Open Data and Blockchains:

An Opportunity to Re-Imagine your Business?

A (very) short introduction to Blockchain

Vassilios Vescoukis

Associate Professor, National Technical University of Athens

OKF Greece, member of the BoD

Opening statements

What this talk is about...

This talk...

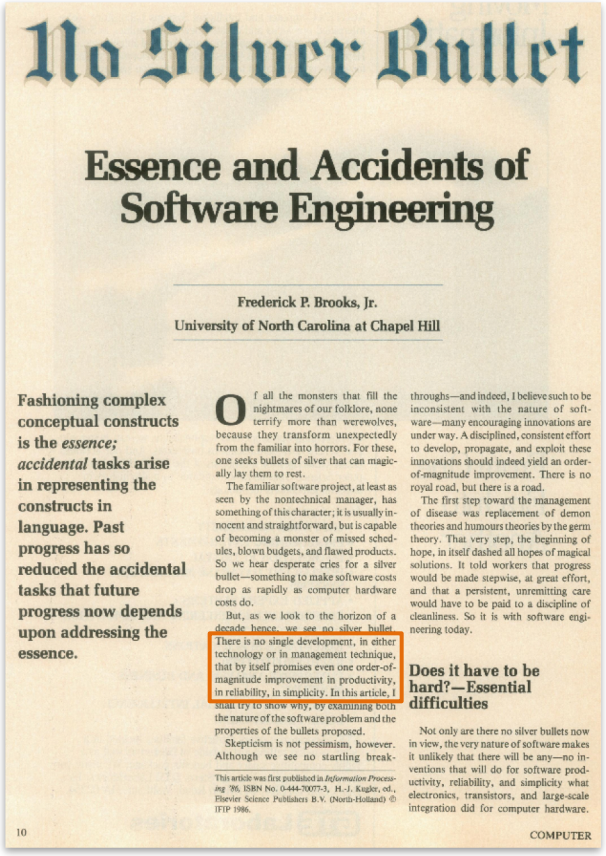
...is not...

- an academic lecture on Blockchain
- an unconditional praise of Blockchain
- focused on some specific Blockchain development tool / environment / ecosystem

...is about...

- introducing the basic principles behind Blockchain
- providing a non-financial example
- setting the context for discussing challenges introduced by Blockchain

No silver bullet...



No Silver Bullet

Essence and Accidents of Software Engineering

Frederick P. Brooks, Jr.
University of North Carolina at Chapel Hill

Fashioning complex conceptual constructs is the *essence;* *accidental* tasks arise in representing the constructs in language. Past progress has so reduced the accidental tasks that future progress now depends upon addressing the essence.

Of all the monsters that fill the nightmares of our folklore, none terrify more than werewolves, because they transform unexpectedly from the familiar into horrors. For these, one seeks bullets of silver that can magically lay them to rest.

The familiar software project, at least as seen by the nontechnical manager, has something of this character; it is usually innocent and straightforward, but is capable of becoming a monster of missed schedules, blown budgets, and flawed products. So we hear desperate cries for a silver bullet—something to make software costs drop as rapidly as computer hardware costs do.

But, as we look to the horizon of a decade hence, we see no silver bullet. There is no single development, in either technology or in management technique, that by itself promises even one order-of-magnitude improvement in productivity, in reliability, in simplicity. In this article, I shall try to show why, by examining both the nature of the software problem and the properties of the bullets proposed.

Skepticism is not pessimism, however. Although we see no startling breakthroughs—and indeed, I believe such to be inconsistent with the nature of software—many encouraging innovations are under way. A disciplined, consistent effort to develop, propagate, and exploit these innovations should indeed yield an order-of-magnitude improvement. There is no royal road, but there is a road.

The first step toward the management of disease was replacement of demon theories and humours theories by the germ theory. That very step, the beginning of hope, in itself dashed all hopes of magical solutions. It told workers that progress would be made stepwise, at great effort, and that a persistent, unremitting care would have to be paid to a discipline of cleanliness. So it is with software engineering today.

Does it have to be hard?—Essential difficulties

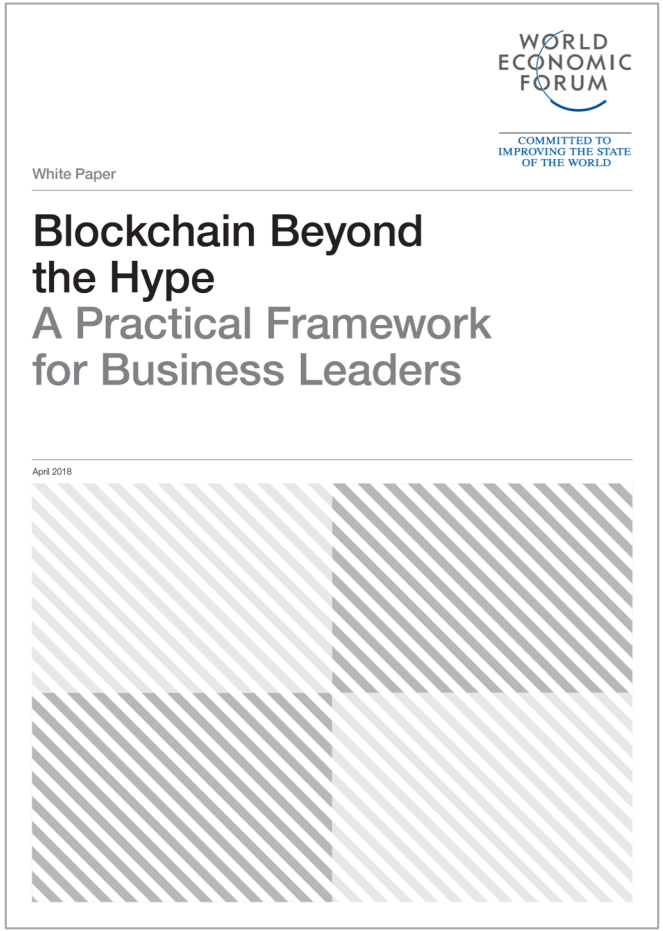
Not only are there no silver bullets now in view, the very nature of software makes it unlikely that there will be any—no inventions that will do for software productivity, reliability, and simplicity what electronics, transistors, and large-scale integration did for computer hardware.

This article was first published in *Information Processing '86*, ISBN No. 0-444-70077-3, H.-J. Kugler, ed., Elsevier Science Publishers B.V. (North-Holland) © IFIP 1986.

"There is no single development, in either technology or management technique, which by itself promises even one order of magnitude improvement in productivity, in reliability, in simplicity"

Frederick P. Brooks, Jr.. 1987.
No Silver Bullet Essence and Accidents of Software Engineering.
Computer 20, 4 (April 1987), 10-19. DOI=10.1109/MC.1987.1663532
http://dx.doi.org/10.1109/MC.1987.1663532

Hype or not?


WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

White Paper

Blockchain Beyond the Hype

A Practical Framework for Business Leaders

April 2018

hype[1]

/hʌɪp/

informal

noun

noun: **hype**

1. extravagant or intensive publicity or promotion.
   "his first album hit the stores amid a storm of hype"
   synonyms: publicity, advertising, promotion, marketing, puff, puffery, propaganda, exposure; More
   - a deception carried out for the sake of publicity.
     plural noun: **hypes**
     "is his comeback a hype?"

verb

verb: **hype**; 3rd person present: **hypes**; past tense: **hyped**; past participle: **hyped**; gerund or present participle: **hyping**

1. promote or publicize (a product or idea) intensively, often exaggerating its benefits.
   "an industry quick to hype its products"
   synonyms: publicize, advertise, promote, push, boost, merchandise, give publicity to, give a puff to, puff, puff up, build up, talk up, beat/bang the drum for; *informal* plug
   "this was another stunt to hype a new product"
   antonyms: play down

Key concepts

Key concepts

Database

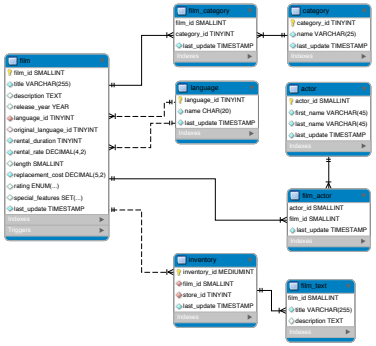
- A collection of data that is organized so that it can be easily accessed, managed and updated
- Data organization is achieved using a data model (conceptual, logical, physical)

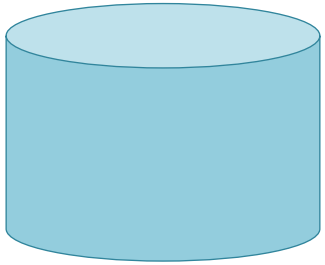
Ledger

- A write-once { database | *table* | *relation* | *catalogue* | *list* | *data structure* | ... }
- You can only add new records on a ledger
- *Can* be implemented on a RDBMS
- Implied simpler structure than a Database, though not necessary
- Often confused with specific implementation contexts, especially Blockchains

Key concepts

DATABASE

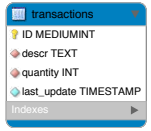


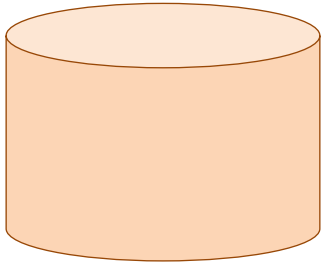


ID	DESCRIPTION	VALUE
1	Purchase	100
2	Purchase	200
3	Sale	-400
4	Sale	-30

ID	DESCRIPTION	VALUE
1	Purchase	100
2	Purchase	200
3	Sale	**-40**
4	Sale	-30

LEDGER



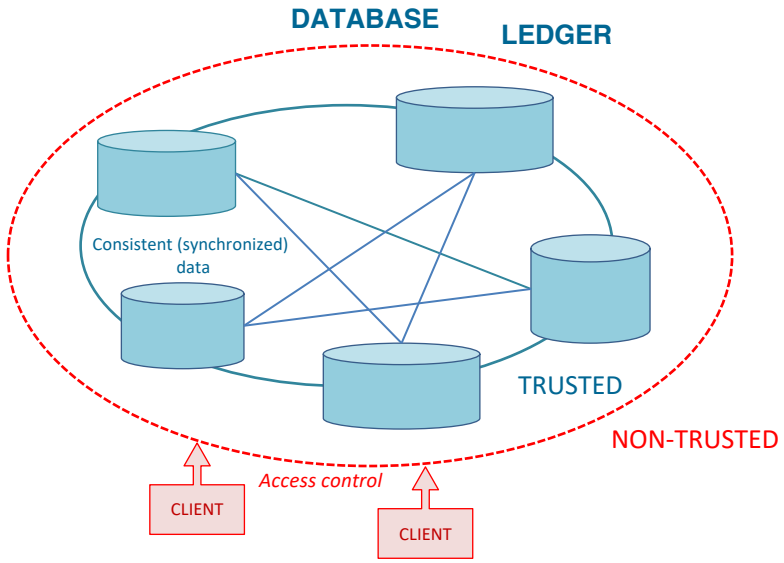


ID	DESCRIPTION	VALUE
1	Purchase	100
2	Purchase	200
3	Sale	-400
4	Correction	400
5	Sale	-40
6	Sale	-30

Key concepts

Distributed

- Databases can be distributed
- Distribution is about redundancy, fault tolerance, performance, etc.
- Ledgers can be distributed, too, for the same reasons!
- Notice the "boundary of trust"



Shared

- Data is synched outside the trust boundary
- Shared ledgers are by definition distributed

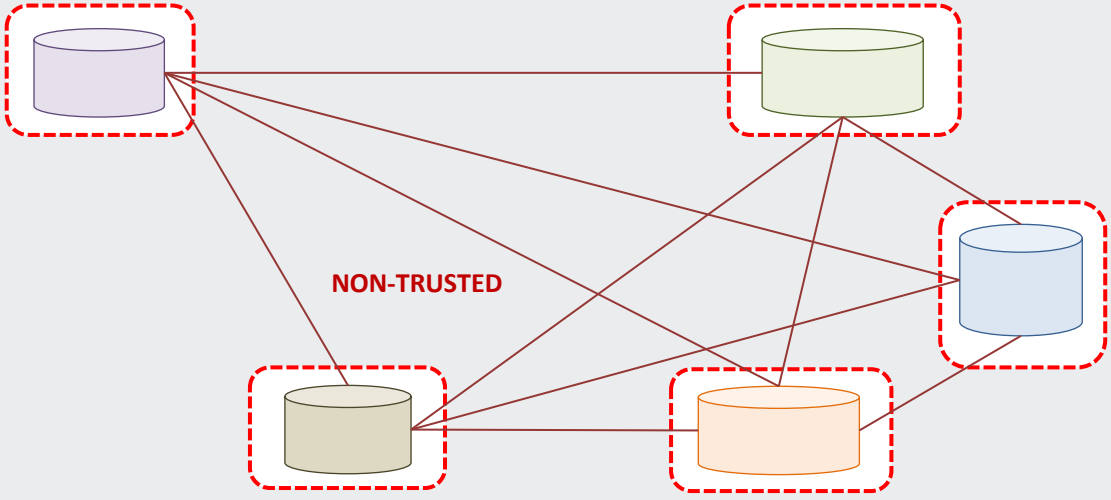
Key concepts

Distributed implementation alone, is not sufficient for a ledger to be characterized as "distributed ledger" in the context of Blockchain terminology

The boundary of trust makes the difference!

Distributed ledgers

A Blockchain *is* a distributed ledger; the opposite is not always true

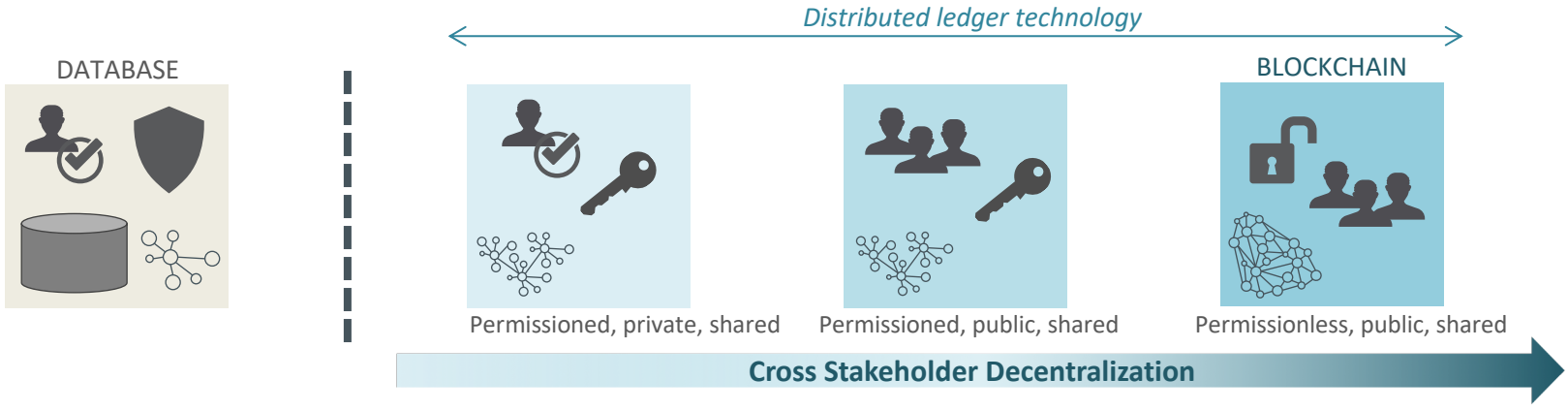


Definitions and the like...

Blockchain as a technology paradigm

Blockchain refers to a family of technologies that support the sharing of ledgers in a way that...

- Transactions are immutable (final, append-only), organized into "chains" of "blocks"
- Business logic is implemented as contracts that define conditions for transactions to happen
- Cryptography is used to protect and validate data
- Neither trust between parties, nor any "third trusted party" is required



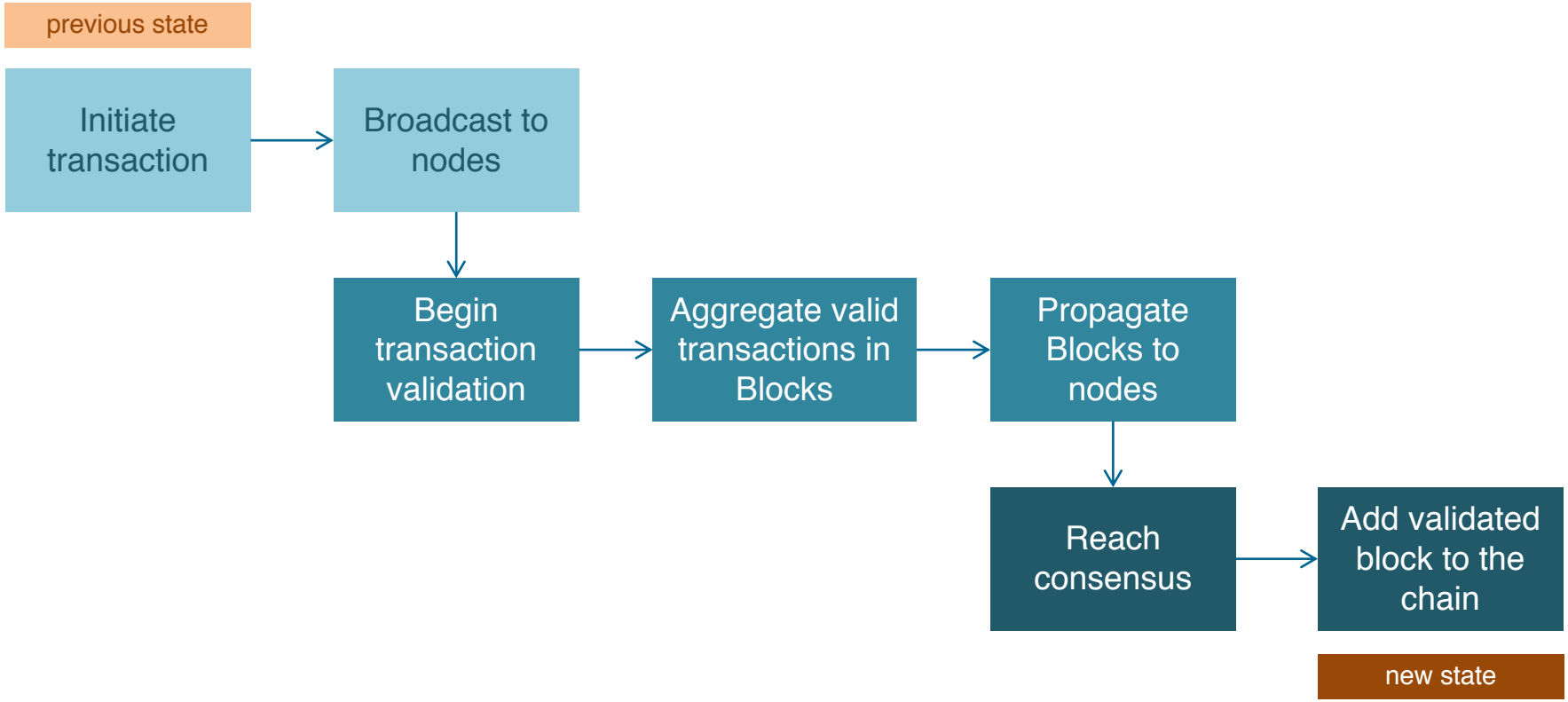
Source: World Economic Forum, "Blockchain Beyond the Hype", White Paper, April 2018

Blockchain

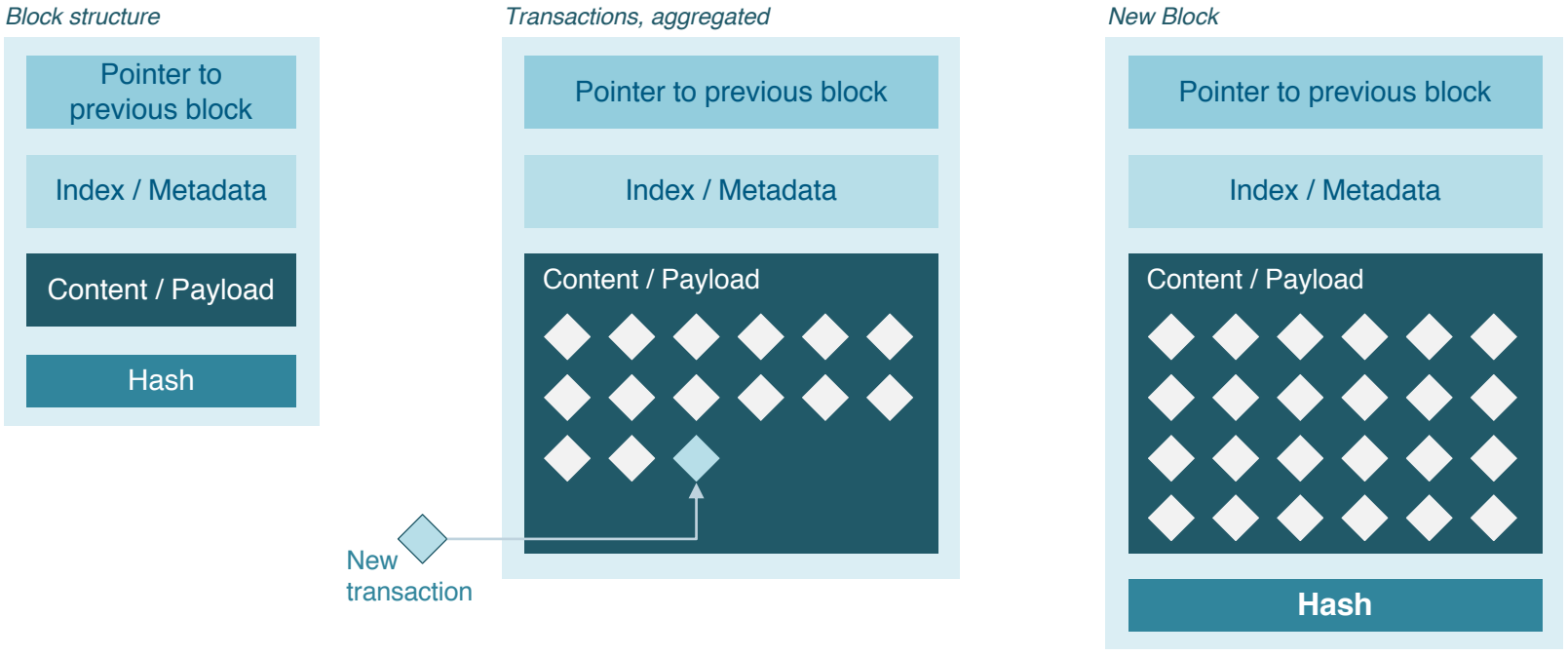
A Blockchain is a public, permanent, append-only, distributed ledger

- Sequence of hash-chained records: FINALITY IMMUTABILITY
  If record N is valid, you cannot change its past
- Procedure to add blocks: PROVENANCE
  who / how can blocks be added?
- Validation rules for new blocks: CONSENSUS
  transactions, digital signatures, consensus mechanism
- Conflict resolution: PROVENANCE
  which version of history is (to be taken as) correct?

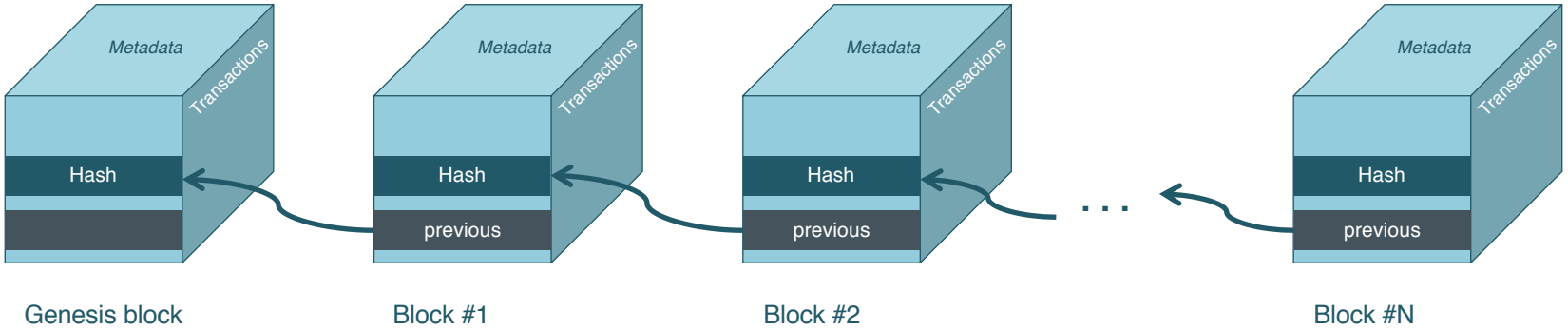
How it works, in principle...



Block internals, in principle...



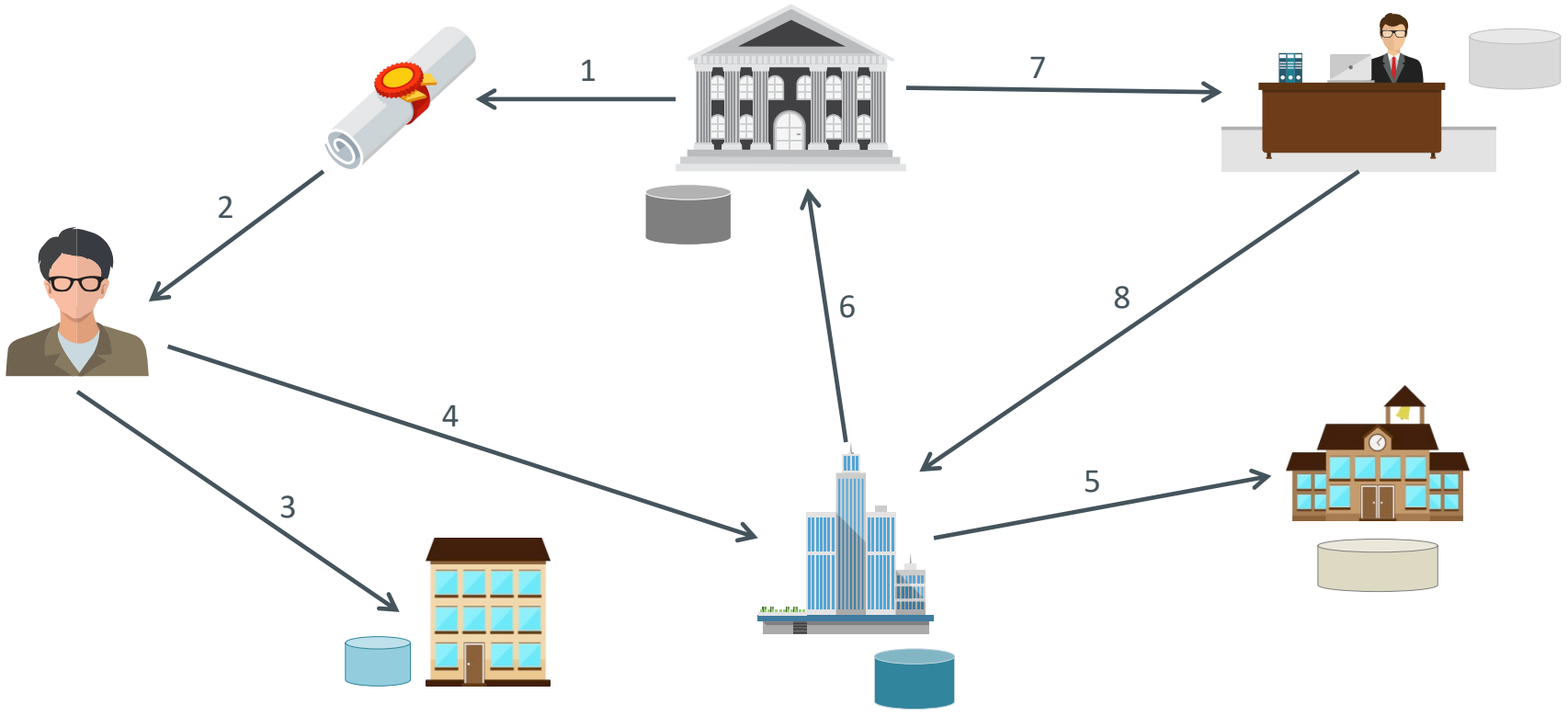
Blocks, chained



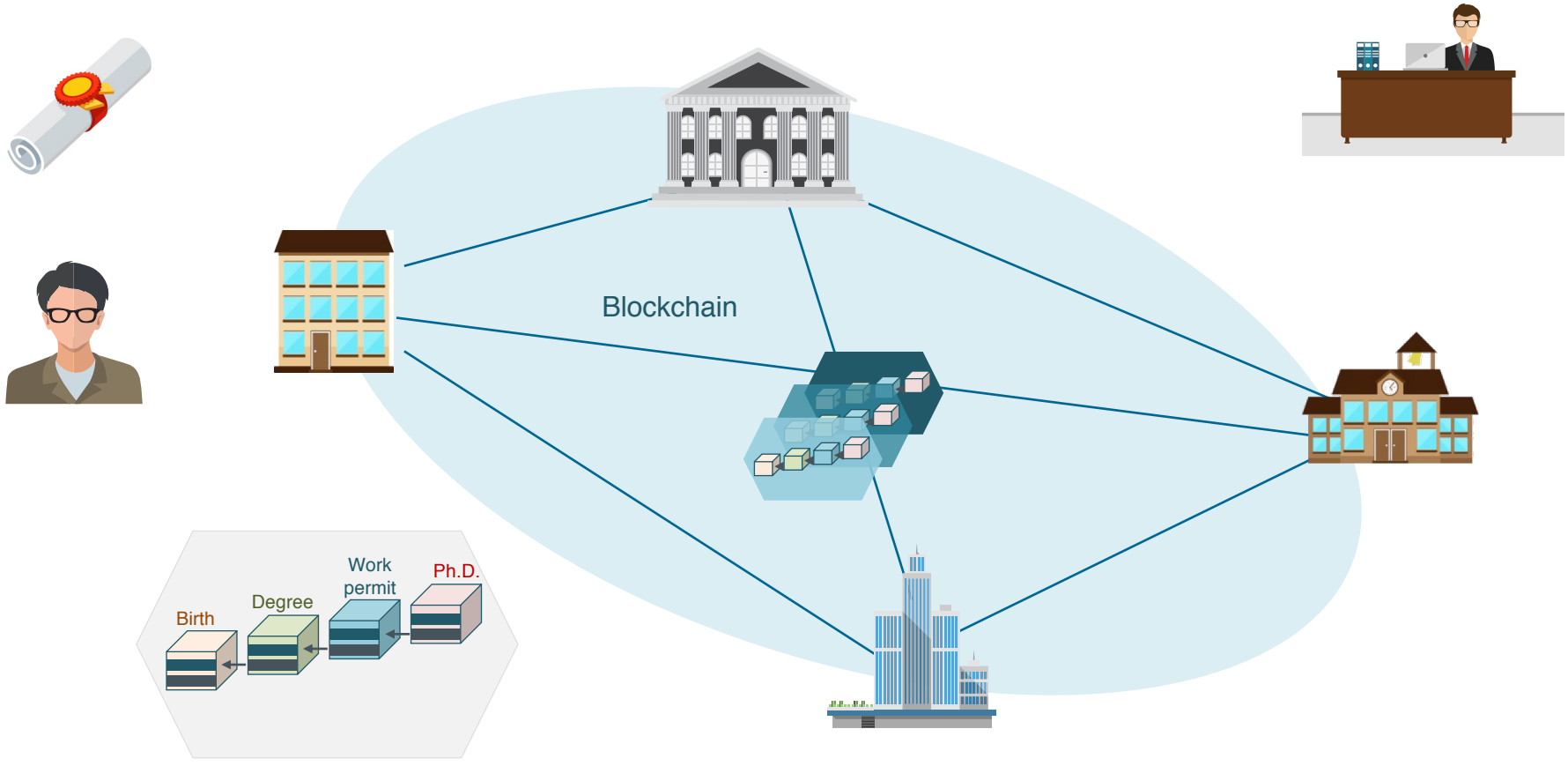
Example

Verification of academic degrees and professional practice permits in the job market

Example - Verification of University degrees and professional practice permits (short version)



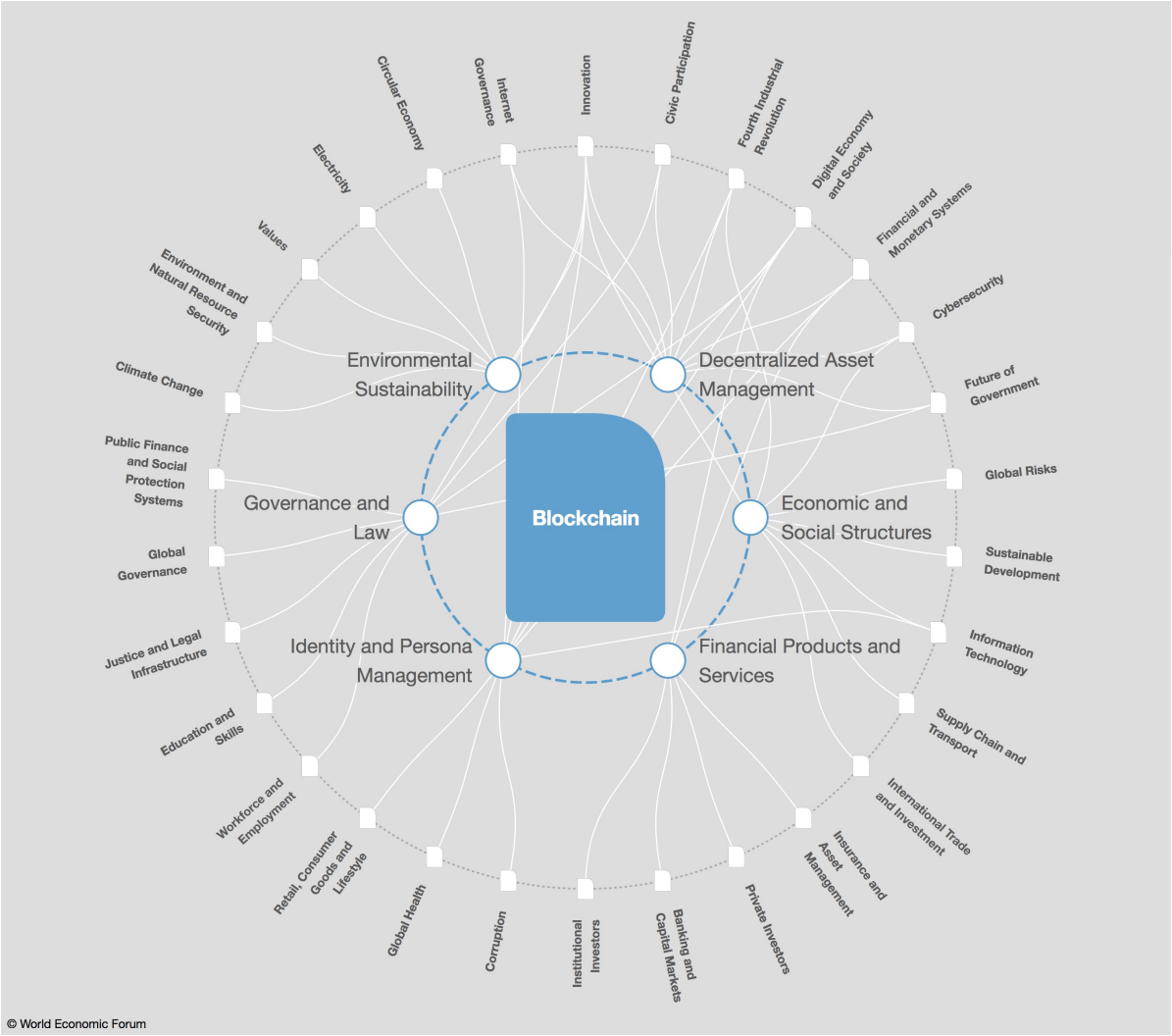
Example - Verification of University degrees and professional practice permits (short version)



Example - Verification of University degrees and professional practice permits (less short version)

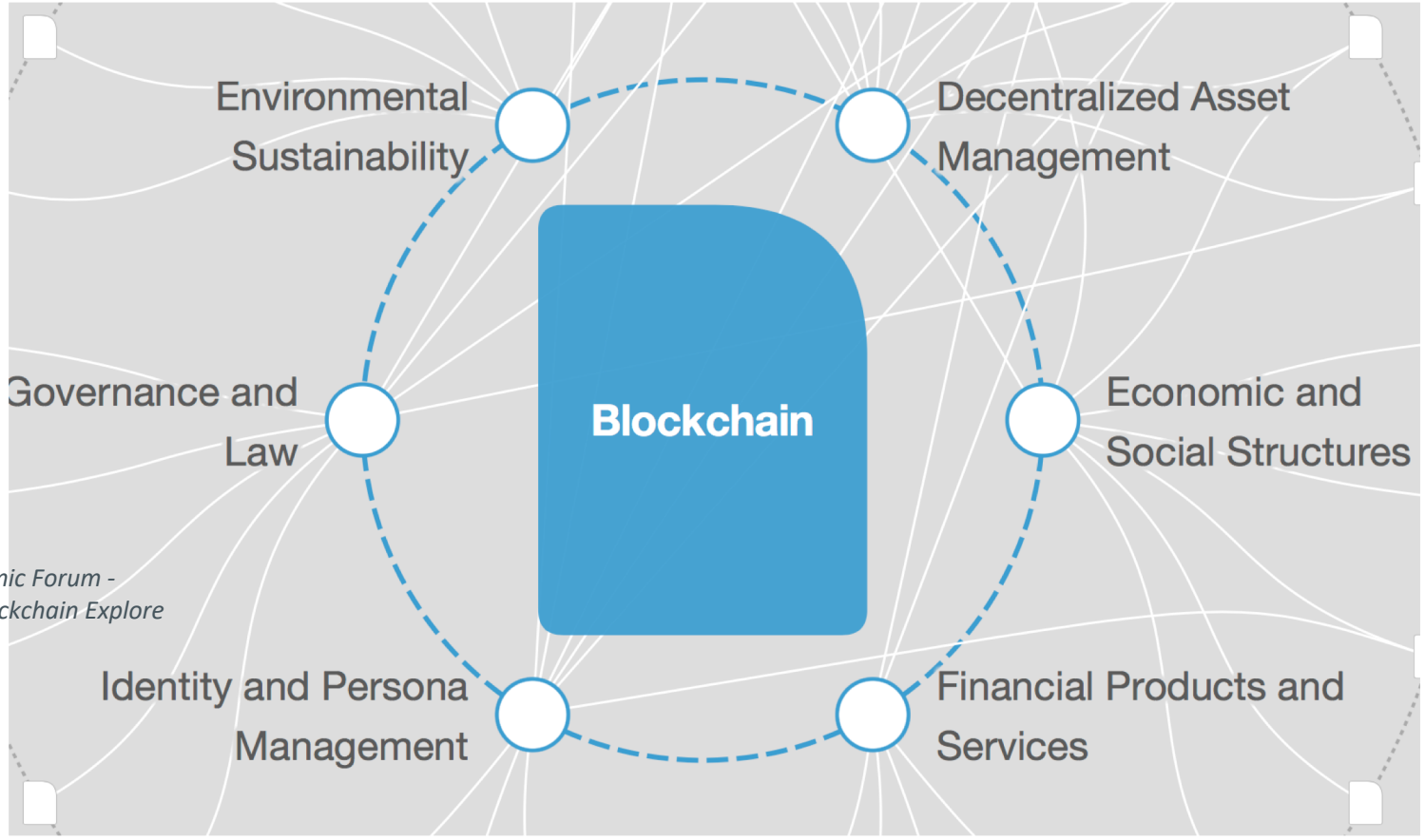
Applications of Blockchain

Applications



Source:
World Economic Forum - TOPLINK - Blockchain Explorec

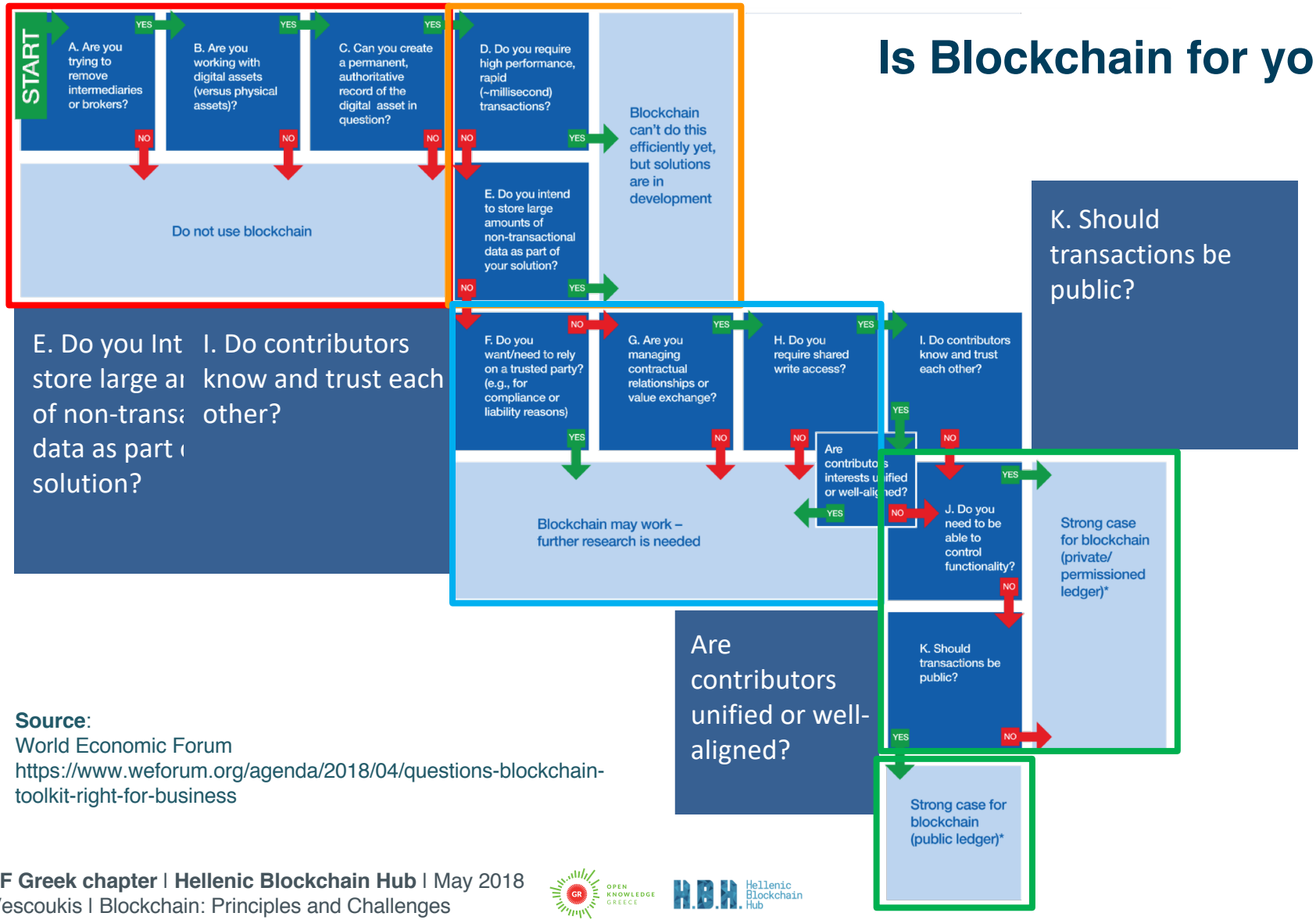
Applications



Source:
World Economic Forum -
TOPLINK - Blockchain Explore

Considerations, material for discussion

Is Blockchain for you?



E. Do you Int
store large a
of non-transa
data as part
solution?

I. Do contributors know and trust each other?

K. Should transactions be public?

Are contributors unified or well-aligned?

Source:
World Economic Forum
https://www.weforum.org/agenda/2018/04/questions-blockchain-toolkit-right-for-business

Issues to consider

Strategy

- What Blockchains to implement? Priorities? Rationale? Cost?

Architecture - Software Engineering

- Mapping of existing (legacy!) aps, systems, databases, web services to efficient ledgers and smart contracts

Migration

- Transitioning, regulatory issues, fear of the new, hype

Politics

- New balance(s) and roles, some currently dominant players will go out of business

Ideas for brainstorming (last session)

How to be a (Blockchain) programmer?

What exactly does a non-biased Blockchain architect?

How to apply well-established Information Systems Engineering principles?

Project ideas, from small pilots to world-changing,
project areas (G2G, G2B, B2G, B2C, ...) and pioneer organizations

Monetization and TCO

Research topics and ideas

How about a summer school?

Thank you!

Contact
v.vescoukis@cs.ntua.gr
about.me/vassilios.vescoukis