Blockchain & Healthcare Standards

Disclaimer

Ewout Kramer
FHIR Core team (and software developer)
Chair HL7 FHIR-Infrastructure WG
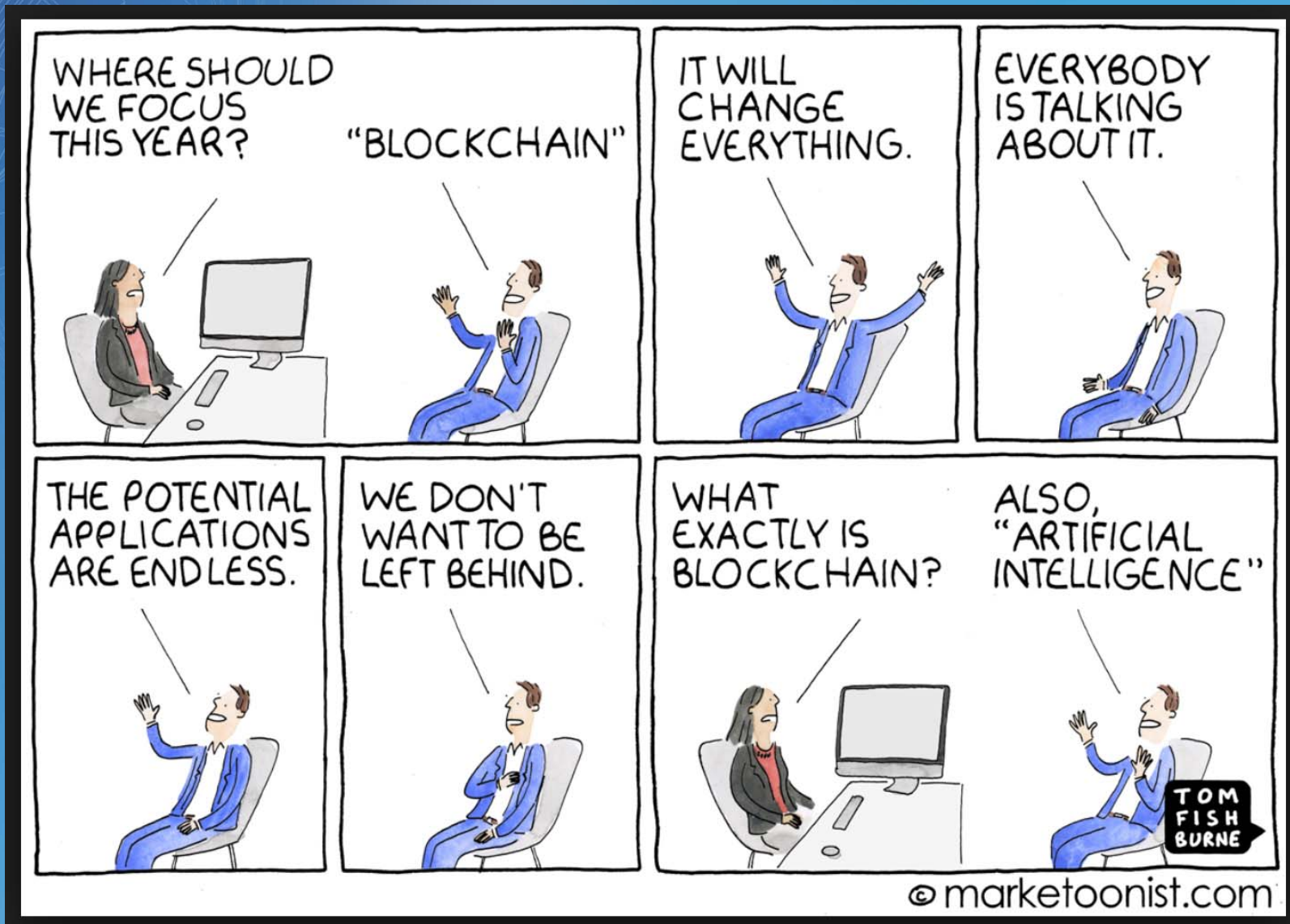Board of FHIR Foundation
CTO of Firely (Amsterdam, NL)

email: ewout@fire.ly
web: http://blog.fire.ly
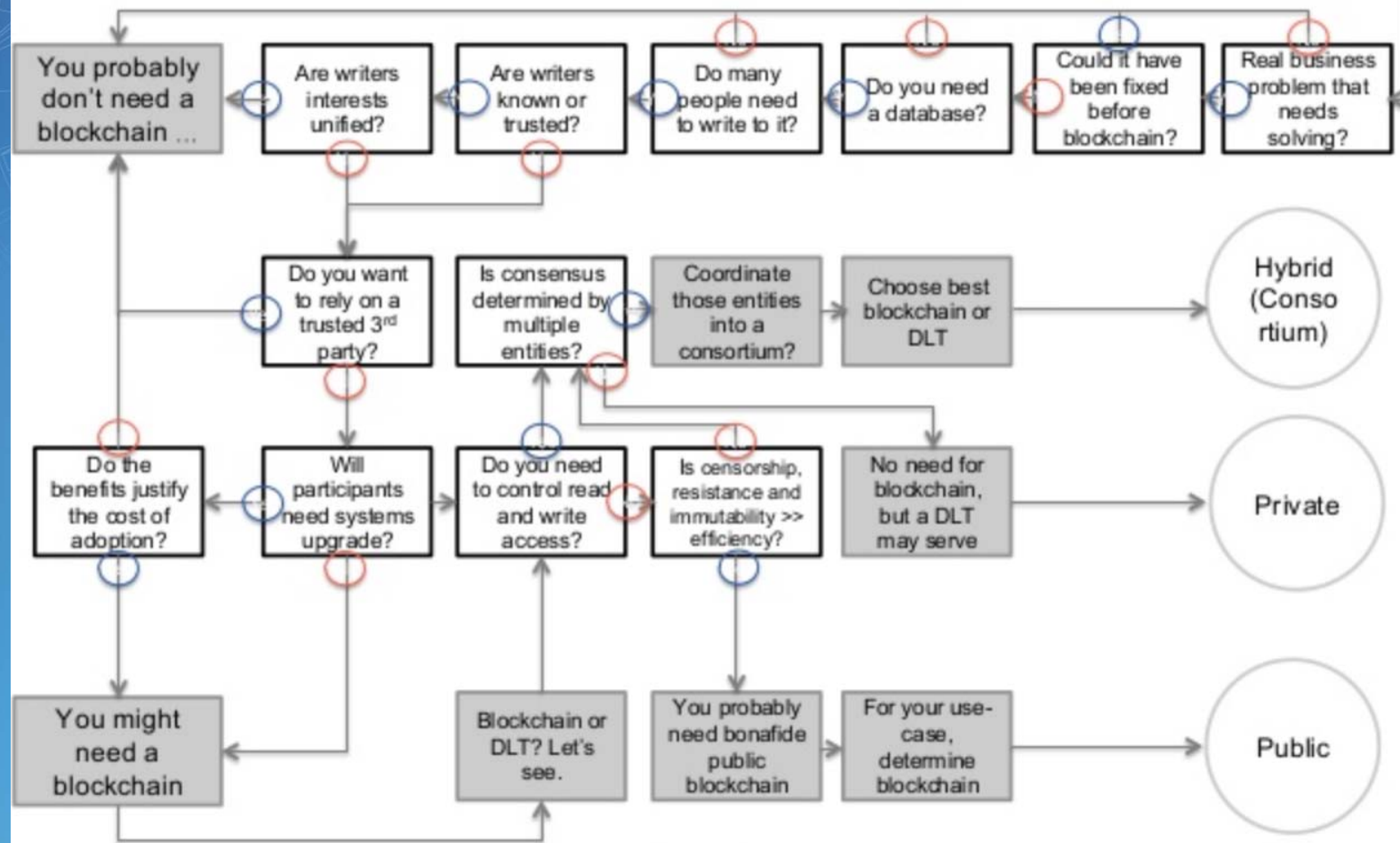
skype: ewoutkramer

Note: Not a Blockchain expert

Do you really need a blockchain? START

You probably don't need a blockchain …

- Are writers interests unified?
- Are writers known or trusted?
- Do many people need to write to it?
- Do you need a database?
- Could it have been fixed before blockchain?
- Real business problem that needs solving?

- Do you want to rely on a trusted 3rd party?
- Is consensus determined by multiple entities?
- Coordinate those entities into a consortium?
- Choose best blockchain or DLT
- Hybrid (Consortium)

- Do the benefits justify the cost of adoption?
- Will participants need systems upgrade?
- Do you need to control read and write access?
- Is censorship, resistance and immutability >> efficiency?
- No need for blockchain, but a DLT may serve
- Private

- You might need a blockchain
- Blockchain or DLT? Let's see.
- You probably need bonafide public blockchain
- For your use-case, determine blockchain
- Public
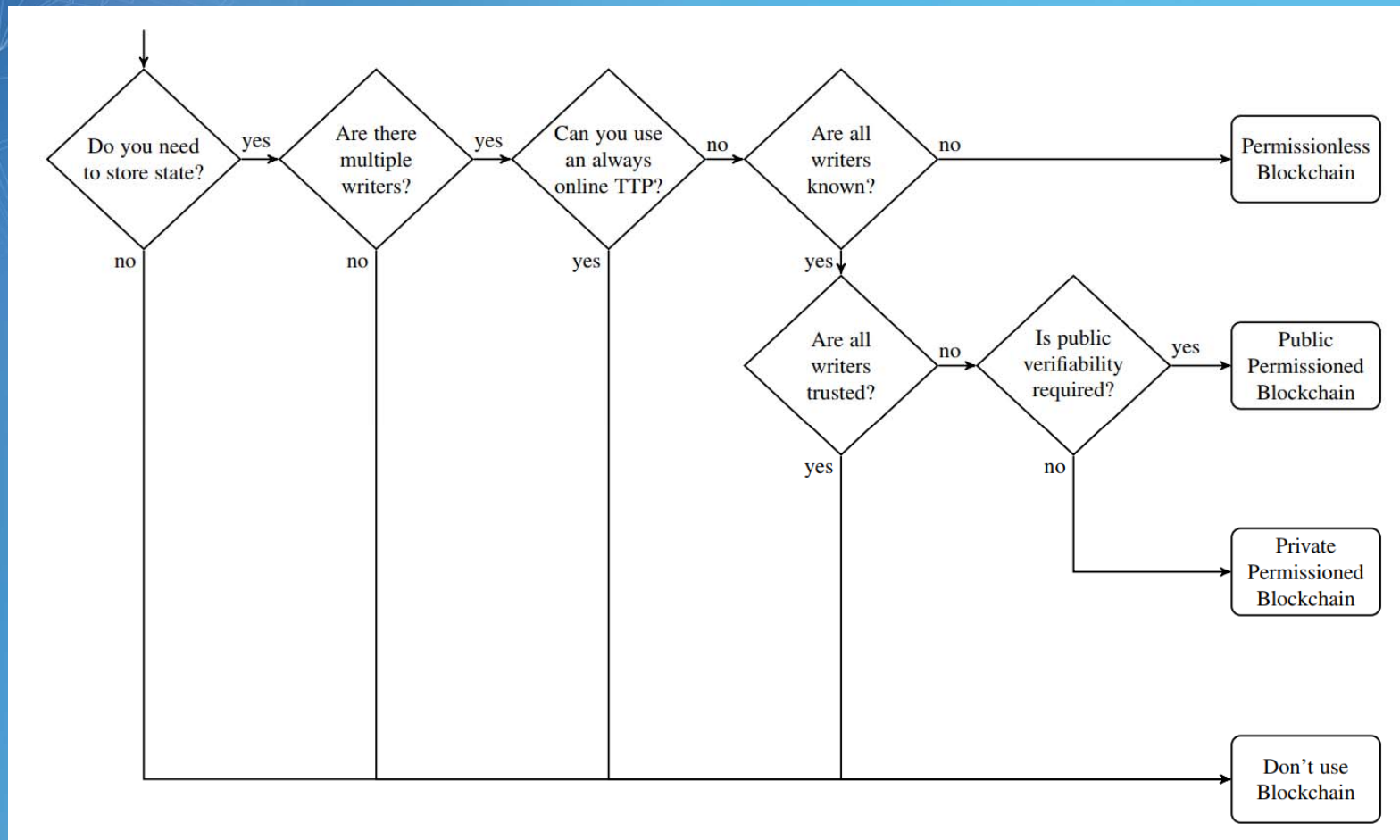
Source: Distributed magazine (issue #01), Jeremy Gardner

/slash

45

From: Karl Wüst∗ , Arthur Gervais† - "Do you need a Blockchain?"

So what is blockchain good at?

"In general, using (...) Blockchain only makes sense when multiple mutually mistrusting entities want to interact and change the state of a system, and are not willing to agree on an online trusted third party."

1

Do you need a Blockchain?

Karl Wüst*, Arthur Gervais†
*karl.wuest@inf.ethz.ch, †arthur.gervais@inf.ethz.ch
Department of Computer Science
ETH Zurich, Switzerland

— ◆ —

Abstract—Blockchain is being praised as a technological innovation which allows to revolutionize how society trades and interacts. This reputation is in particular attributable to its properties of allowing mutually mistrusting entities to exchange financial value and interact without relying on a trusted third party. A blockchain moreover provides an integrity protected data storage and allows to provide process transparency.
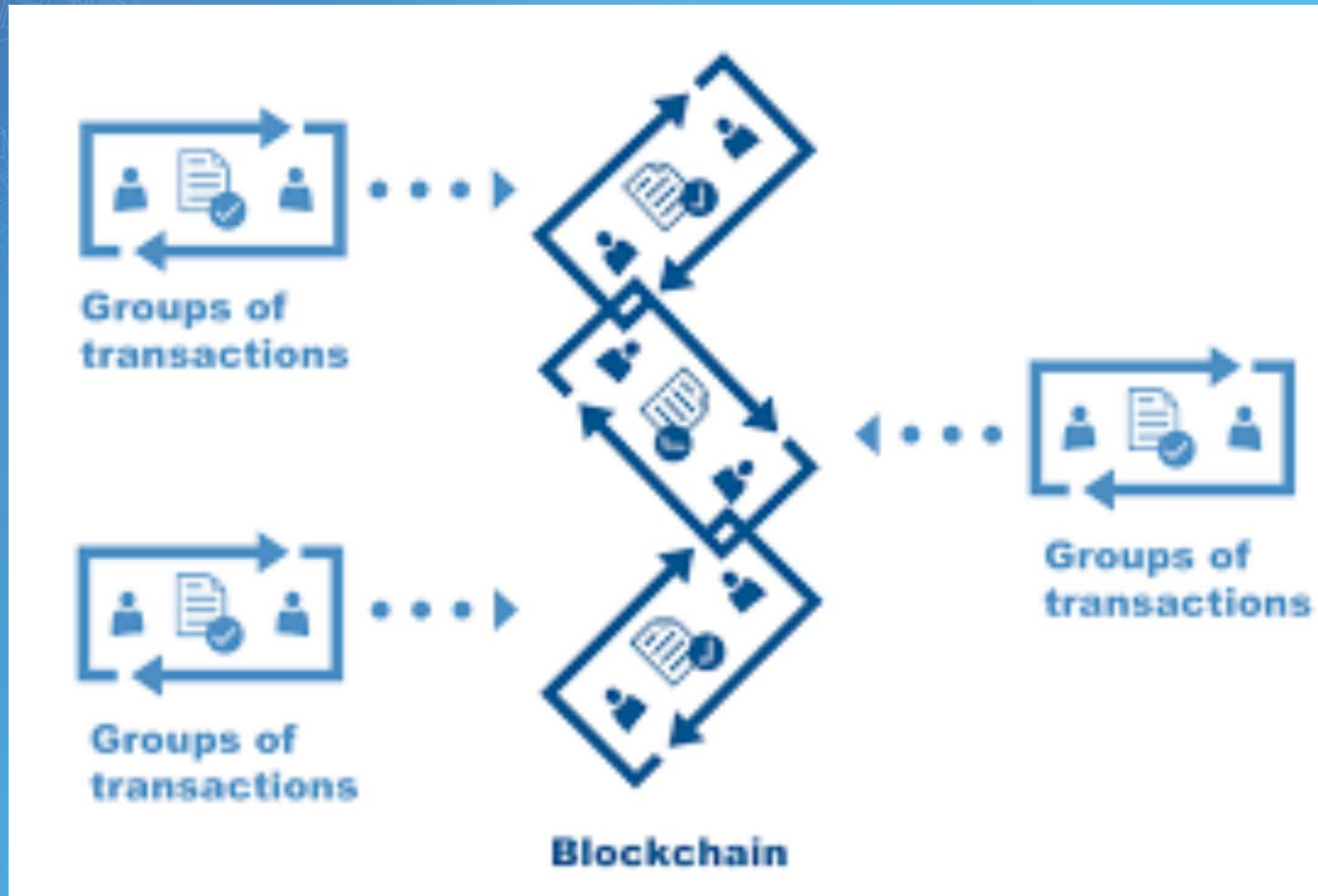
In this article we critically analyze whether a blockchain is indeed the appropriate technical solution for a particular application scenario. We differentiate between permissionless (e.g., Bitcoin/Ethereum) and permissioned (e.g. Hyperledger/Corda) blockchains and contrast their properties to those of a centrally managed database. We provide a structured methodology to determine the appropriate technical solution to solve a particular application problem. Given our methodology, we analyze in depth three use cases — Supply Chain Management, Interbank and International Payments, and Decentralized Autonomous Organizations and conclude the article with an outlook for further opportunities.

The remainder of this article is organized as follows. In Section 2, we briefly describe the most important background about blockchain. In Section 3 we provide a structured methodology to identify if a blockchain makes sense, and if yes, which type of blockchain would be appropriate. Based on our methodology, we analyze proposed use cases in detail in Section 4. In Section 5, we review related work in the area, and we conclude the article in Section 6.

2 BACKGROUND ON BLOCKCHAIN

In the following section, we detail the required blockchain background and the involved parties. The name blockchain stems from its technical structure — a chain of blocks. Each block is linked to the previous block with a cryptographic hash. A block is a datastructure which allows to store a list of transactions.

What is blockchain (simplified)

Groups of transactions

Groups of transactions

Groups of transactions

Blockchain

Bitcoin *distributed* network

GLOBAL BITCOIN NODES DISTRIBUTION
Reachable nodes as of Tue Mar 06 2018
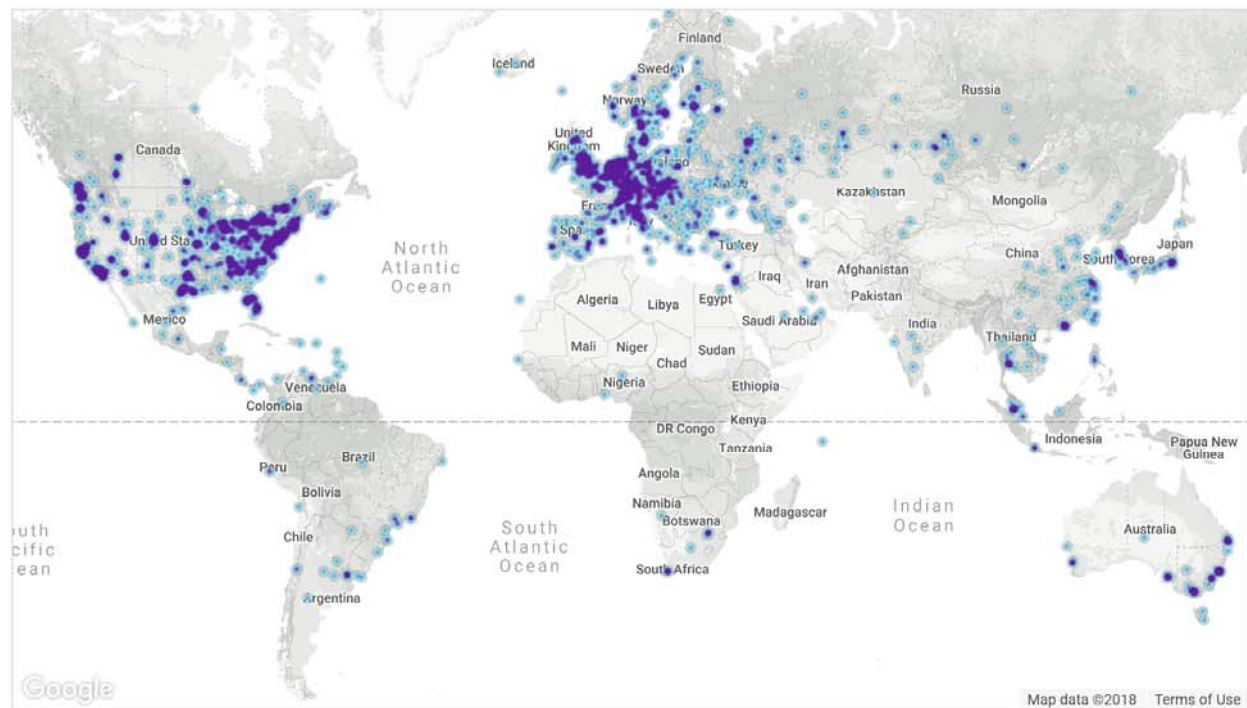07:25:25 GMT-0800 (Pacific Standard Time).

11799 NODES
24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	2754 (23.34%)
2	Germany	2034 (17.24%)
3	China	1567 (13.28%)
4	France	755 (6.40%)
5	Netherlands	533 (4.52%)
6	Canada	422 (3.58%)
7	United Kingdom	380 (3.22%)
8	Russian Federation	374 (3.17%)
9	n/a	268 (2.27%)
10	Singapore	227 (1.92%)

More (102) »

Aspects of a blockchain

- Low throughput (for example 7-66 transactions/second for the Bitcoin network)
- Data is copied across multiple nodes
- Works best with small amounts of data
- Data is public & verifiable
- Ordered in time
- Is a ledger – not a database

So, what about this?

"Healthcare is very suitable for blockchain, because a lot of data is still stored in data silos at hospitals, doctors, health insurers and other institutions. With cryptographic technology can enable secure exchange, so that they communicate with each other."

So, let's try some use cases

- **EU GDPR "right to be forgotten" logging**
  - Small amount of data
  - Lack of trust
  - Not privacy sensitive (but what about other kinds of consent?)

So, let's try some use cases

- **Medication intake, blood pressure monitors, IoT measurements**
  - Problem: How to extend trust from the digital to the physical?
  - Small amounts of data, but possibly lots of it
  - Privacy

So, let's try some use cases

- **Organ Donor Registry**
  - Small amount of data, low # of transactions
  - How to establish identity?
  - Privacy versus accessibility
  - Often there is a TTP

So, let's try some use cases

- **Provider certification registry**
  - Little amount of data, low latency ok
  - Small number of "writers"
  - Pre-existing agreements between parties
  - Needs trust "in the physical world"

Digital & Physical – effect on trust

- In the ubiquitous example – bitcoin – the information in the ledger represents the only reality – it's fully digital. Even the identities!

- In Healthcare there's an interface between the digital and physical world
  - There is a human healthcare process involved
  - Most of the time this requires a framework of trust outside of the blockchain
  - In any case we need to connect digital identities to physical entities

Conclusions so far

- "Open" blockchain less applicable, maybe put attention to more restricted types of blockchains (which may just be fancy distributed databases)
- (FHIR) Consent resource primary candidate
- Creating a fingerprint insensitive to "bit rot"
- Fixing the identity problem

- The last two are being piloted in other industries and will see resolution in the next 18 months – just sit & wait
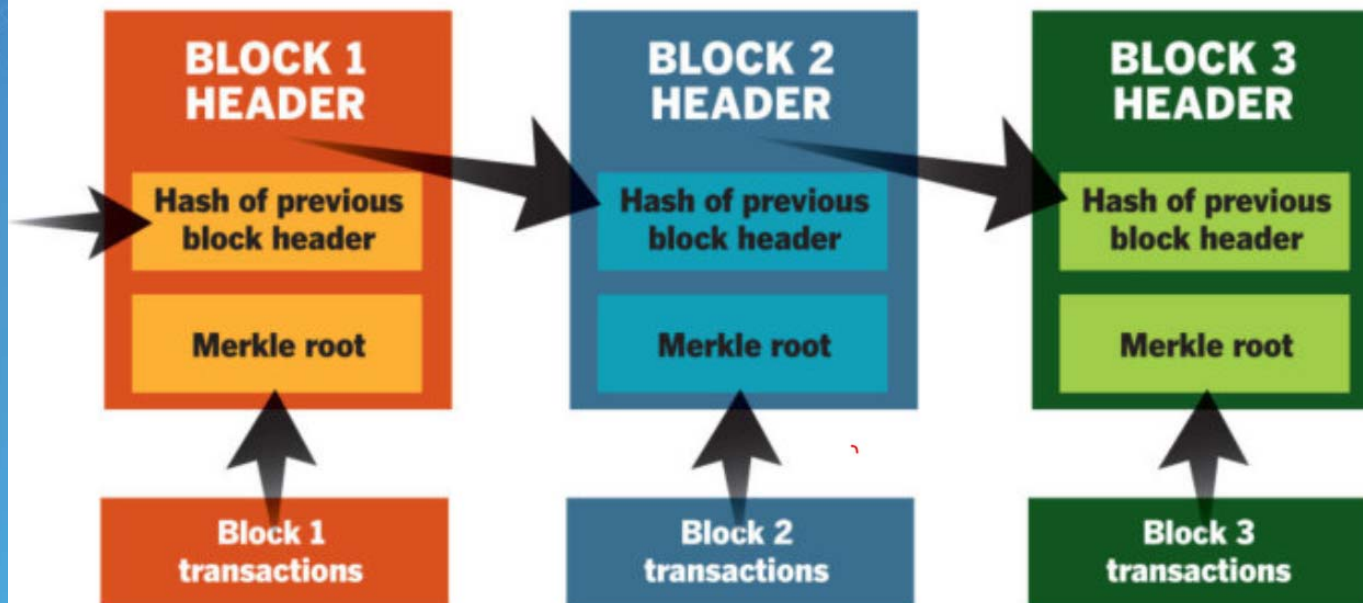
QUESTIONS?

email: ewout@fire.ly
web: http://blog.fire.ly

skype: ewoutkramer

To blockchain or not? A sliding scale...

	Assertion	Answer	
Network	A significant number of participants will be transacting on the network (>100)	Agree/Yes	☐
	You don't trust the participants in the network and don't need/want to know them	Agree/Yes	☐
Performance	A limited amount of data needs to be stored for every transaction (a few fields)	Agree/Yes	☐
	The business process doesn't requires a high throughput (scalability)	Agree/Yes	☐
Business logic	The business logic is simple	Agree/Yes	☐
	Privacy of transactions is not an important feature	Agree/Yes	☐
	The system will be standalone, it doesn't need to access external data or be integrated in the IT legacy	Agree/Yes	☐
Consensus	No arbitrator shall be involved in case of a dispute	Agree/Yes	☐
	All participants can be involved in the validation of transactions (Vs only a group of known validators)	Agree/Yes	☐
	You need strict immutability of the record (no amend & cancel, even by admin)	Agree/Yes	☐

With blockchain technology, each page in a ledger of transactions forms a block. That block has an impact on the next block or page through cryptographic hashing. In other words, when a block is completed, it creates a unique secure code, which ties into the next page or block, creating a chain of blocks, or blockchain.

BLOCK 1 HEADER	BLOCK 2 HEADER	BLOCK 3 HEADER
Hash of previous block header	Hash of previous block header	Hash of previous block header
Merkle root	Merkle root	Merkle root
Block 1 transactions	Block 2 transactions	Block 3 transactions

SIMPLIFIED BITCOIN BLOCK CHAIN

- **Permissionless Blockchain**
- **Permissioned Blockchain (writers are known)**
- **When does a blockchain simply becomes a fancy new centralized database**
- **Solves technical trust, but most of the time you need to establish trust using regulations and out-of-band agreements on data standards etc. so you become a set of known-writiers -> BC still necessary?**

So, let's try some use cases

- GDPR "right to be forgotten"
- Organ Donor Registry
- Consent to data processing and sharing
- Immunization registry
- Provider certification registry
- Receipt of medication dispense
- Medication Administration log
- Claims & reimbursement