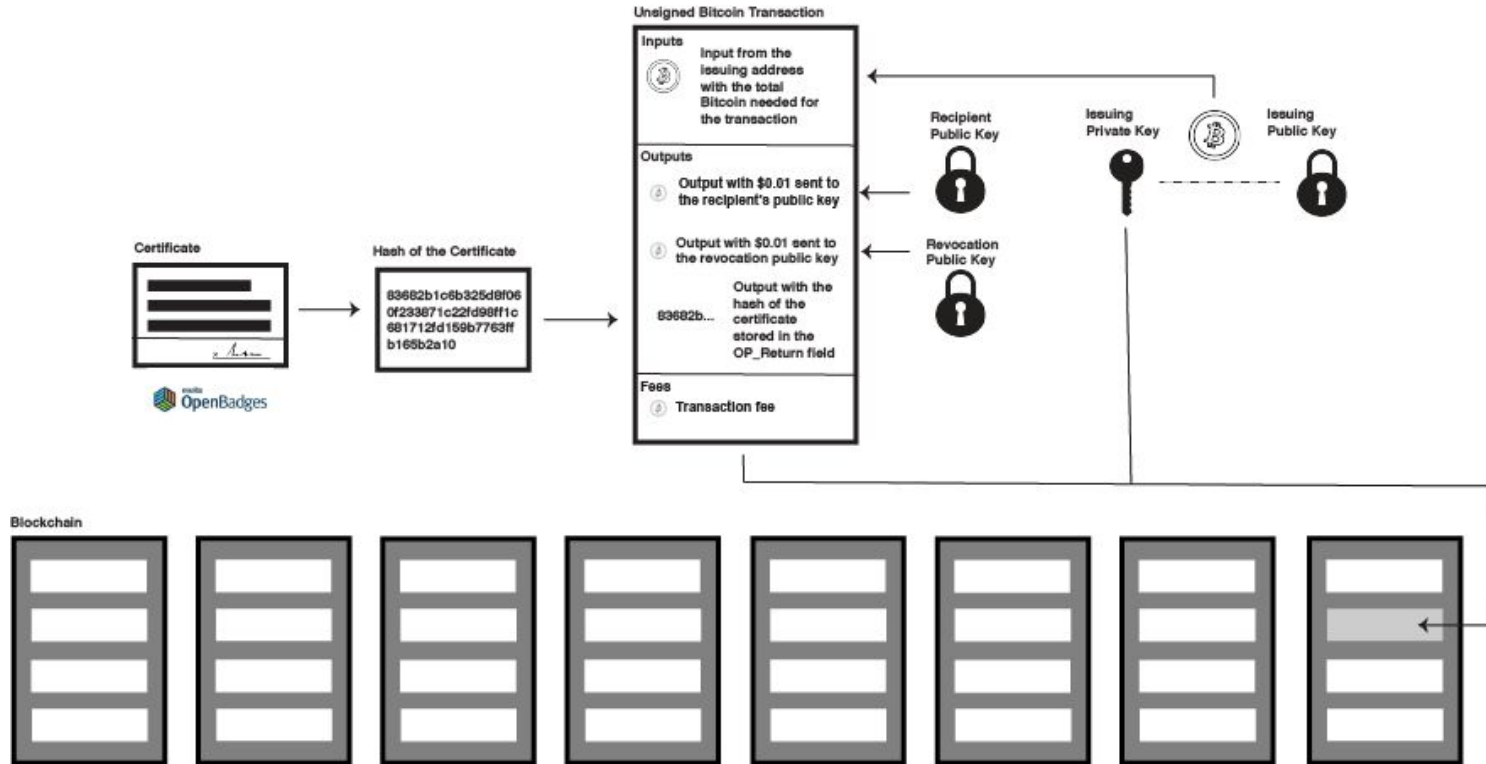
- Less cost, 1/10 than now
- 0.1% of block



One-certificate-one-transaction



One-certificate-one-transaction



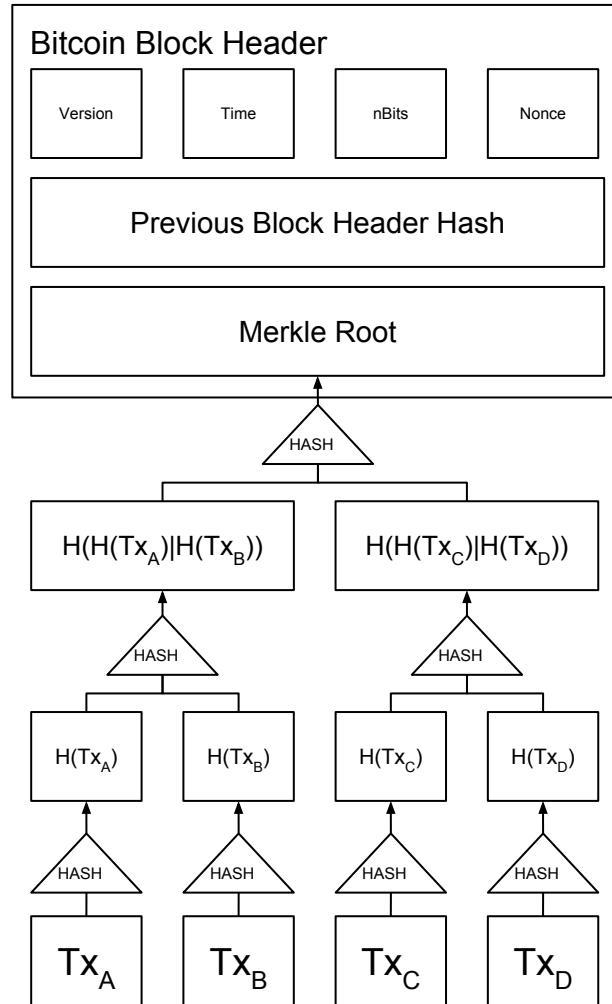
3000 degrees/year * 40 exam/year * 40000 universities ≈ ...

80MB blocks!

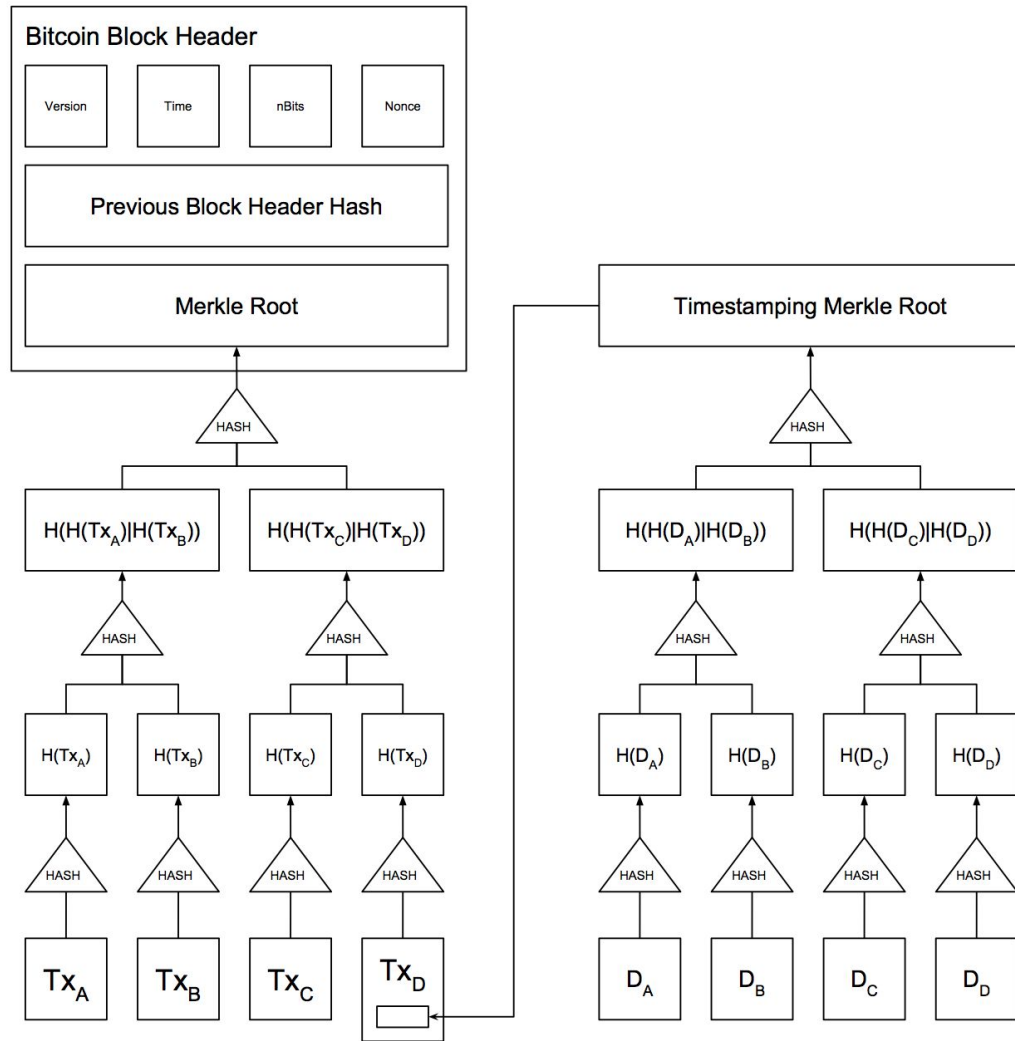
Agenda

- Why Timestamping @ Scaling
- **Aggregating timestamps**
- Timestamping Proof formats
 - OpenTimestamps
 - Chainpoint

Aggregating Timestamps

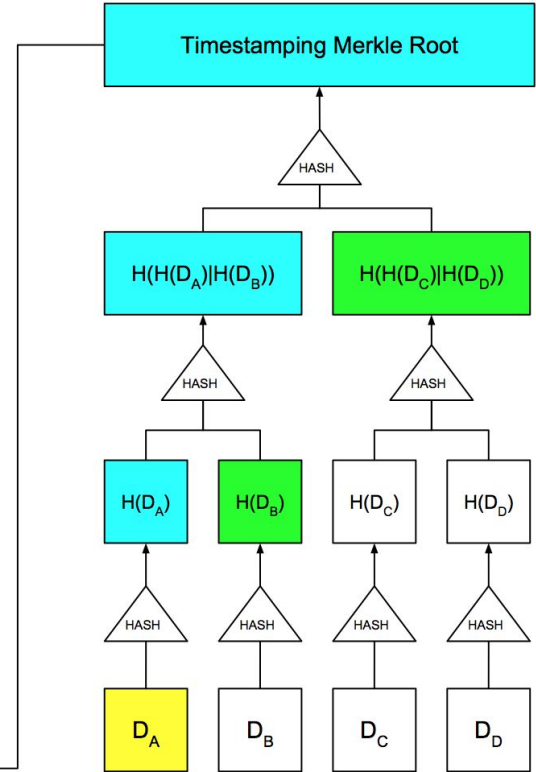
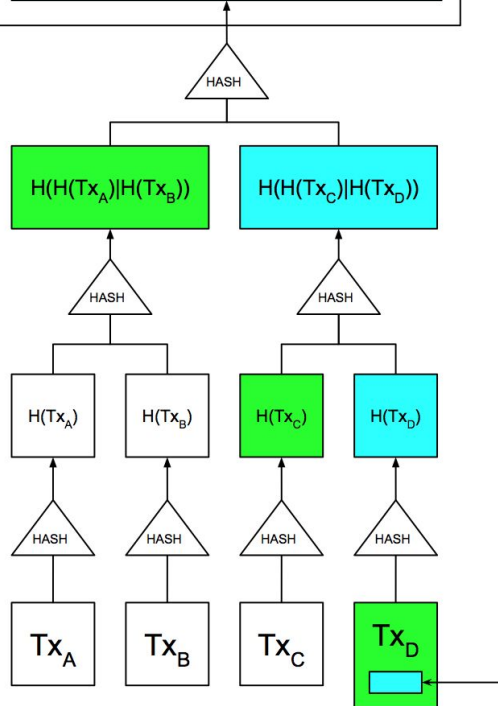
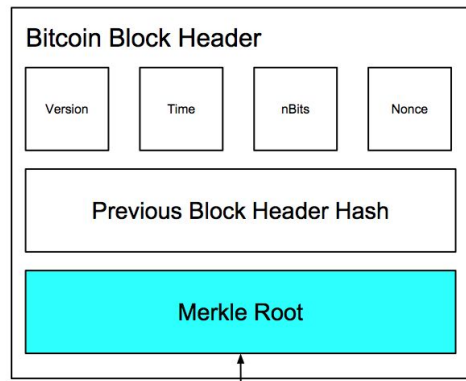


Aggregating Timestamps

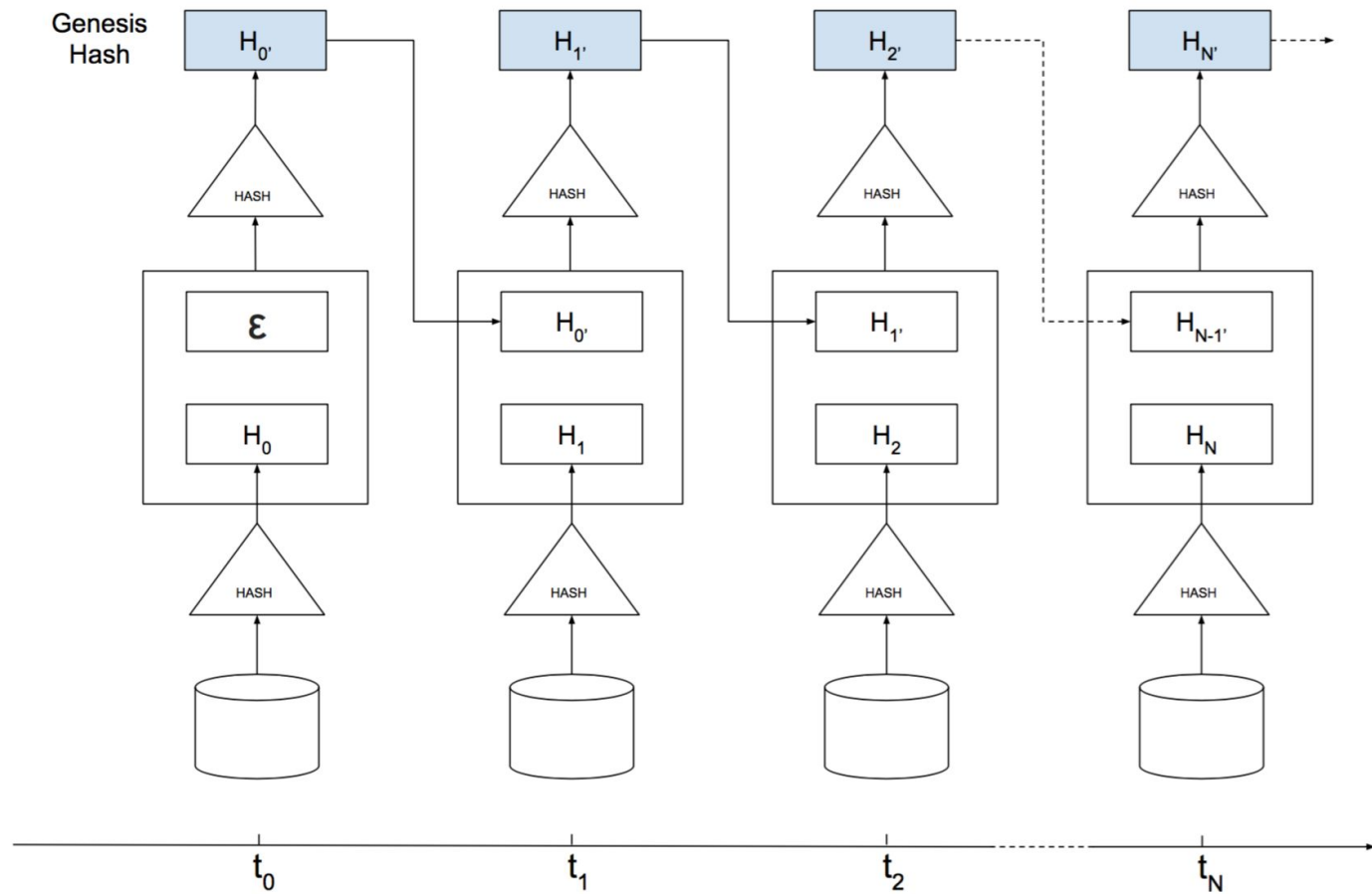


Aggregating Timestamps

✓ scalability



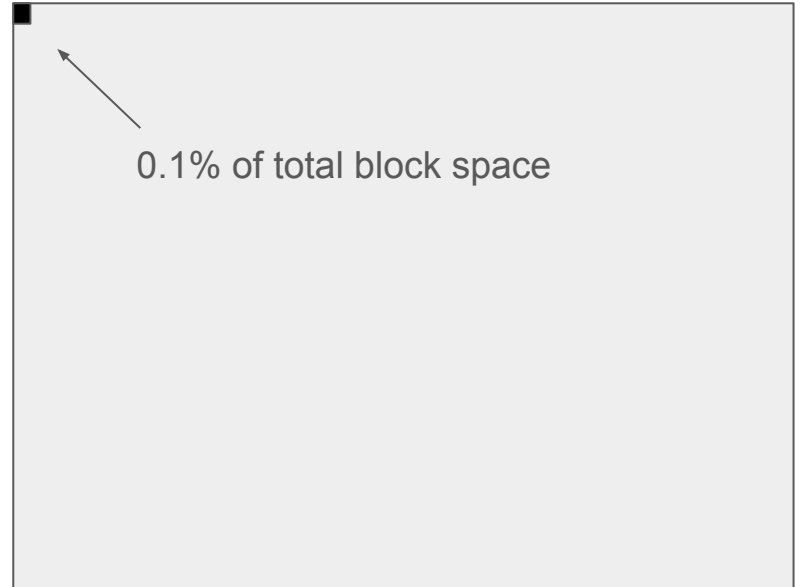
Hashchain



Claim

≈ 200 txs/day for global timestamping needs

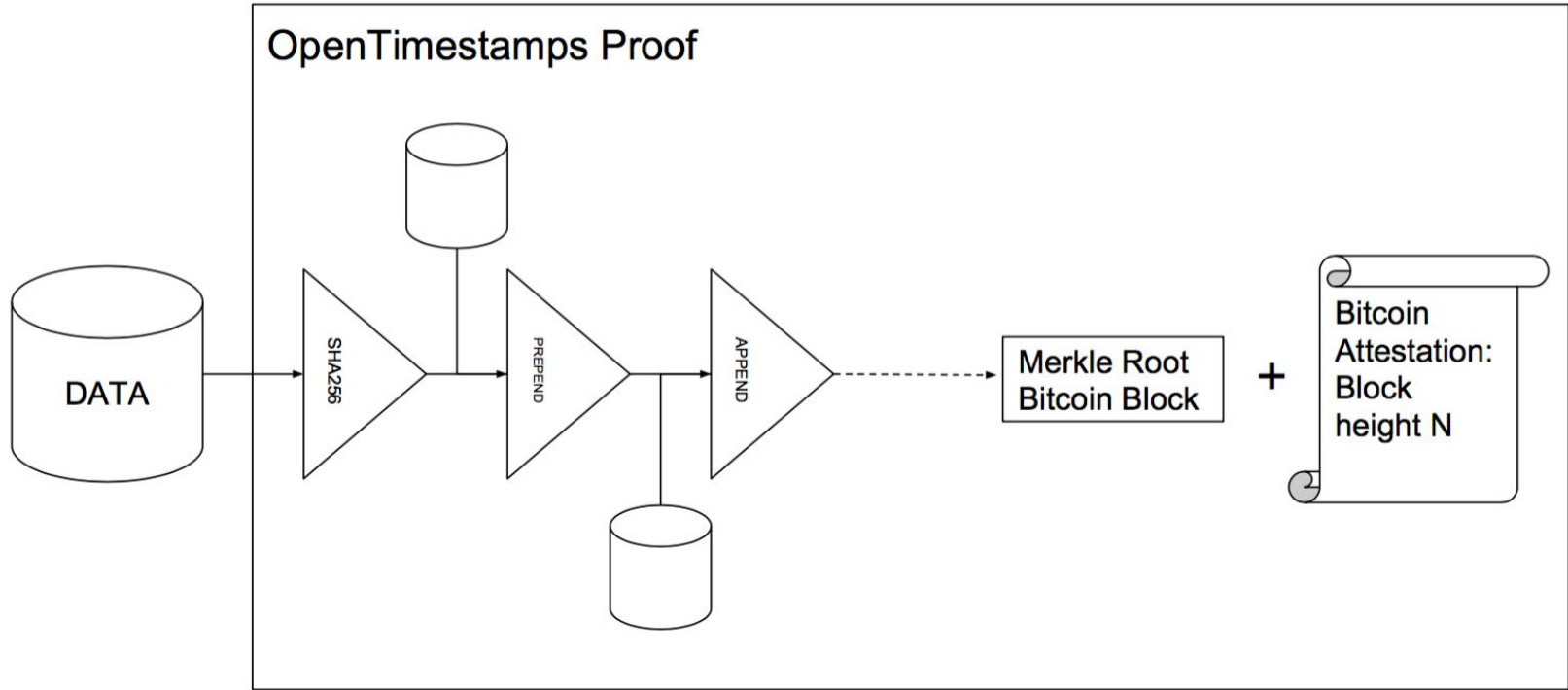
- Less cost, 1/10 than now
- 0.1% of block



Agenda

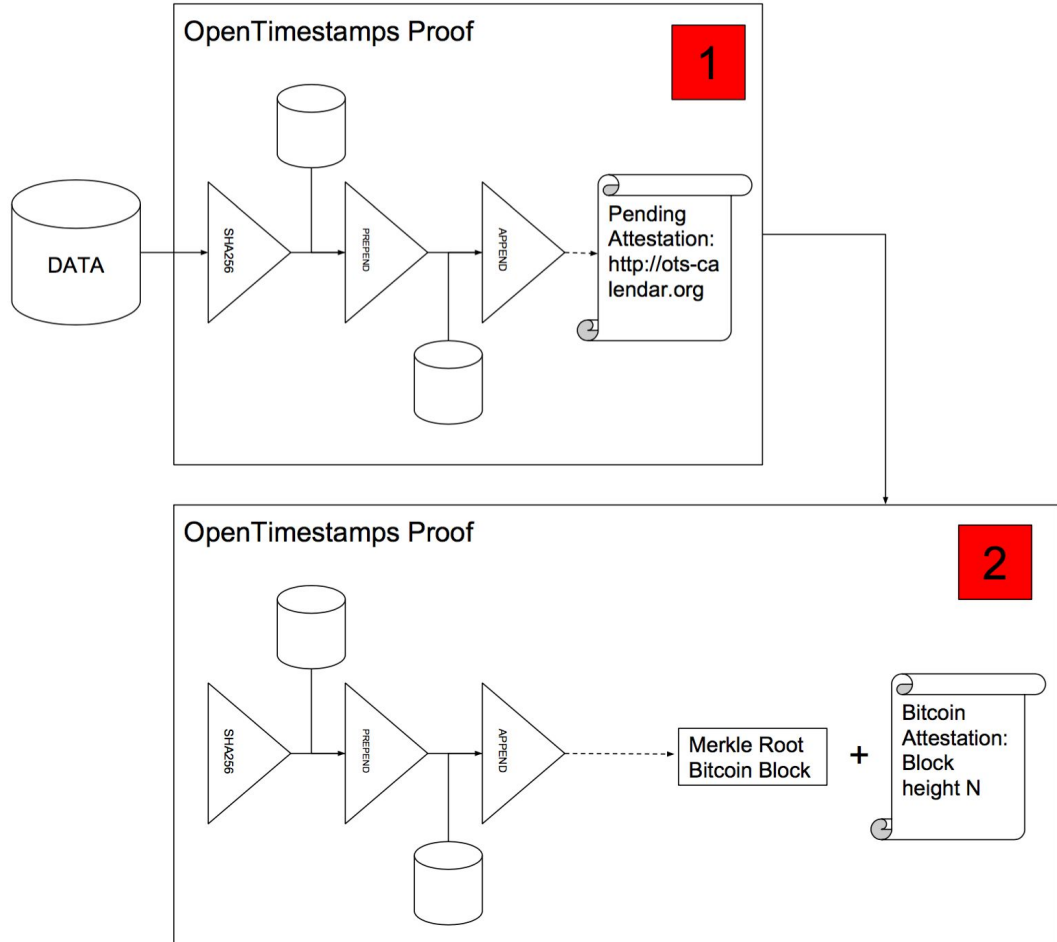
- Why Timestamping @ Scaling
- Aggregating timestamps
- **Timestamping Proof formats**
 - **OpenTimestamps**
 - Chainpoint

OpenTimestamps

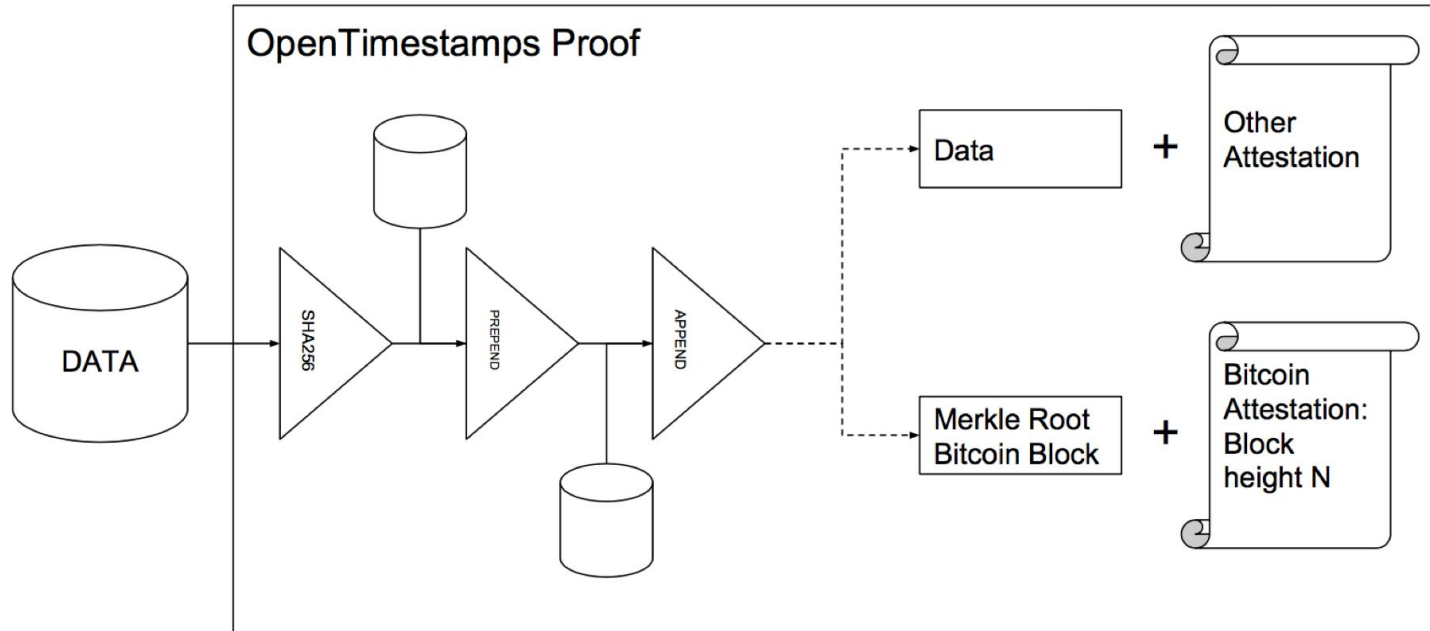


OpenTimestamps

Incomplete proof

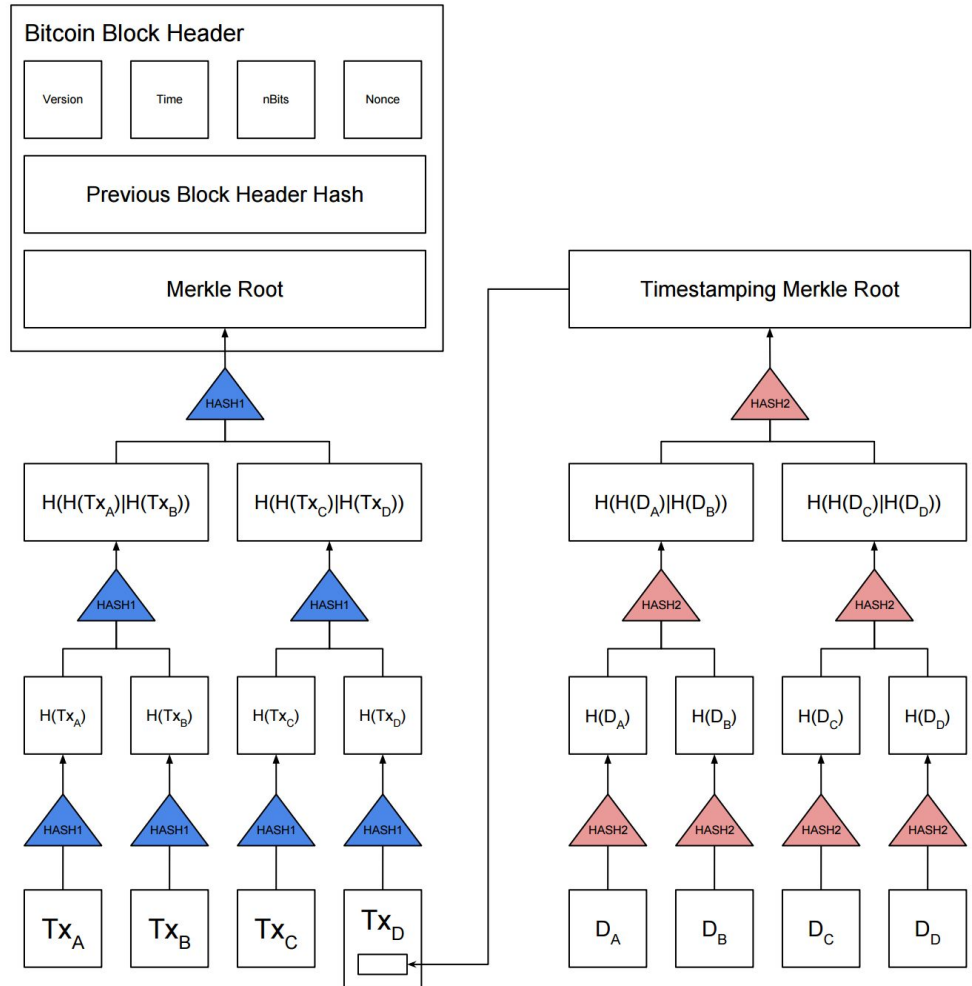


OpenTimestamps branch



OpenTimestamps


Different hash function




OpenTimestamps

Github integration

Verified

 This commit was signed with a **verified signature**.

 **RCasatta**
Riccardo Casatta

GPG key ID: EFDBB6FD8C350E75
[Learn about signing commits](#)

```
commit 9b8f3f29b550df6362ea4672ea57850446d4d09c
```

```
ots: Got 1 attestation(s) from https://alice.btc.calendar.opentimestamps.org
ots: Got 1 attestation(s) from https://bob.btc.calendar.opentimestamps.org
ots: Success! Bitcoin attests data existed as of Fri Oct 7 15:37:47 2016 CEST
ots: Good timestamp
```

```
gpg: Signature made Fri Oct 7 15:30:58 2016 CEST using RSA key ID 8C350E75
gpg: Good signature from "Riccardo Casatta <riccardo.casatta@gmail.com>" [ultimate]
Author: Riccardo Casatta <riccardo.casatta@gmail.com>
Date: Fri Oct 7 15:30:52 2016 +0200
```

First git commit with OpenTimestamps

```
$ git cat-file -p 9b8f3f29b550df6362ea4672ea57850446d4d09c
tree a709725f6f1b290077d4af0d3aa3ff144594e265
parent 6e2674a2a7a8e338642c4e5aafb8737d538483dc
author Riccardo Casatta <riccardo.casatta@gmail.com> 1475847052 +0200
committer Riccardo Casatta <riccardo.casatta@gmail.com> 1475847052 +0200
pgpsig -----BEGIN PGP SIGNATURE-----
```

```
iQIcBAABCAAGBQJX960SAAoJE0/btv2MNQ51QFUQAIQsK3VqT3PuI+d05erVKRYS
zdgTDk0l7yTuHnq+WPYTs2bpK4mcJC0wCS7xuexDQE3/0HnTbY+NtdjC6UPWTG3N
Urf1qHvCyZDEo5hpuwG0+hLxIzXqpE88TUIxG0/zK6kHZFfjYzfJ8YdyB9KBp7y
MHTaxxbmk67Ug0DS1JJzD5jSrtjQ9MdoDTvsYPQUoT83Z/a0bzDKDHNAkaj3hN02
YHvsbkVBy3TtwYodopyQP2CZiIiIyLsiPG+6n3by4EWNDZzuHQjkHYKwBX+CDvDR
/9B6hW/2mzgFj8FF9Wf+o7VXyHynNVcz0xXSQlBDfIqmg0GXacXlAFRRQthH3oy9
maYAn+3n1zIoyBmuV01VAui35Exp9LxoVBUf0MYa3eHKd7nNiYm0vc+J7H61EQGD
iWzEgxD6qA8VerNBFCExUhDq4PL8cQkZLPhSMYqgGKp+iUC/F0/Q2AHYwbloV4p9
2ytVxNXjE2oxlMxvYxh3y0p3z6M0zXEokUe3PN4qPVT/sdtbGIRNjgFwWauTHYLc
QkGN0o0cNGzPjyRouyc9FJG1Wnefx5hYUlcAC2v1Z1H3GapBzH+NRZeVkf/WxIlF
q1CoanRcbRuSboiKn+UnXkXrACWft6Fq0pfscc0n1mYV1mnxtaEjhNuIshZ89QAA
vbIFU5yc1MrWbWCJ8zNW
=aB0E
-----END PGP SIGNATURE-----
```

```
-----BEGIN OPENTIMESTAMPS GIT TIMESTAMP-----
```

```
AQD/8BAkqHoGFaGmRVU4+ffrctbtCPEEV/ejk/AI/j10CuJttLUAg9/jDS75DI4s
K2h0dHBz0i8vYm9iLmJ0Yy5jYWxlbmRhci5vcGVudGltZXN0YW1wcy5vcmfwEE1g
0v/0BFQzvrmb9T8kT0I8QRX960S8AgjLLN00W1iQCD3+MNLvkmj4taHR0cHM6
Ly9hbGljZS5idGMuY2FsZW5kYXIub3BlbnRpbWVzdGFTchMub3Jn
-----END OPENTIMESTAMPS GIT TIMESTAMP-----
```

First git commit with OpenTimestamps

OpenTimestamps

Binary format

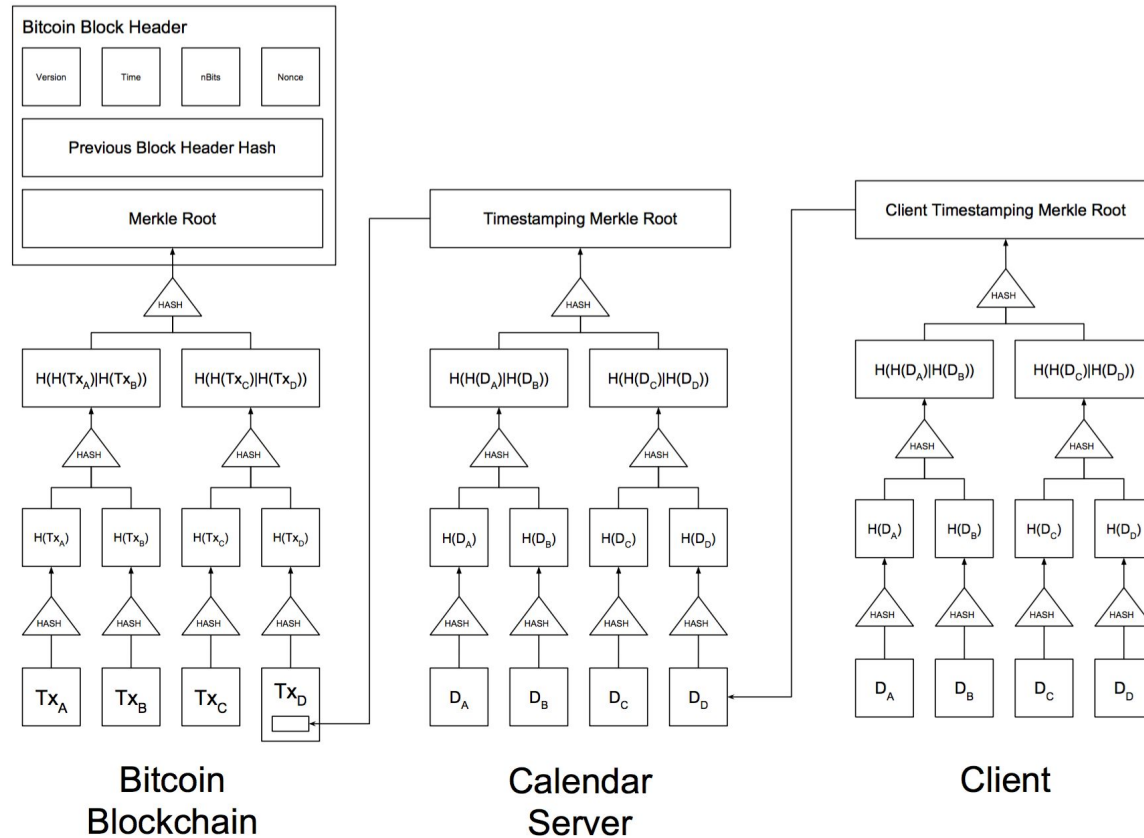
```
$ ./ots info examples/hello-world.txt.ots
File sha256 hash: 03ba204e50d126e4674c005e04d82e84c21366780af1f43bd54a37816b6ab340
Timestamp:
ripemd160
prepend 0100000001e482f9d32ecc3ba657b69d898010857b54457a90497982ff56f97c4ec58e6f98010000006b48
append 88ac00000000
sha256
sha256
prepend a987f716c533913c314c78e35d35884cac943fa42cac49d2b2c69f4003f85f88
sha256
sha256
prepend dec55b3487e1e3f722a49b55a7783215862785f4a3acb392846019f71dc64a9d
sha256
sha256
prepend b2ca18f485e080478e025dab3d464b416c0e1ecb6629c9aefce8c8214d042432
sha256
sha256
append 11b0e90661196ff4b0813c3eda141bab5e91604837bdf7a0c9df37db0e3a1198
sha256
sha256
append c34bc1a4a1093ffd148c016b1e664742914e939efabe4d3d356515914b26d9e2
sha256
sha256
append c3e6e7c38c69f6af24c2be34ebac48257ede61ec20a21b9535e4443277be30646
sha256
sha256
prepend 0798bf8606e00024e5d54bf0c960f629dfb9dad69157455b6f2652c0e8de81
sha256
sha256
append 3f9ada6d6baa244006bb0aad51448ad2fafb9d4b6487a0999cfff26b91f0f536
sha256
sha256
prepend c703019e959a8dd3faef7489bb328ba485574758e7091f01464eb65872c975c8
sha256
sha256
append cbfefff513ff84b915e3fed6f9d799676630f8364ea2a6c7557fad94a5b5d788
sha256
sha256
prepend 0be23709859913babd4460bbddf8ed213e7c8773a4b1face30f8acfd093b705
sha256
sha256
verify BitcoinBlockHeaderAttestation(358391)
```



```
00000000 00 4f 70 65 6E 54 69 6D 65 73 74 61 6D 70 73 00
00000010 00 50 72 6F 6F 66 00 BF 89 E2 E8 84 E8 92 94 01
00000020 08 03 BA 20 4E 50 D1 26 E4 67 4C 00 5E 04 D8 2E
00000030 84 C2 13 66 78 0A F1 F4 3B D5 4A 37 81 6B 6A B3
00000040 40 03 F1 C8 01 01 00 00 00 01 E4 82 F9 D3 2E CC
00000050 3B A6 57 B6 9D 89 80 10 85 7B 54 45 7A 90 49 79
00000060 82 FF 56 F9 7C 4E C5 8E 6F 98 01 00 00 00 6B 48
00000070 30 45 02 21 00 B2 53 AD D1 D1 CF 90 84 43 38 A4
00000080 75 A0 4F F1 3F C9 E7 BD 24 2B 07 76 2D EA 07 F5
00000090 60 8B 2D E3 67 02 20 00 B2 68 CA 9C 33 42 B3 76
000000A0 9C DD 06 28 91 31 7C DC EF 87 AA C3 10 B6 85 5E
000000B0 9D 93 89 8E BB E8 EC 01 21 02 0D 8E 4D 10 7D 2B
000000C0 33 9B 00 50 EF DD 4B 4A 09 24 5A A0 56 04 8F 12
000000D0 53 96 37 4E A6 A2 AB 07 09 C6 FF FF FF FF 02 65
000000E0 33 E6 05 00 00 00 00 19 76 A9 14 0B F0 57 D4 0F
000000F0 BB A6 74 48 62 51 5F 5B 55 A2 31 0D E5 77 2F 88
00001000 AC A0 86 01 00 00 00 00 00 19 76 A9 14 F0 06 88
00001100 AC 00 00 00 00 08 08 F1 20 A9 87 F7 16 C5 33 91
00001200 3C 31 4C 78 E3 5D 35 88 4C AC 94 3F A4 2C AC 49
00001300 D2 B2 C6 9F 40 03 F8 5F 88 08 08 F1 20 DE C5 5B
00001400 34 87 E1 E3 F7 22 A4 9B 55 A7 78 32 15 86 27 85
00001500 F4 A3 AC B3 92 84 60 19 F7 1D C6 5A 9D 08 08 F1
00001600 20 B2 CA 18 F4 85 E0 80 47 8E 02 5D AB 3D 46 4B
00001700 41 6C 0E 1E CB 66 29 C9 AE FC E8 C8 21 4D 04 24
00001800 32 08 08 F0 20 11 B0 E9 06 61 19 6F F4 B0 81 3C
00001900 3E DA 14 1B AB 5E 91 60 48 37 BD F7 A0 C9 DF 37
00001A00 DB 0E 3A 11 98 08 08 F0 20 C3 4B C1 A4 A1 09 3F
00001B00 FD 14 8C 01 6B 1E 66 47 42 91 4E 93 9E FA BE 4D
00001C00 3D 35 65 15 91 4B 26 D9 E2 08 08 F0 20 C3 E6 E7
00001D00 C3 8C 69 F6 AF 24 C2 BE 34 EB AC 48 25 7E DE 61
00001E00 EC 0A 21 B9 53 5E 44 43 27 7B E3 06 46 08 08 F1
00001F00 02 07 98 BF 86 06 E0 00 24 E5 D5 04 48 F0 C9 60
00002000 F6 29 DF B9 DA D6 91 57 45 5B 6F 26 52 C0 E8 DE
00002100 81 08 08 F0 20 3F 9A DA 6D 60 BA A2 44 00 6B B0
00002200 AA D5 14 48 AD 2F AF B9 D4 B6 48 7A 09 99 CF F2
00002300 6B 91 F0 F5 36 08 08 F1 20 C7 03 01 9E 95 9A 8D
00002400 D3 FA EF 74 89 BB 32 8B A4 85 57 47 58 E7 09 1F
00002500 01 46 4E B6 58 72 C9 75 C8 08 08 F0 20 CB FE FF
00002600 F5 13 FF 84 B9 15 E3 FE D6 F9 D7 99 67 66 30 F8
00002700 36 4E A2 A6 C7 55 7F AD 94 A5 B5 D7 88 08 08 F1
00002800 20 0B E2 37 09 85 99 13 BA BD 44 60 BB DD F8 ED
00002900 21 3E 7C 87 73 A4 B1 FA CE 30 F8 AC FD F0 93 B7
00002A00 05 08 08 00 05 88 96 0D 73 D7 19 01 03 F7 EF 15
```

```
.OpenTimestamps.
.Proof.....
....NP.&.gL.^...
...fx...;J7.kj.
@.....
;W.....{TEz.Iy
.V.|N..o.....kH
0E.!..S.....C8.
u.O.?....$.v-..
`.-.g....h..3B.v
...(.1|.....^
.....!...M.}+
3..P..KJ.$Z.V...
S.7N.....e
3.....v....W..
..tHbQ_[U.1..w/.
.....v....
.....3.
<1Lx.]5.L.?.,.I
....@.._....[
4....".U.x2.'!
.....].
.....G..]=FK
A[...f).....!M.$
2....a.o...<
>.....^.`H7.....?
...:.....K....
....k.fGB.N....M
=5e..K&.....
..i..$.4..H%~.a
...!S^DC!{..F...
.....$.K..
.).....WE[o&R...
....?.m`.D.k.
...H./....Hz....
k...6.....
...t..2...WGX...
.FN.Xr.u.....
.....gf0.
6N...U.....
...7.....D`....
!>|.s...0.....
.....S.....
```

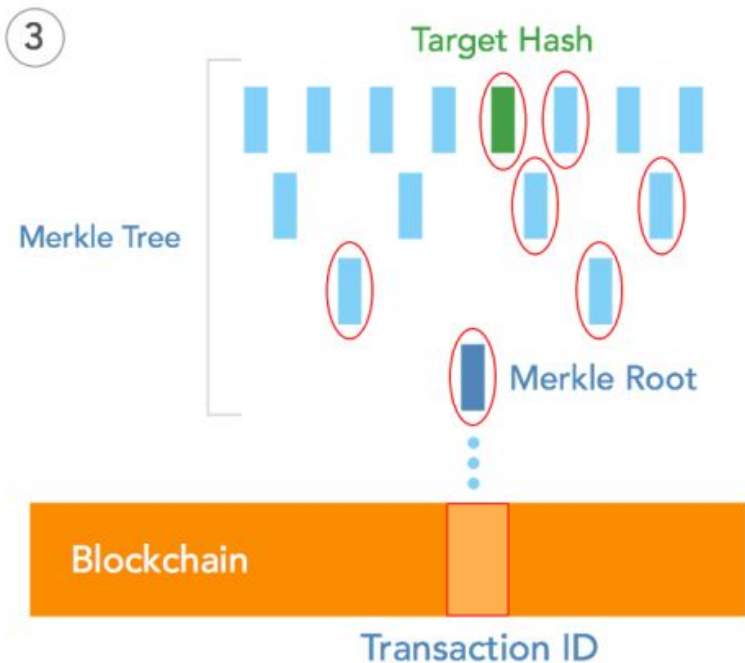

OpenTimestamps Merkle tree on the client



Agenda

- Why Timestamping @ Scaling
- Aggregating timestamps
- **Timestamping Proof formats**
 - OpenTimestamps
 - **Chainpoint**

Chainpoint



JSON-LD example of a Chainpoint 2.0 receipt:

```
{
  "@context": "https://w3id.org/chainpoint/v2",
  "type": "ChainpointSHA256v2",
  "targetHash": "bdf8c9bdf076d6aff0292a1c9448691d2ae283f2ce41b045355e2c8cb8e85ef2",
  "merkleRoot": "51296468ea48ddb5c546abb85b935c73058fd8acdb0b953da6aa1ae966581a7a",
  "proof": [
    {
      "left": "bdf8c9bdf076d6aff0292a1c9448691d2ae283f2ce41b045355e2c8cb8e85ef2"
    },
    {
      "left": "cb0dbbedb5ec5363e39be9fc43f56f321e1572cfcf304d26fc67cb6ea2e49faf"
    },
    {
      "right": "cb0dbbedb5ec5363e39be9fc43f56f321e1572cfcf304d26fc67cb6ea2e49faf"
    }
  ],
  "anchors": [
    {
      "type": "BTCOpReturn",
      "sourceId": "f3be82fe1b5d8f18e009cb9a491781289d2e01678311fe2b2e4e84381aafadee"
    }
  ]
}
```

Chainpoint Blockchain Receipt

Receipt Types:

Chainpoint 2.0 supports the following Secure Hashing Algorithm types.

ChainpointSHA224v2	Chainpoint 2.0 receipt using SHA-224
ChainpointSHA256v2	Chainpoint 2.0 receipt using SHA-256
ChainpointSHA384v2	Chainpoint 2.0 receipt using SHA-384
ChainpointSHA512v2	Chainpoint 2.0 receipt using SHA-512
ChainpointSHA3-224v2	Chainpoint 2.0 receipt using SHA3-224
ChainpointSHA3-256v2	Chainpoint 2.0 receipt using SHA3-256
ChainpointSHA3-384v2	Chainpoint 2.0 receipt using SHA3-384
ChainpointSHA3-512v2	Chainpoint 2.0 receipt using SHA3-512

Anchor Types:

Chainpoint 2.0 supports the following anchor types. Additional anchor types are under development.

BTCOpReturn	Anchored to a Bitcoin transaction within an OP_RETURN output
ETHData	Anchored to an Ethereum transaction using the data field

Chainpoint

JSON-LD

```
{
  "@context": "https://w3id.org/chainpoint/v2",
  "type": "ChainpointSHA256v2",
  "targetHash": "8588e72758782320ad91244b76113c30ba88df2384d9a4c0b75791540dfcdf",
  "merkleRoot": "1780c0b33885414a9020b87192a2aa51017b63f3ed66f273388ec6f0665208a7",
  "proof": [
    {
      "left": "167106490d2f599c596725608991f3cb8abea861cdd46a084e4b346e4f367c27"
    },
    {
      "right": "b41bcfad77ddb187001944112d4d628a56ee9c68a3d6495619518d2a90ffbc52"
    },
    {
      "right": "7ac298b30ea49ec55d02c60086d870ac957072188815737720f4bdf74dbc990e"
    }
  ],
  "anchors": [
    {
      "type": "BTCOpReturn",
      "sourceId": "7282594965e4220acb8e2b97f1e21f230fd7adb1f8828dc979b5b3457d2ca4be"
    }
  ]
}

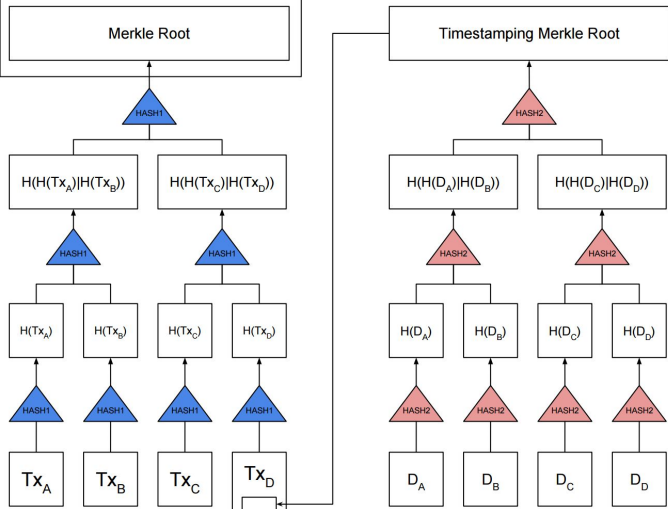
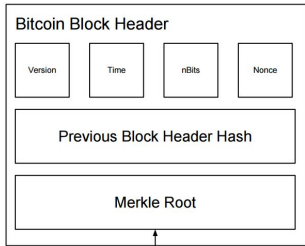
{
  "@context": "https://w3id.org/chainpoint/v2",
  "type": "ChainpointSHA256v2",
  "targetHash": "8588e72758782320ad91244b76113c30ba88df2384d9a4c0b75791540dfcdf",
  "merkleRoot": "1780c0b33885414a9020b87192a2aa51017b63f3ed66f273388ec6f0665208a7",
  "proof": [
    {
      "left": "167106490d2f599c596725608991f3cb8abea861cdd46a084e4b346e4f367c27"
    },
    {
      "right": "b41bcfad77ddb187001944112d4d628a56ee9c68a3d6495619518d2a90ffbc52"
    },
    {
      "right": "7ac298b30ea49ec55d02c60086d870ac957072188815737720f4bdf74dbc990e"
    }
  ],
  "anchors": [
    {
      "type": "ETHData",
      "sourceId": "0xef16a47d4d05ae31c36b058c1caf8a1566089f4e43f22a62dc1475a3cc2c1b7c"
    }
  ]
}
```

Same
target
hash

(fake receipt)

Chainpoint

JSON-LD



```

{
  "@context": "https://w3id.org/chainpoint/v2",
  "type": "ChainpointSHA256v2",
  "targetHash": "8588e72758782320ad91244b76113c30ba88df2384d9a4c0b75791540dfcdf",
  "merkleRoot": "1780c0b33885414a9020b87192a2aa51017b63f3ed66f273388ec6f0665208a7",
  "proof": [
    {
      "left": "167106490d2f599c596725608991f3cb8abea861cdd46a084e4b346e4f367c27"
    },
    {
      "right": "b41bcfad77ddb187001944112d4d628a56ee9c68a3d6495619518d2a90ffbc52"
    },
    {
      "right": "7ac298b30ea49ec55d02c60086d870ac957072188815737720f4bdf74dbc990e"
    }
  ],
  "anchors": [
    {
      "type": "BTCOpReturn",
      "sourceId": "7282594965e4220acb8e2b97f1e21f230fd7adb1f8828dc979b5b3457d2ca4be"
    }
  ]
}

```

```

{
  "@context": "https://w3id.org/chainpoint/v2",
  "type": "ChainpointSHA3256v2",
  "targetHash": "8588e72758782320ad91244b76113c30ba88df2384d9a4c0b75791540dfcdf",
  "merkleRoot": "1780c0b33885414a9020b87192a2aa51017b63f3ed66f273388ec6f0665208a7",
  "proof": [
    {
      "left": "167106490d2f599c596725608991f3cb8abea861cdd46a084e4b346e4f367c27"
    },
    {
      "right": "b41bcfad77ddb187001944112d4d628a56ee9c68a3d6495619518d2a90ffbc52"
    },
    {
      "right": "7ac298b30ea49ec55d02c60086d870ac957072188815737720f4bdf74dbc990e"
    }
  ],
  "anchors": [
    {
      "type": "ETHData",
      "sourceId": "0xef16a47d4d05ae31c36b058c1caf8a1566089f4e43f22a62dc1475a3cc2c1b7c"
    }
  ]
}

```

Same target hash

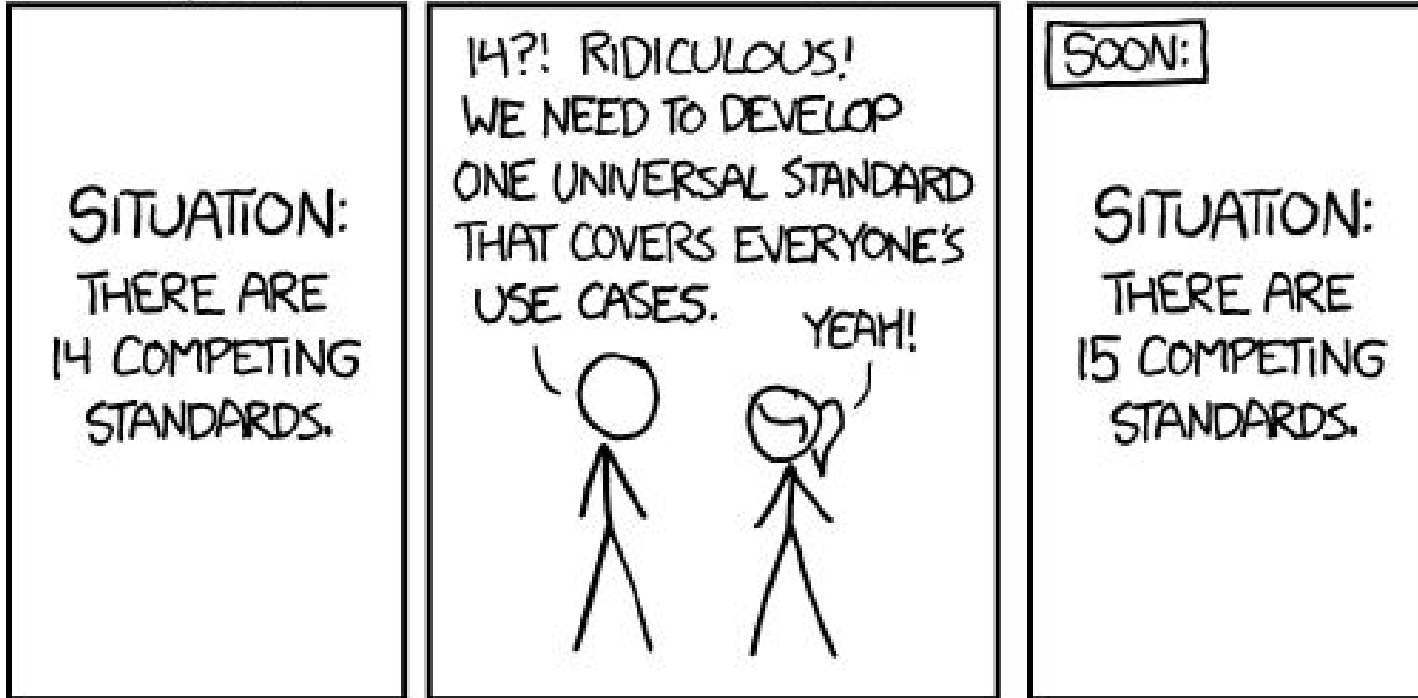
(fake receipt)

Chainpoint compression

Plain JSON	586 bytes	
MsgPack	546 bytes	93%
gzipped	423 bytes	72%
MsgPack + Gzip	418 bytes	71%

HOW STANDARDS PROLIFERATE:

(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC.)



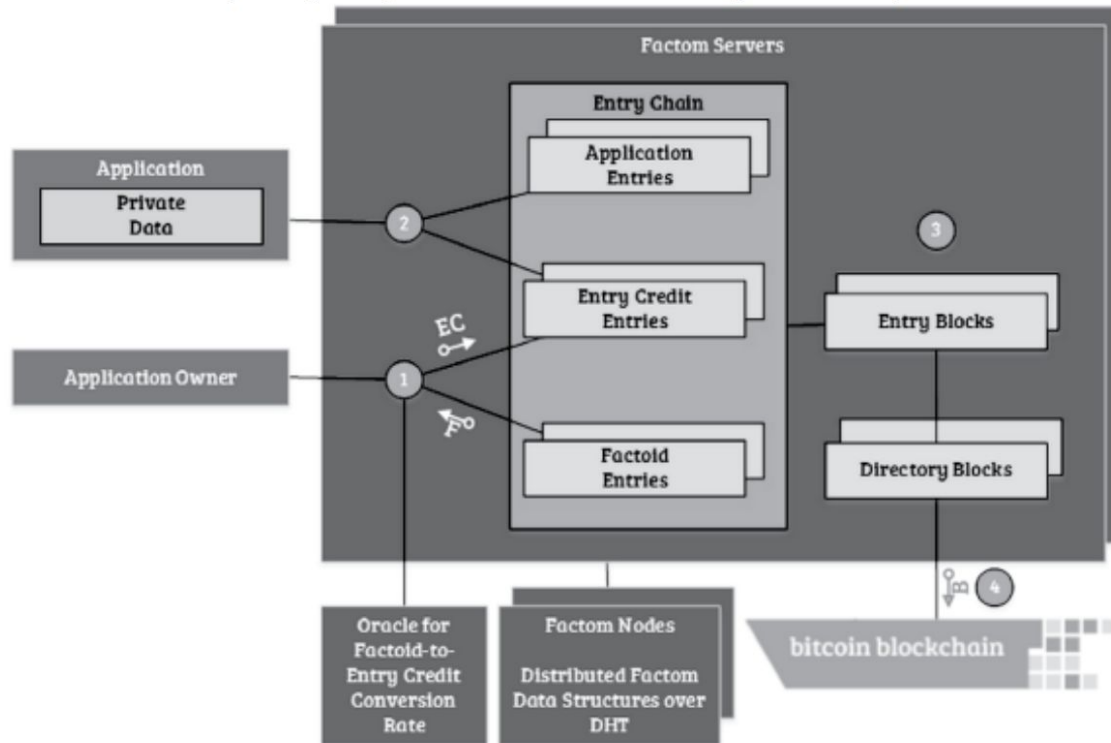
Slides soon available on twitter @RCasatta

Thanks to Giacomo Zucco, Mir Liponi, Peter Todd.

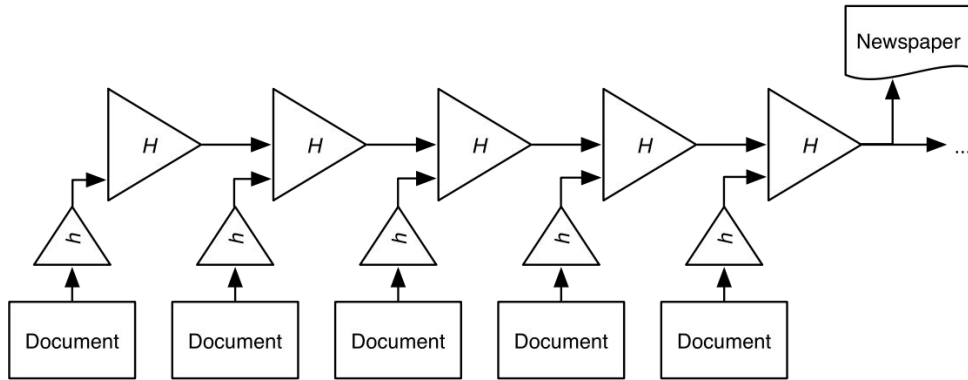
Trusted Timestamping (OT)

- Difference between trustless and trusted timestamping
- Linked Timestamping - Guardtime ⁽⁶⁾
- Roughtime ⁽⁷⁾

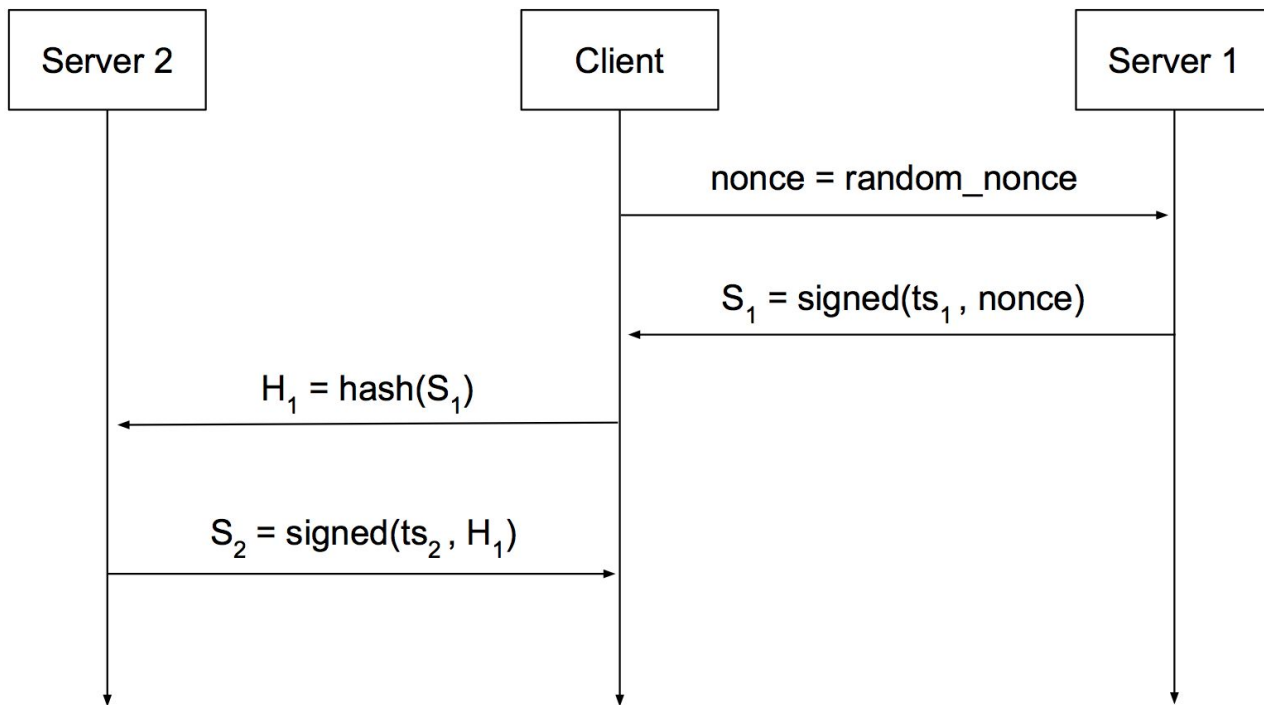
Comparison - Factom



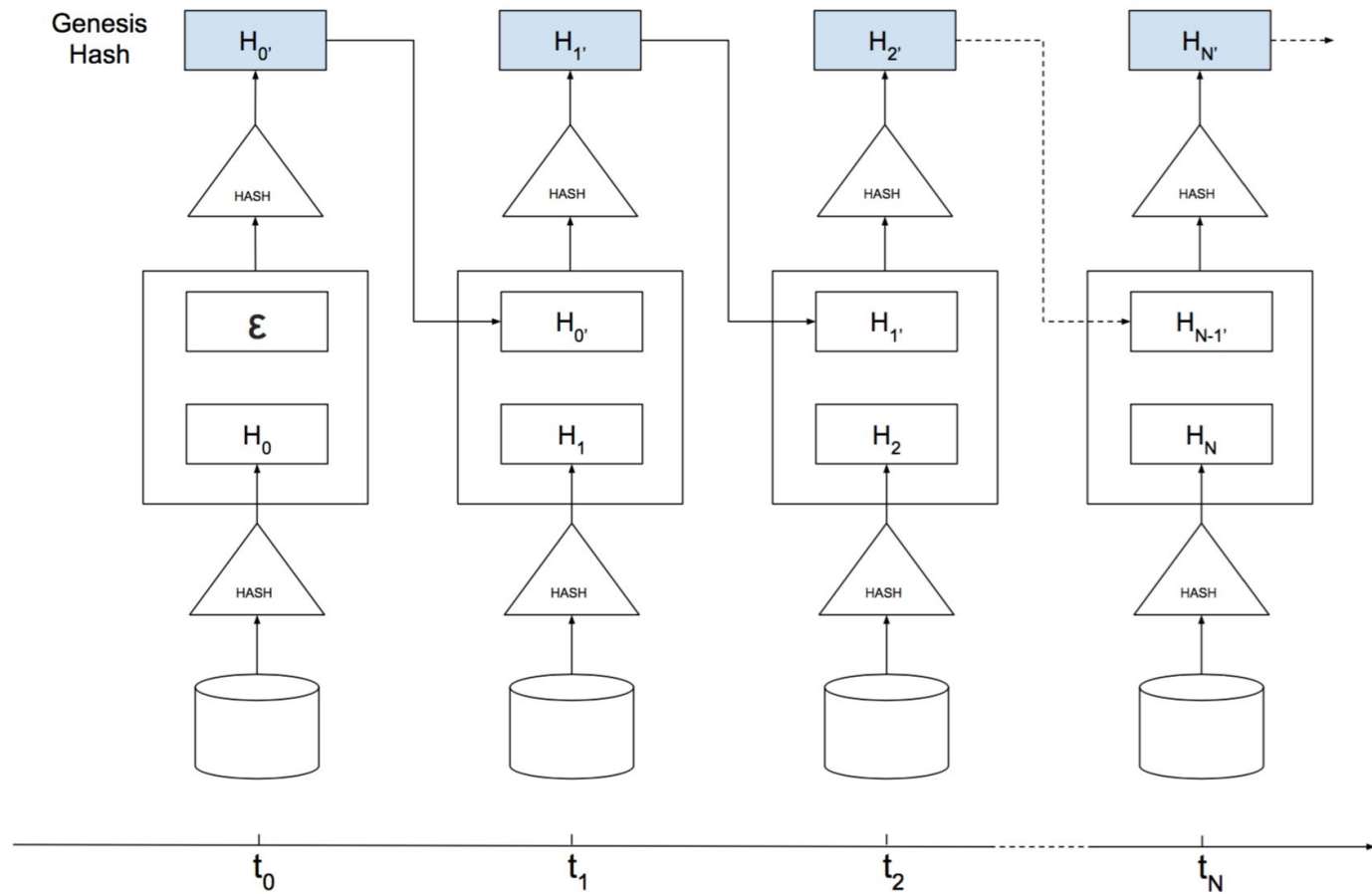
Guardtime - Trusted Timestamping (OT)



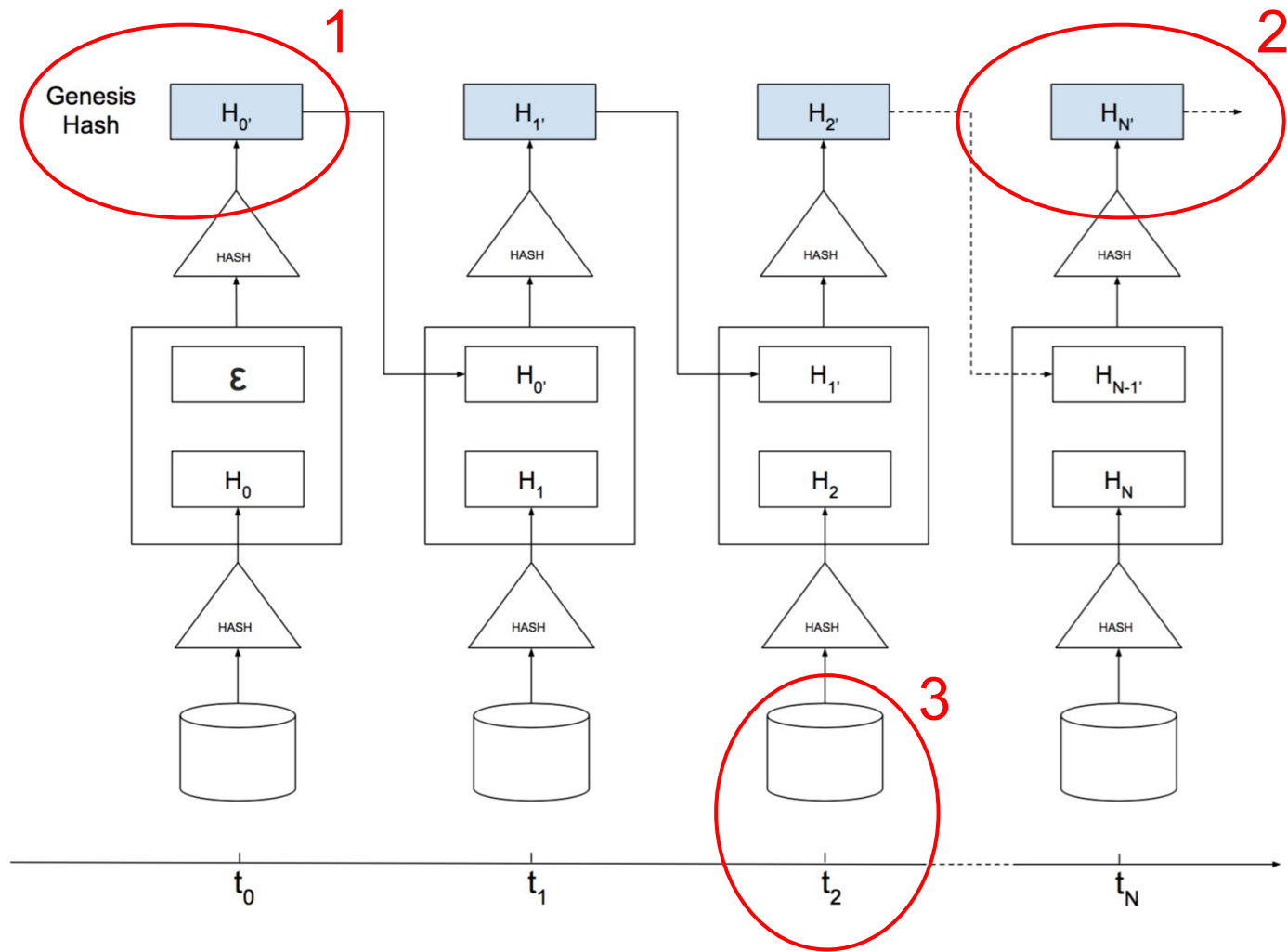
Roughtime - Trusted Timestamping (OT)



Hashchain



Hashchain



Hashchain

✓ scalability

✓ proof of (past) publication

