Blockchain in the Limelight

Leila Bahri

Researcher

lbahri@kth.se

Oct. 15, 2019, Castor Days

Stockholm

"Blockchain, an early-stage technology that enables the decentralized, secure storage and transfer of information, has the potential to be a powerful tool for tracking and transactions that can minimize friction, reduce corruption, increase trust and empower users."

World Economic Forum

How can we ensure that everyone – from the most marginalized members of society to the most powerful – benefits from blockchain's transformative potential?

Blockchain, an early-stage technology that enables the decentralized, secure storage and transfer of information, has the potential to be a powerful tool for tracking and transactions that can minimize friction, reduce corruption, increase trust and empower users. Cryptocurrencies built on distributed ledger technologies (DLT) have emerged as potential gateways to new wealth creation and disrupters across financial markets. Other revolutionary use cases are being explored in almost every sector, ranging from energy and shipping to media.

DLT has the potential to transform entire systems, but it also faces challenges, including lack of interoperability, security threats, centralization of power and unwillingness to experiment due to recent overhype. The Platform for Shaping the Future of Blockchain and Distributed Ledger Technology at the World Economic Forum aims to support the co-designing and testing of policy frameworks and governance protocols to accelerate the societal benefits of, and mitigate the risks from, distributed ledger technology. We work with our partners to advance a systemic and inclusive approach to governing DLT, which makes it possible to ensure that everyone can benefit from this powerful technology.

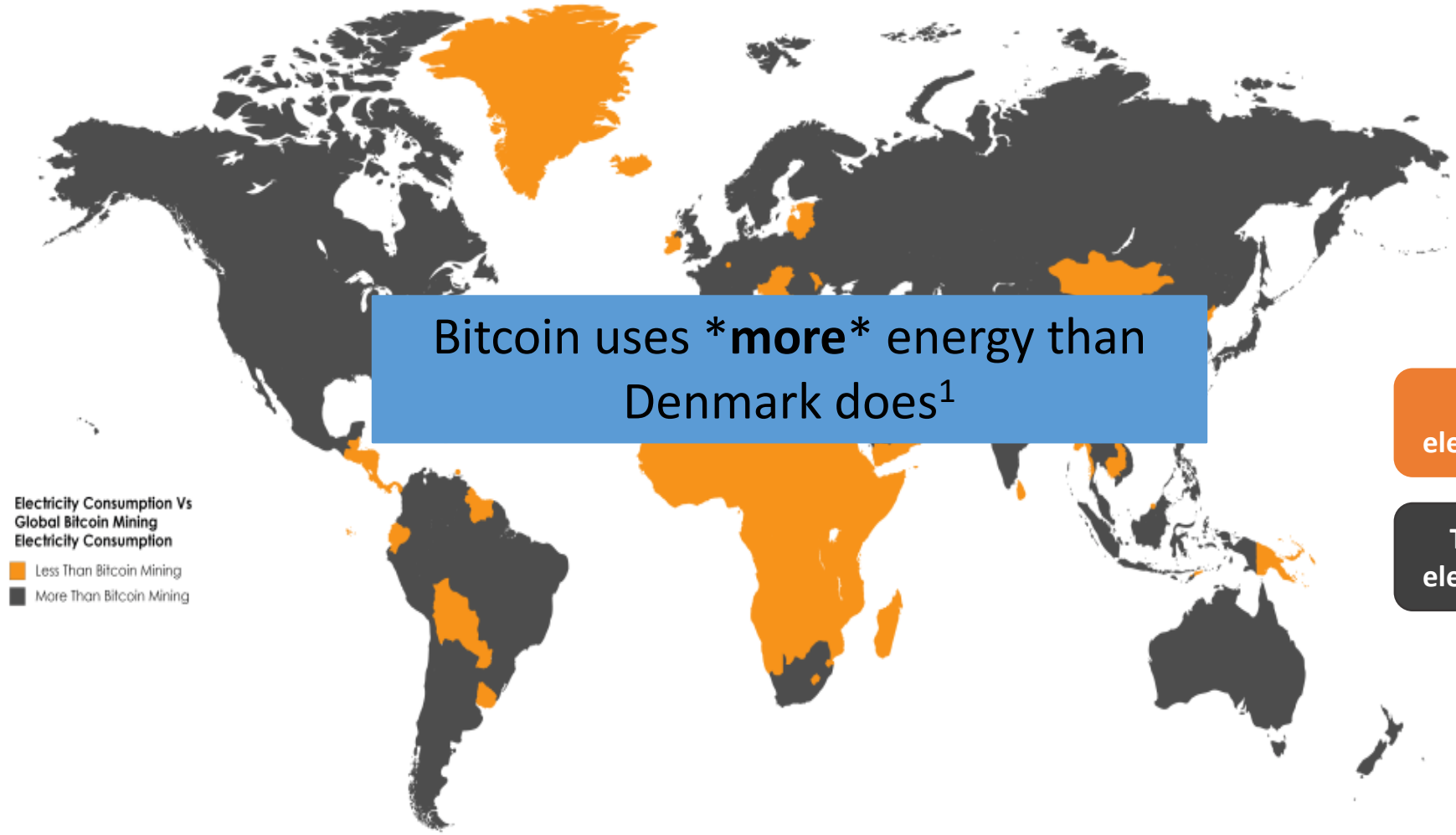
"How can we ensure that everyone – from the most marginalized members of society to the most powerful – benefits from blockchain's transformative potential?"

World Economic Forum

But What is Blockchain?

- Bitcoin
- Cryptocurrency
- Public ledger
- Mining
- Proof-of-Work
- Energy consumption

With Bitcoin, there are 10 types of countries in the world, …



Bitcoin uses *__more__* energy than Denmark does[1]

Those that consume less electricity than Bitcoin Mining

Those that consume more electricity than Bitcoin Mining

Source: https://powercompare.co.uk/bitcoin/

The map above shows which countries consume less electricity than the amount consumed by global bitcoin mining

1 https://news.abs-cbn.com/business/11/06/18/mining-bitcoin-uses-more-energy-than-denmark-study

Why does Mining (Proof-of-Work) consume that much energy?

Why is mining ever needed?

To Create / Find new Bitcoins!

Why is mining ever needed?

To Create / Find new Bitcoins!

There is more to mining than creating Bitcoins → Reaching consensus

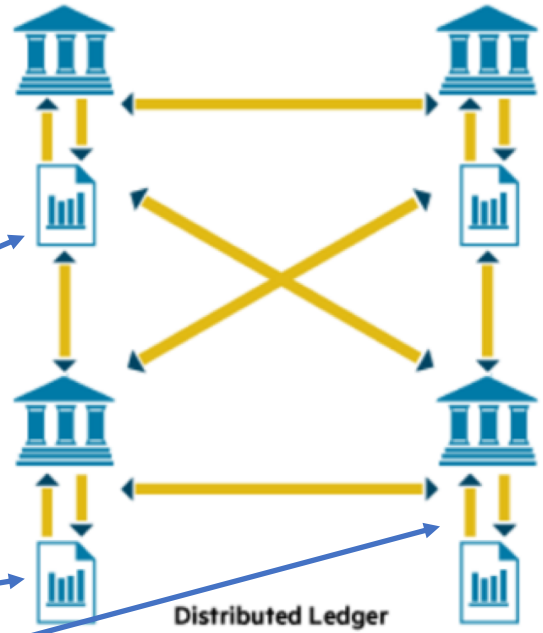
There is more to mining than creating Bitcoins…

Cash

Date	Description	Debit	Credit	Balance
Jan. 1, 20X3	Balance forward			$ -
Jan. 1, 20X3	Journal page 1	$ 25,000		25,000
Jan. 4, 20X3	Journal page 1		$ 2,000	23,000
Jan. 8, 20X3	Journal page 1	4,000		27,000
Jan. 18, 20X3	Journal page 2		500	26,500
Jan. 25, 20X3	Journal page 2	4,800		31,300
Jan. 28, 20X3	Journal page 2		5,000	26,300

There is more to mining than creating Bitcoins…

Ledger collaboratively managed by the open public



Cash

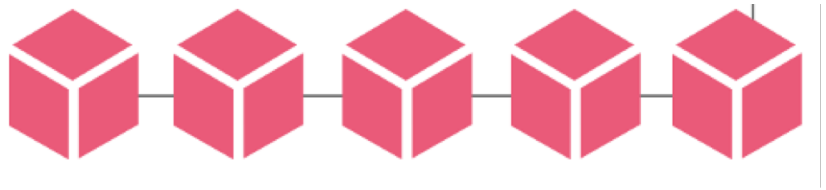
Date	Description	Debit	Credit	Balance
Jan. 1, 20X3	Balance forward			$ -
Jan. 1, 20X3	Journal page 1	$ 25,000		25,000
Jan. 4, 20X3	Journal page 1		$ 2,000	23,000
Jan. 8, 20X3	Journal page 1	4,000		27,000
Jan. 18, 20X3	Journal page 2		500	26,500
Jan. 25, 20X3	Journal page 2	4,800		31,300
Jan. 28, 20X3	Journal page 2		5,000	26,300

Issue: How to agree on the state of the ledger among the members of the P2P network

A data structure / data representation point …

Cash				
Date	**Description**	**Debit**	**Credit**	**Balance**
Jan. 1, 20X3	Balance forward			$ -
Jan. 1, 20X3	Journal page 1	$ 25,000		25,000
Jan. 4, 20X3	Journal page 1		$ 2,000	23,000
Jan. 8, 20X3	Journal page 1	4,000		27,000
Jan. 18, 20X3	Journal page 2		500	26,500
Jan. 25, 20X3	Journal page 2	4,800		31,300
Jan. 28, 20X3	Journal page 2		5,000	26,300

Change presentation

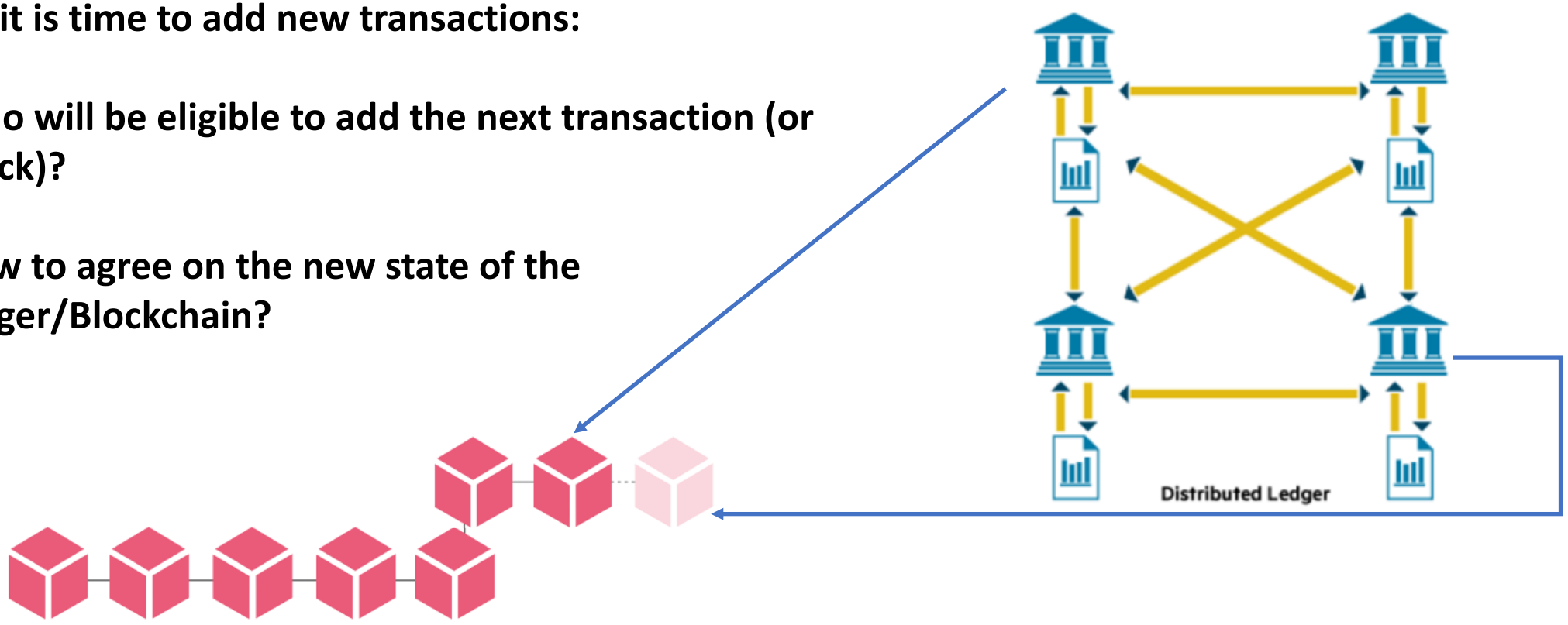


Call this a Block Chain (Chain of Blocks)

There is more to mining than creating Bitcoins…

When it is time to add new transactions:

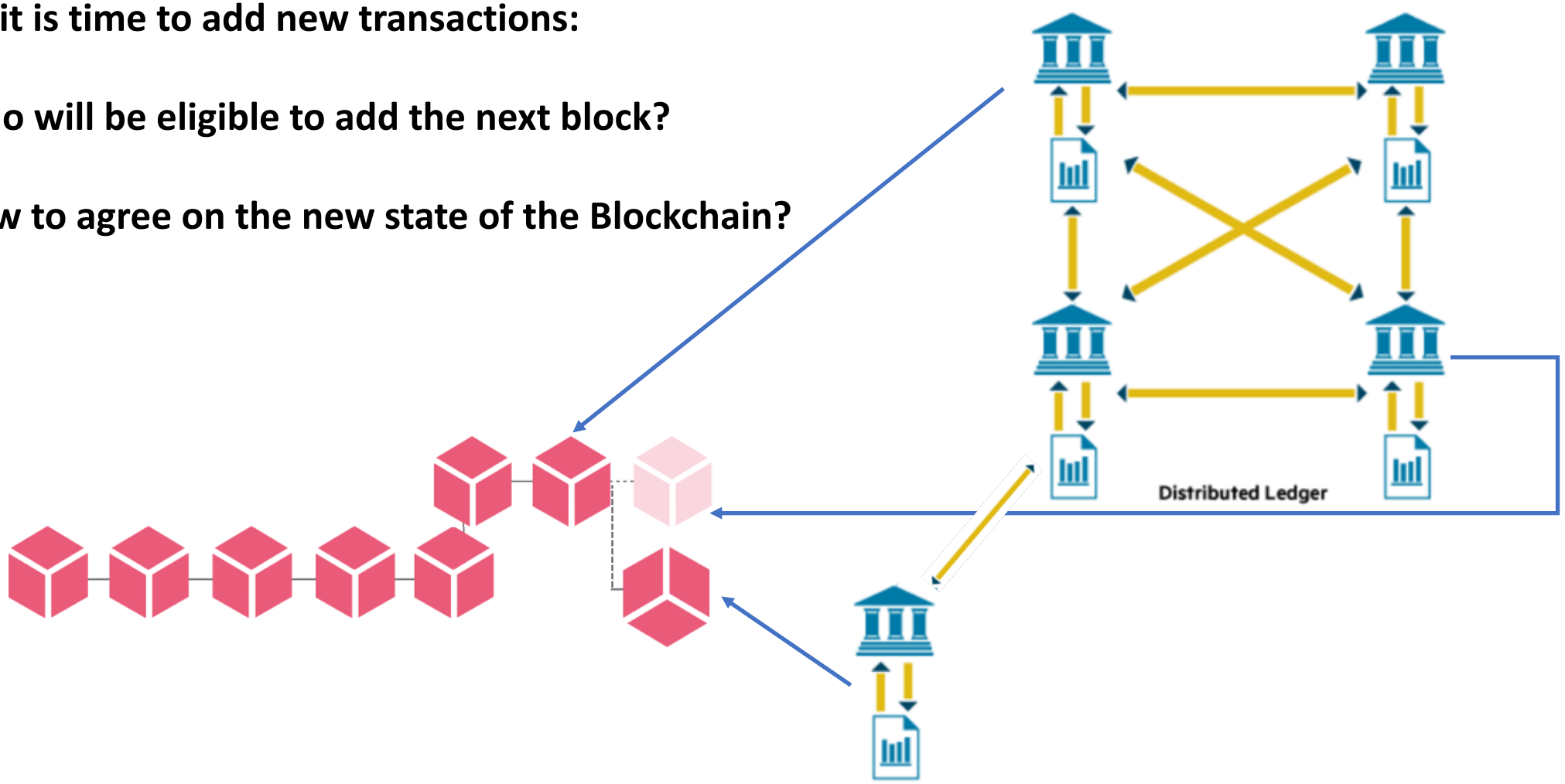
- **Who will be eligible to add the next transaction (or block)?**
- **How to agree on the new state of the ledger/Blockchain?**



There is more to mining than creating Bitcoins…

When it is time to add new transactions:

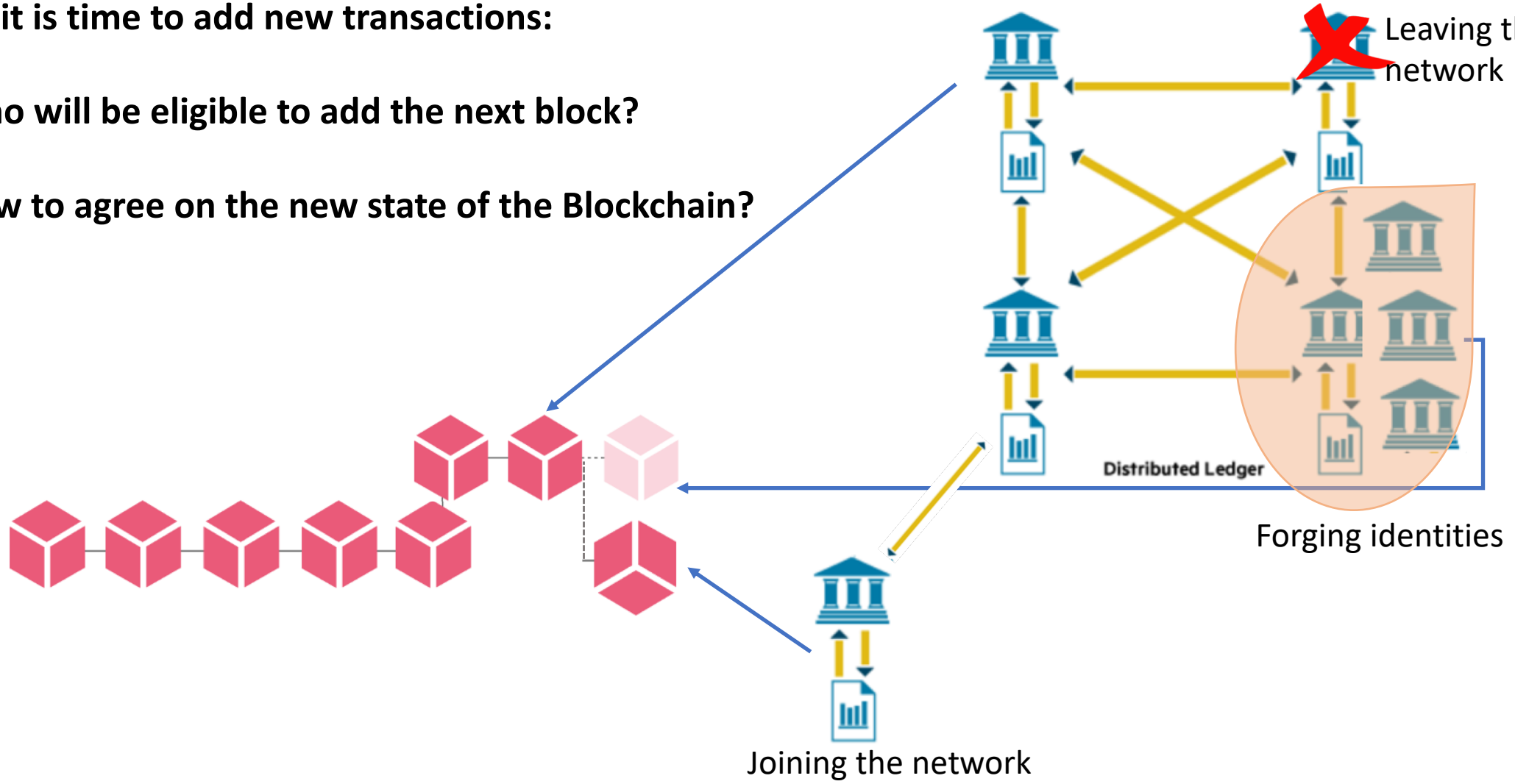
- **Who will be eligible to add the next block?**
- **How to agree on the new state of the Blockchain?**



There is more to mining than creating Bitcoins…

When it is time to add new transactions:

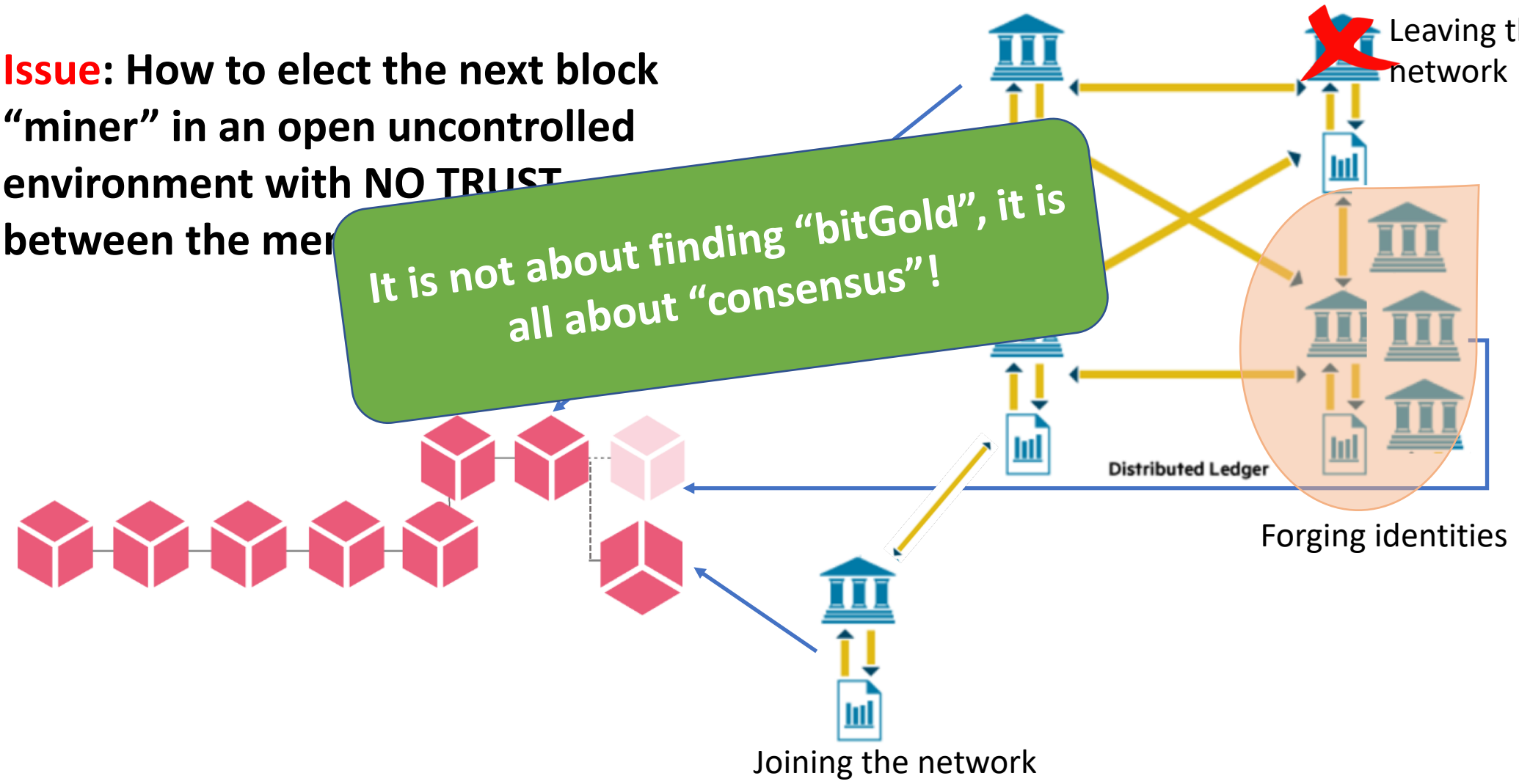
- **Who will be eligible to add the next block?**
- **How to agree on the new state of the Blockchain?**



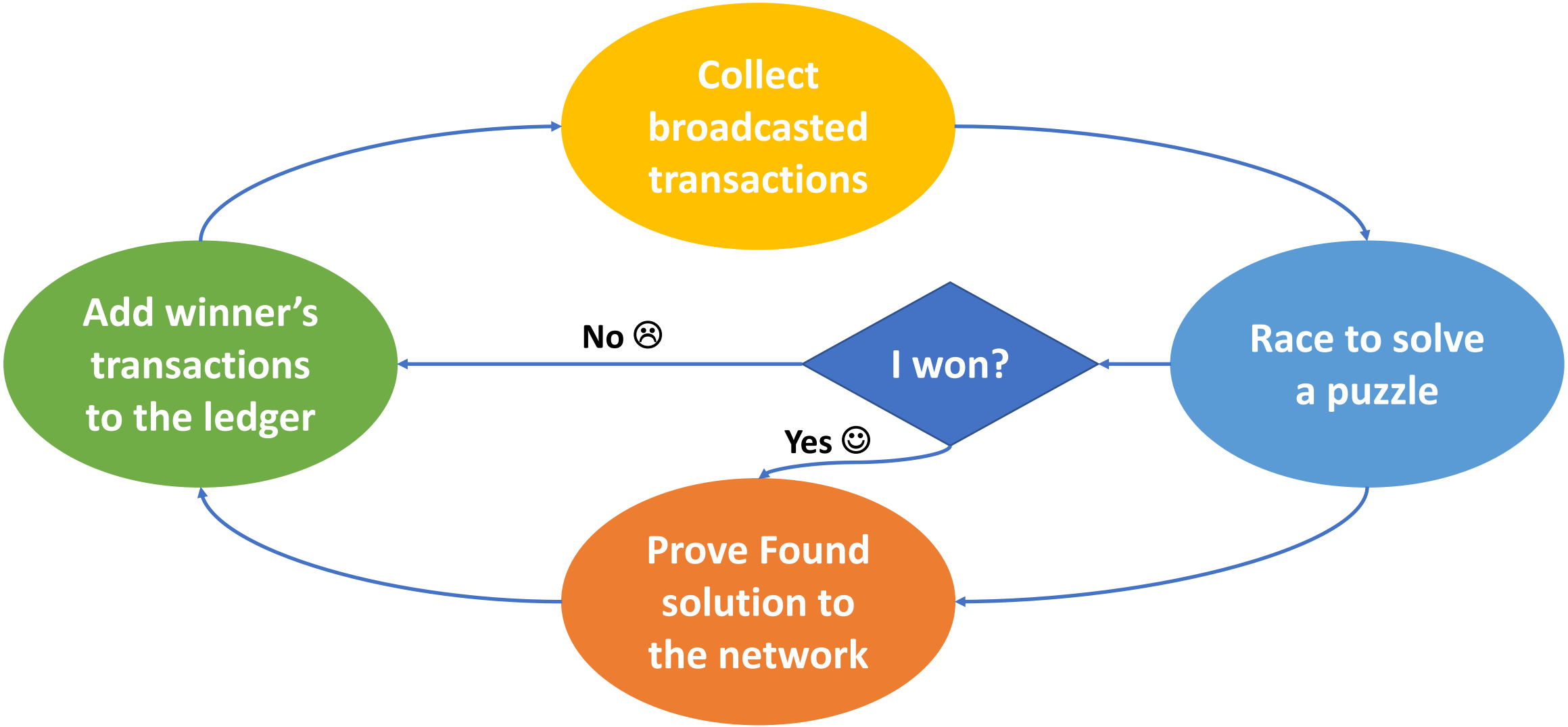
There is more to mining than creating Bitcoins…

Issue: How to elect the next block "miner" in an open uncontrolled environment with NO TRUST between the mer

It is not about finding "bitGold", it is all about "consensus"!



Mining (PoW) - Consensus with NO TRUST



Mining (PoW) - Consensus with NO TRUST

Roots:

- Playing little tricks with Cryptographic Hash Functions

Advantages:

- One CPU one vote → Cannot forge virtual peers
- Secure provable consensus mechanism
- Simple and easy for verification

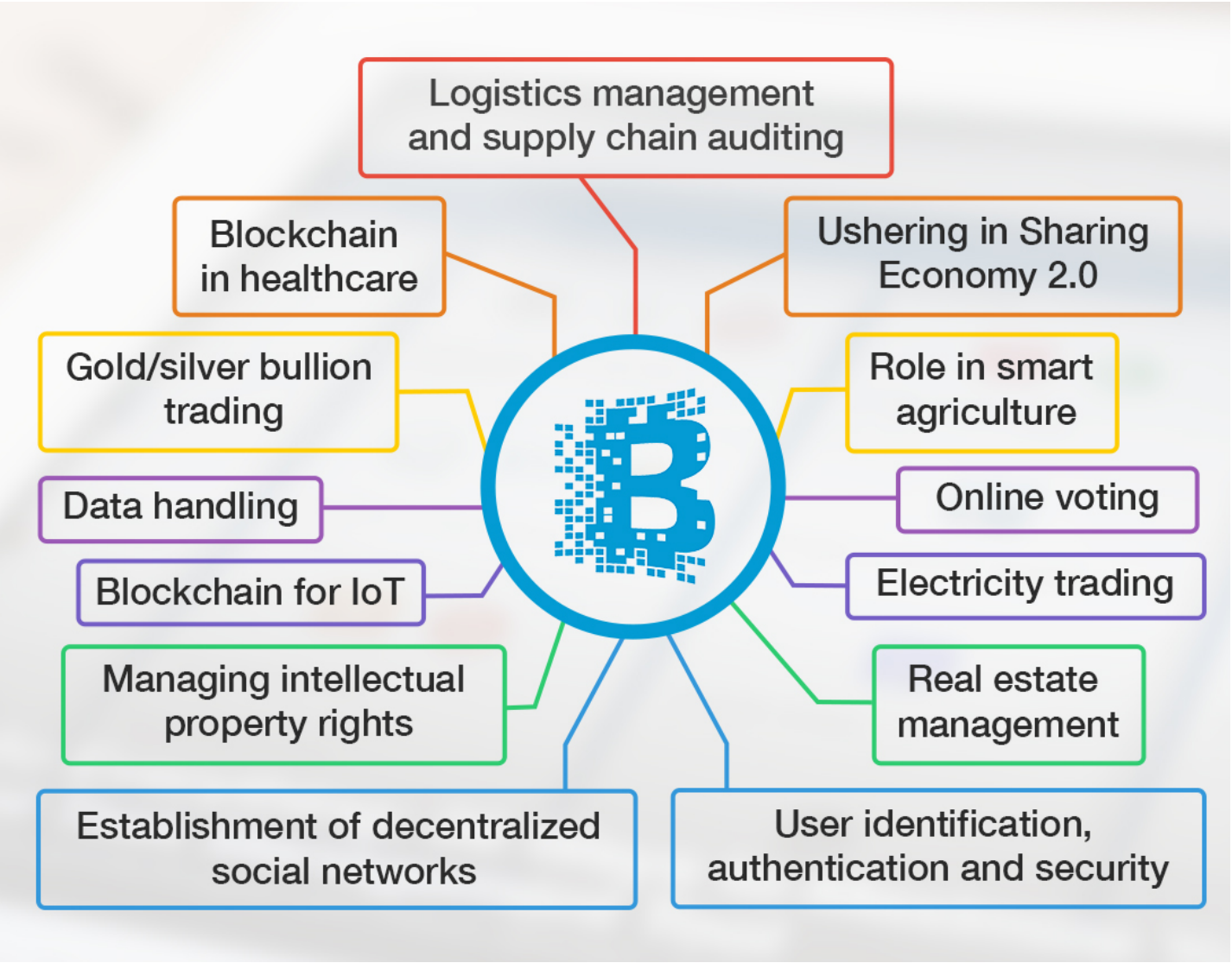
Disadvantage

- Burns TOO MUCH energy

What is a Blockchain

A ledger of timestamped transactions, securely chained in a time-based ordered manner (from old to new), that is created and maintained by a peer-to-peer system using a consensus mechanism that provides security guarantees against identity forging.

Possible Uses of Blockchain



Adapted from: https://teks.co.in/site/blog/blockchain-beyond-financial-services-13-applications-use-cases/

Any alternatives to PoW?

- Proof-of-Something (for real decentralized systems)
  - Proof-of-Stake
  - Proof-of-Activity
  - Proof-of-Useful-Work
  - Proof-of-Trust[1]
- Permissioned Blockchain with traditional consensus algorithms
  - Decentralization is put at stake (?)

[1] "Trust Mends Blockchain – Living uo to Expectation", L. Bahri & Sarunas Girdzijauskas. Published at ICDCS'2019

Thank you for your trust ☺

lbahri@kth.se