Do I need a blockchain?

A quick appraisal

Marco d'Itri
<md@linux.it>
@rfc1036

Italian Hacker Camp 2018 - 3 August 2018

What is a Merkle tree?

A way to efficiently distribute authenticated data:

- A graph representing some data: generally, a binary tree.
- Each node contains the hashes of its child nodes.
- Specific data can be verified by accessing only some branches.

The tree can be downloaded from non-trusted entities and its content verified by everybody who knows the hash at the root of the tree.

Who decides which tree is the true one?

A mechanism to build distributed consensus is needed to agree on what is the current root hash.

Central authority:

- A trusted entity adds new entries and publishes the tree.
- Everybody else can use the root hash to verify the data.

Blockchain:

- Nodes cooperate to add new entries and reach a consensus.
- Everybody else can verify the consensus reached about the data.

A blockchain removes the need to trust third parties!

Do I need a blockchain?

You don’t need a blockchain.

- A blockchain is just a slow database (also: really expensive).
- Most people find practical to trust third parties.

Any questions?

`https://www.linux.it/~md/text/blockchain-ihc2018.pdf`

(Google . . . Marco d'Itri . . . I feel lucky)