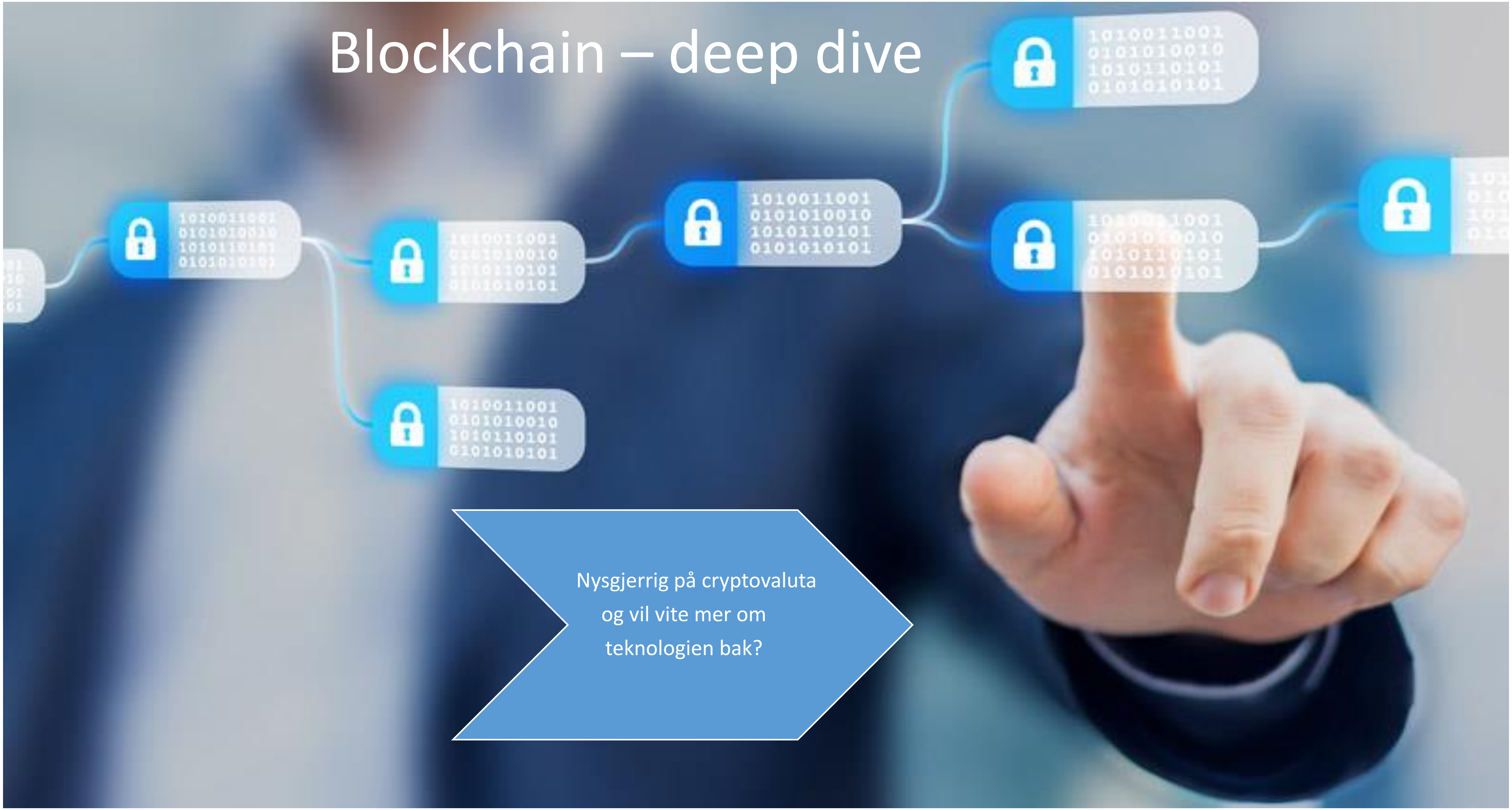
Blockchain – deep dive

Common Norge 21. august 2018
Magne Kofoed
IT Resource Group AS
Tlf 908 97 168
E-post magne.kofoed@gmail.com

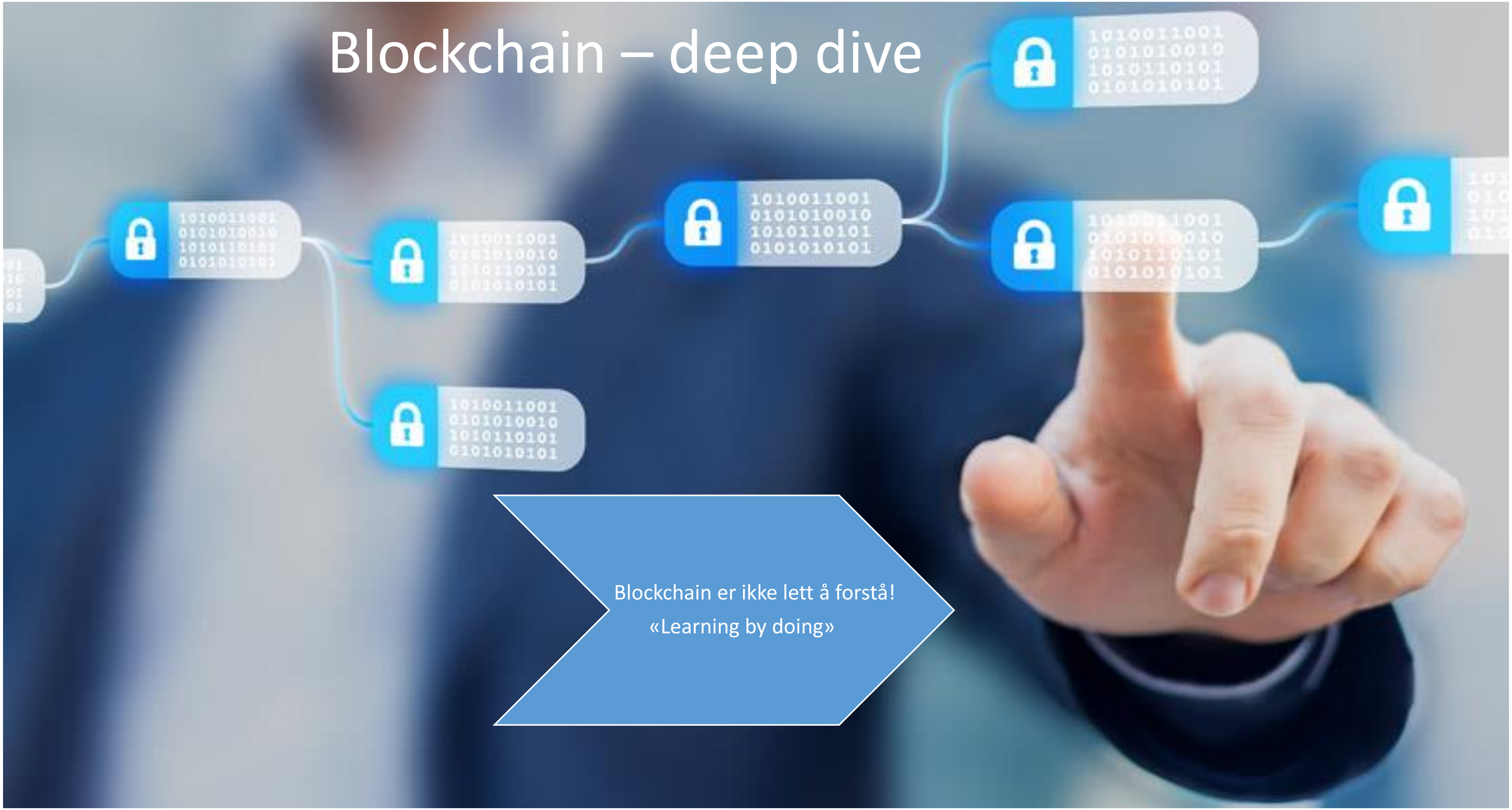
Bitcoin explained

Blockchain – deep dive



Nysgjerrig på cryptovaluta og vil vite mer om teknologien bak?

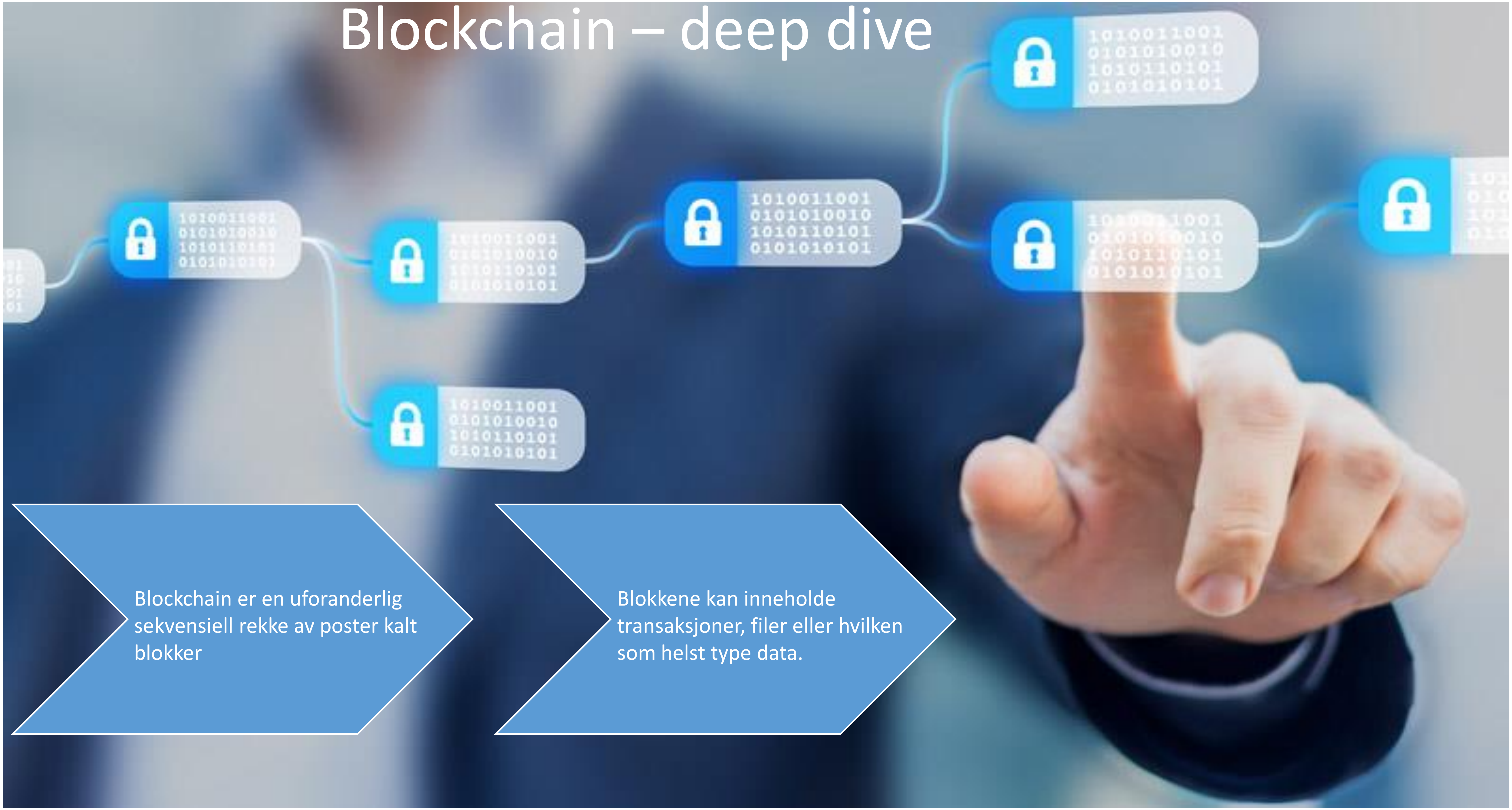
Blockchain – deep dive



Blockchain er ikke lett å forstå!

«Learning by doing»

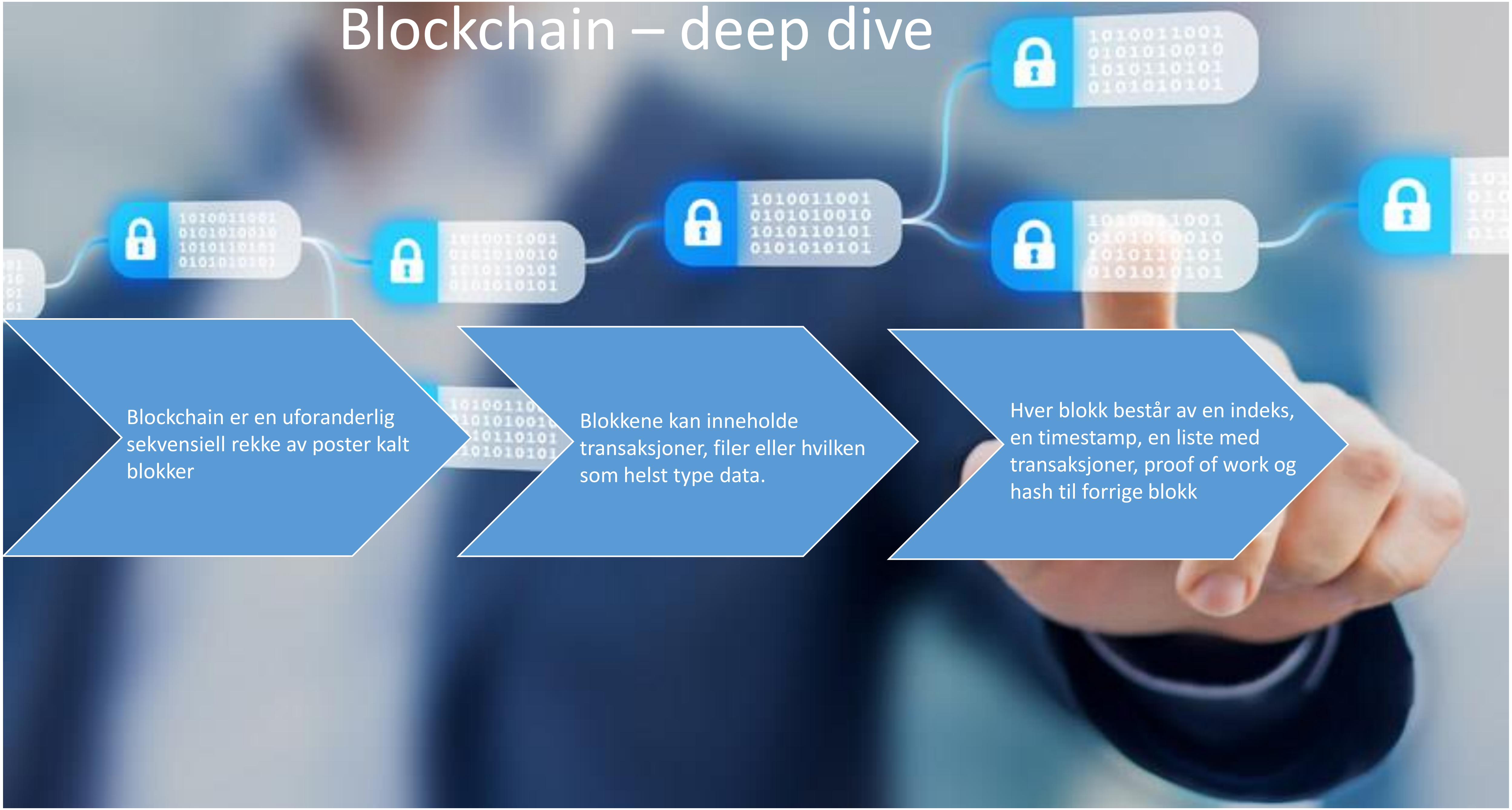
Blockchain – deep dive



Blockchain er en uforanderlig sekvensiell rekke av poster kalt blokker

Blokkene kan inneholde transaksjoner, filer eller hvilken som helst type data.

Blockchain – deep dive

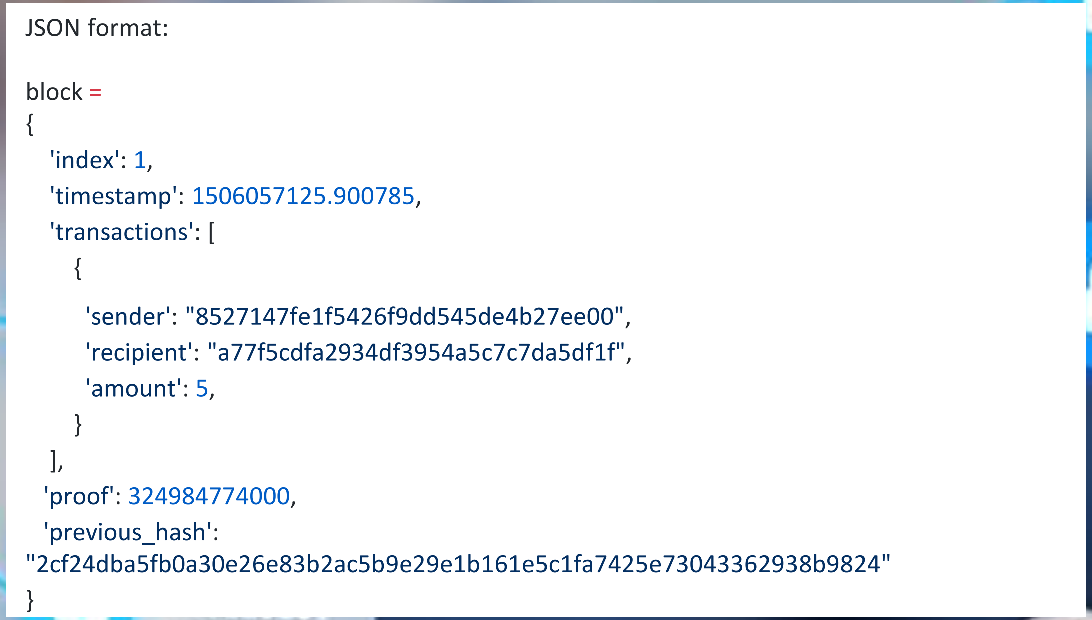


Blockchain er en uforanderlig sekvensiell rekke av poster kalt blokker

Blokkene kan inneholde transaksjoner, filer eller hvilken som helst type data.

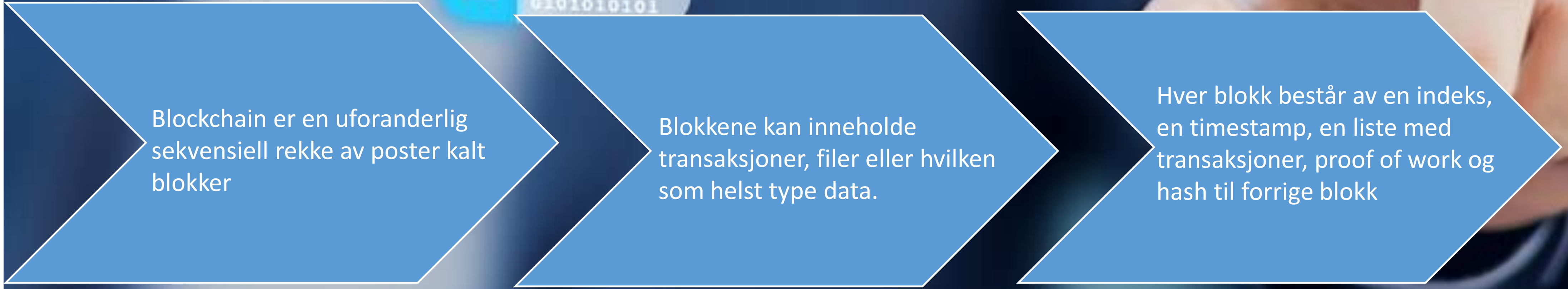
Hver blokk består av en indeks, en timestamp, en liste med transaksjoner, proof of work og hash til forrige blokk

Blockchain – deep dive



JSON format:

```
block =
{
   'index': 1,
   'timestamp': 1506057125.900785,
   'transactions': [
      {
        'sender': "8527147fe1f5426f9dd545de4b27ee00",
        'recipient': "a77f5cdfa2934df3954a5c7c7da5df1f",
        'amount': 5,
      }
   ],
  'proof': 324984774000,
  'previous_hash':
"2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824"
}
```



Blockchain er en uforanderlig sekvensiell rekke av poster kalt blokker

Blokkene kan inneholde transaksjoner, filer eller hvilken som helst type data.

Hver blokk består av en indeks, en timestamp, en liste med transaksjoner, proof of work og hash til forrige blokk

JSON format:

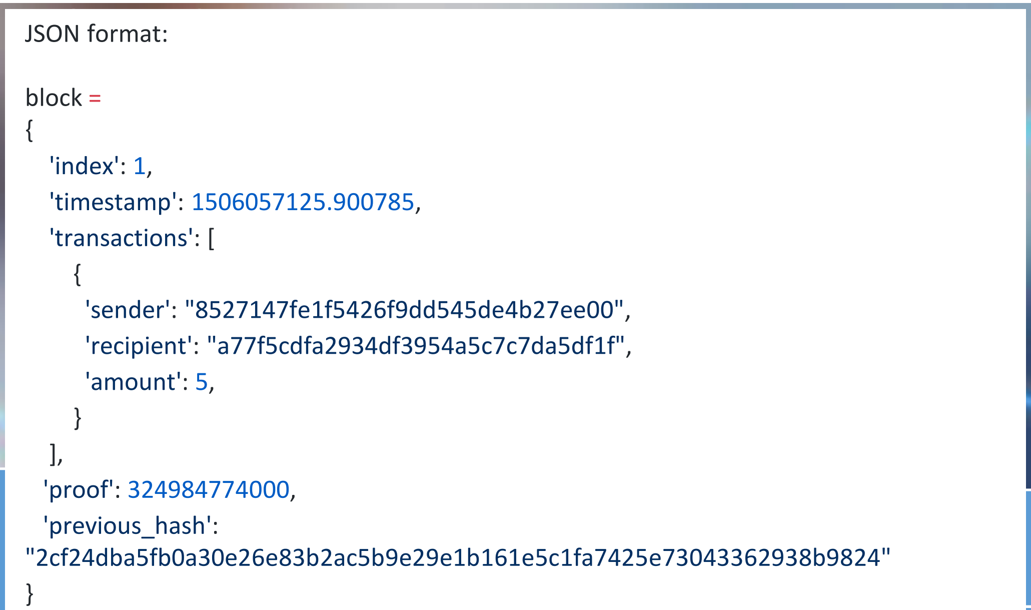
```
block =
{
   'index': 1,
   'timestamp': 1506057125.900785,
   'transactions': [
      {
        'sender': "8527147fe1f5426f9dd545de4b27ee00",
        'recipient': "a77f5cdfa2934df3954a5c7c7da5df1f",
        'amount': 5,
      }
   ],
  'proof': 324984774000,
  'previous_hash':
"2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824"
}
```

Blockchain er en uforanderlig sekvensiell rekke av poster kalt blokker

Blokkene kan inneholde transaksjoner, filer eller hvilken som helst type data.

Hver blokk består av en indeks, en timestamp, en liste med transaksjoner, proof of work og hash til forrige blokk

Blockchain er lagret i minne på http servere



JSON format:

```
block =
{
   'index': 1,
   'timestamp': 1506057125.900785,
   'transactions': [
      {
        'sender': "8527147fe1f5426f9dd545de4b27ee00",
        'recipient': "a77f5cdfa2934df3954a5c7c7da5df1f",
        'amount': 5,
      }
   ],
  'proof': 324984774000,
  'previous_hash':
"2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824"
}
```

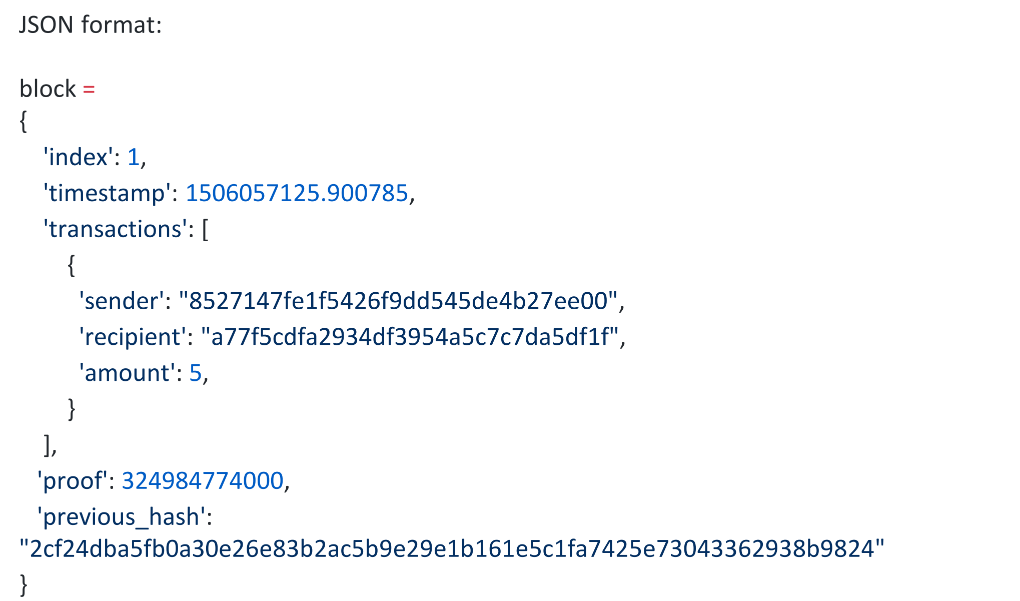
Blockchain er en uforanderlig sekvensiell rekke av poster kalt blokker

Blokkene kan inneholde transaksjoner, filer eller hvilken som helst type data.

Hver blokk består av en indeks, en timestamp, en liste med transaksjoner, proof of work og hash til forrige blokk

Blockchain er lagret i minne på http servere

Kommuniserer med http servere og blockchain via REST api



JSON format:

```
block =
{
   'index': 1,
   'timestamp': 1506057125.900785,
   'transactions': [
      {
        'sender': "8527147fe1f5426f9dd545de4b27ee00",
        'recipient': "a77f5cdfa2934df3954a5c7c7da5df1f",
        'amount': 5,
      }
   ],
  'proof': 324984774000,
  'previous_hash':
"2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824"
}
```

Blockchain er en uforanderlig sekvensiell rekke av poster kalt blokker

Blokkene kan inneholde transaksjoner, filer eller hvilken som helst type data.

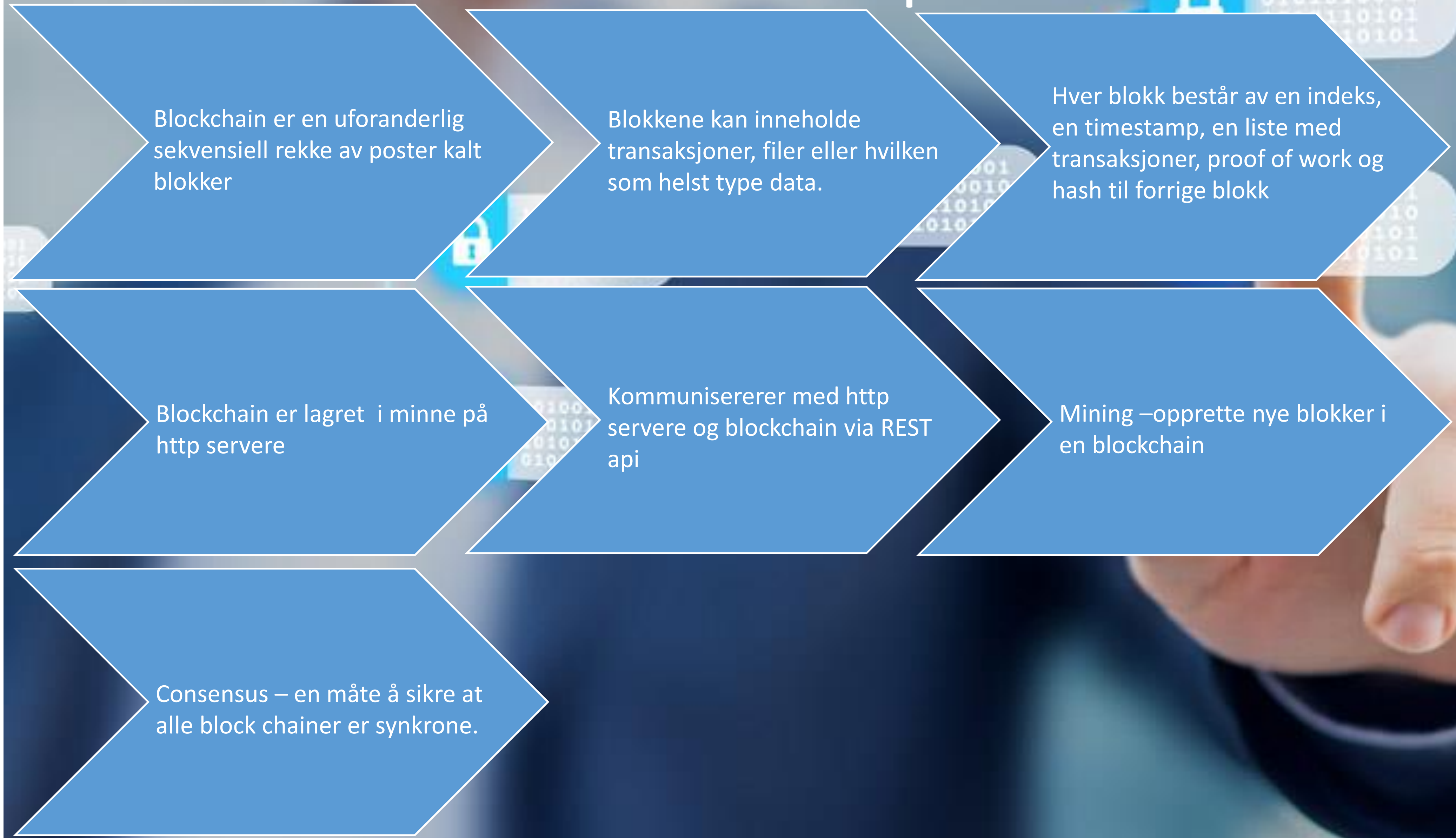
Hver blokk består av en indeks, en timestamp, en liste med transaksjoner, proof of work og hash til forrige blokk

Blockchain er lagret i minne på http servere

Kommuniserer med http servere og blockchain via REST api

Mining –opprette nye blokker i en blockchain

Blockchain – deep dive



Blockchain er en uforanderlig sekvensiell rekke av poster kalt blokker

Blokkene kan inneholde transaksjoner, filer eller hvilken som helst type data.

Hver blokk består av en indeks, en timestamp, en liste med transaksjoner, proof of work og hash til forrige blokk

Blockchain er lagret i minne på http servere

Kommuniserer med http servere og blockchain via REST api

Mining –opprette nye blokker i en blockchain

Consensus – en måte å sikre at alle block chainer er synkrone.

Blockchain – deep dive

Blockchain er en uforanderlig sekvensiell rekke av poster kalt blokker

Blokkene kan inneholde transaksjoner, filer eller hvilken som helst type data.

Hver blokk består av en indeks, en timestamp, en liste med transaksjoner, proof of work og hash til forrige blokk

Blockchain er lagret i minne på http servere

Kommuniserer med http servere og blockchain via REST api

Mining –opprette nye blokker i en blockchain

Consensus – en måte å sikre at alle block chainer er synkrone.

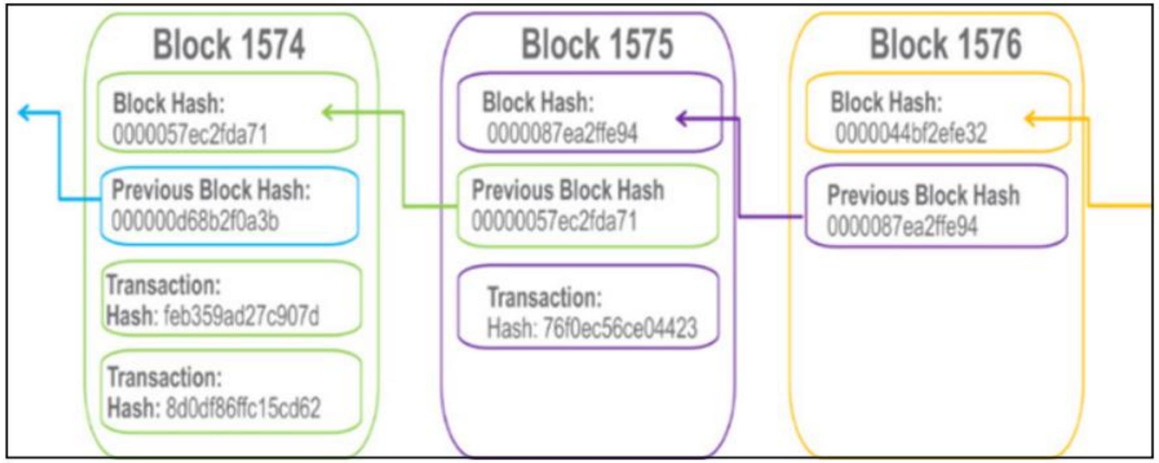
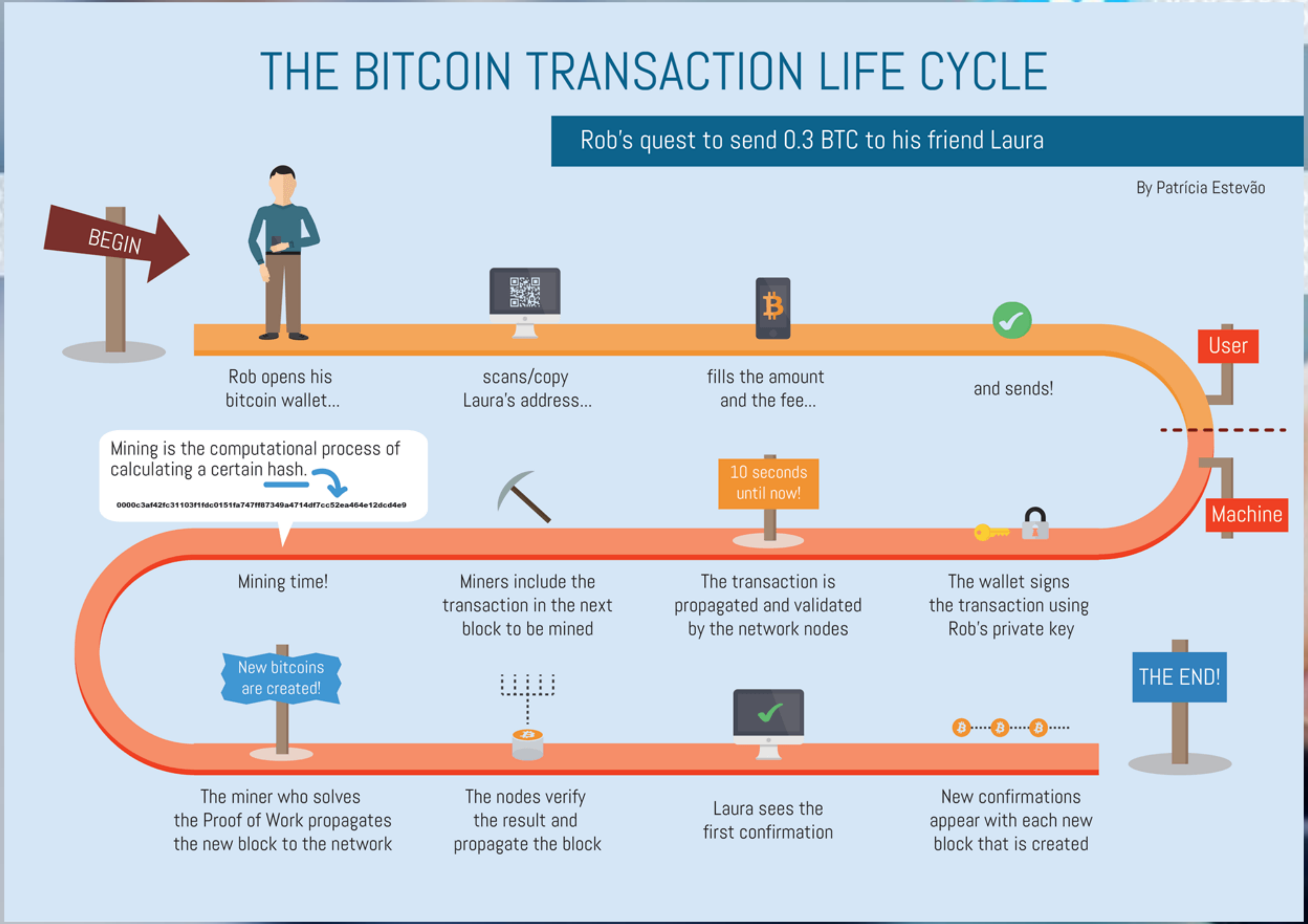


FIGURE 2-1: Blockchain stores transaction records in a series of connected blocks.

Blockchain – deep dive



THE BITCOIN TRANSACTION LIFE CYCLE

Rob's quest to send 0.3 BTC to his friend Laura

By Patrícia Estevão

Rob opens his bitcoin wallet...

scans/copy Laura's address...

fills the amount and the fee...

and sends!

The wallet signs the transaction using Rob's private key

The transaction is propagated and validated by the network nodes

Miners include the transaction in the next block to be mined

Mining is the computational process of calculating a certain hash.

0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9

Mining time!

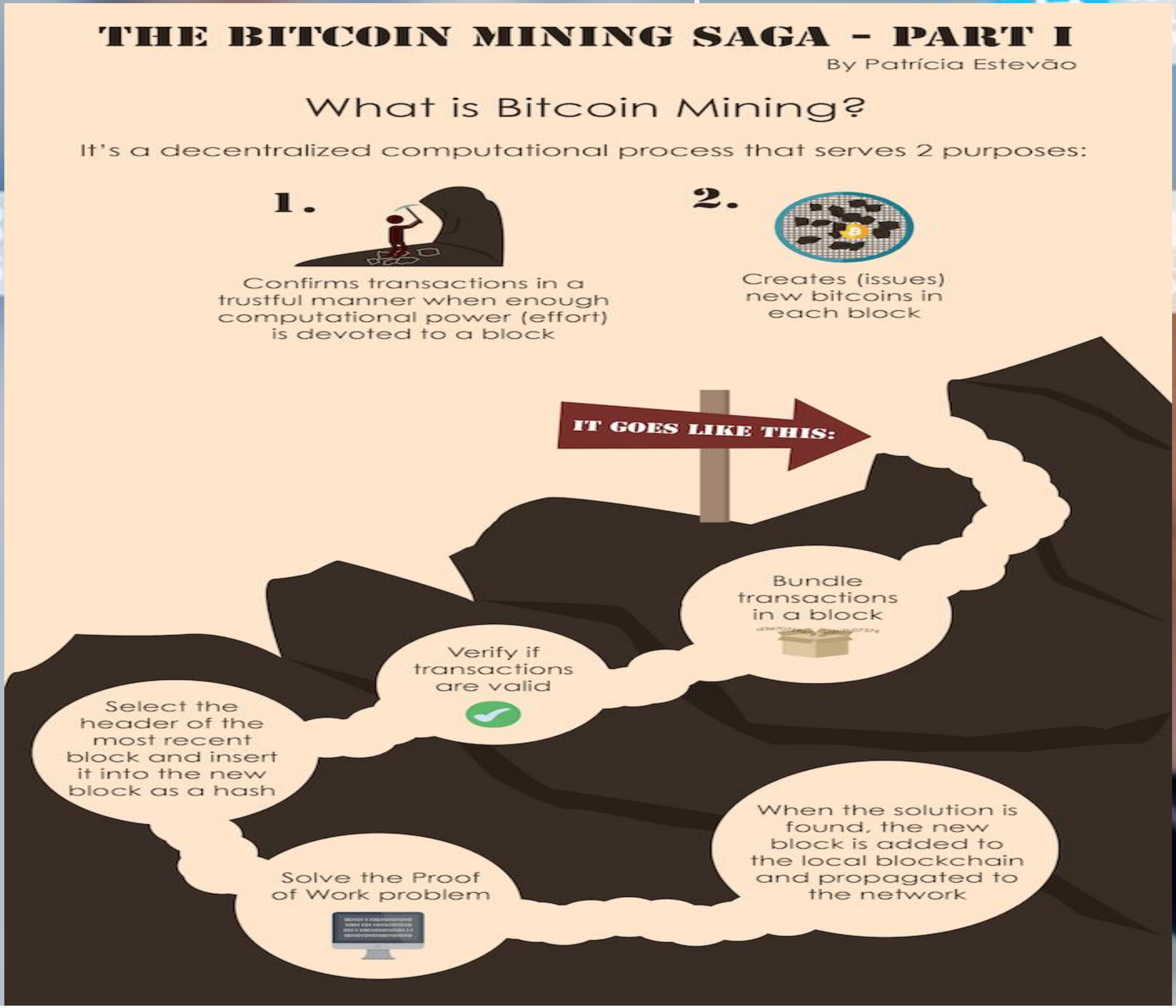
The miner who solves the Proof of Work propagates the new block to the network

The nodes verify the result and propagate the block

Laura sees the first confirmation

New confirmations appear with each new block that is created

Blockchain – deep dive



THE BITCOIN MINING SAGA - PART I

By Patrícia Estevão

What is Bitcoin Mining?

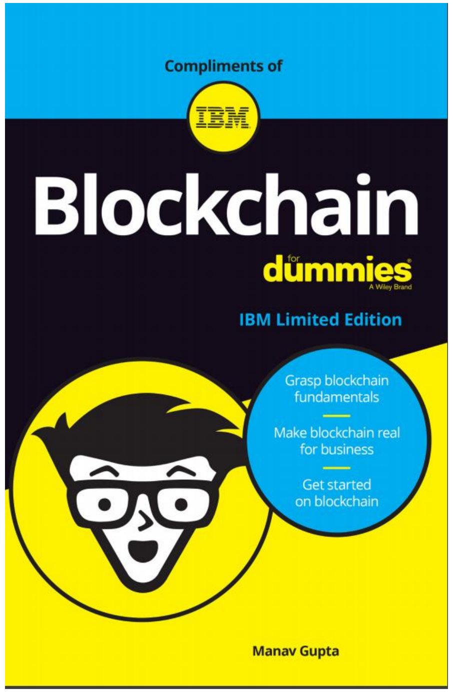
It's a decentralized computational process that serves 2 purposes:

1. Confirms transactions in a trustful manner when enough computational power (effort) is devoted to a block

2. Creates (issues) new bitcoins in each block

IT GOES LIKE THIS:

- Bundle transactions in a block
- Verify if transactions are valid
- Select the header of the most recent block and insert it into the new block as a hash
- Solve the Proof of Work problem
- When the solution is found, the new block is added to the local blockchain and propagated to the network


Compliments of
IBM
Blockchain
for dummies
A Wiley Brand
IBM Limited Edition
Grasp blockchain fundamentals
Make blockchain real for business
Get started on blockchain
Manav Gupta

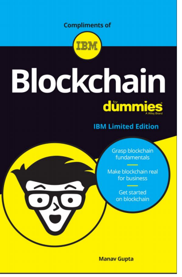
Blockchain – deep dive

Bitcoin has several advantages over other current transaction systems, including the following:

» Cost-effective: Bitcoin eliminates the need for intermediaries.

» Efficient: Transaction information is recorded once and is available to all parties through the distributed network.

» Safe and secure: The underlying ledger is tamper-evident. A transaction can’t be changed; it can only be reversed with another transaction, in which case both transactions are visible.


Compliments of
IBM
Blockchain
for dummies
A Wiley Brand
IBM Limited Edition
Grasp blockchain fundamentals
Make blockchain real for business
Get started on blockchain
Manav Gupta

Blockchain – deep dive

Decentralization

Bitcoin does not have a central authority and the bitcoin network is decentralized:

- There is no central server, bitcoin ledger is distributed.

- The ledger is public, anybody can store it on their computer.

- There is no single administrator, the ledger is maintained by a network of equally privileged miners.

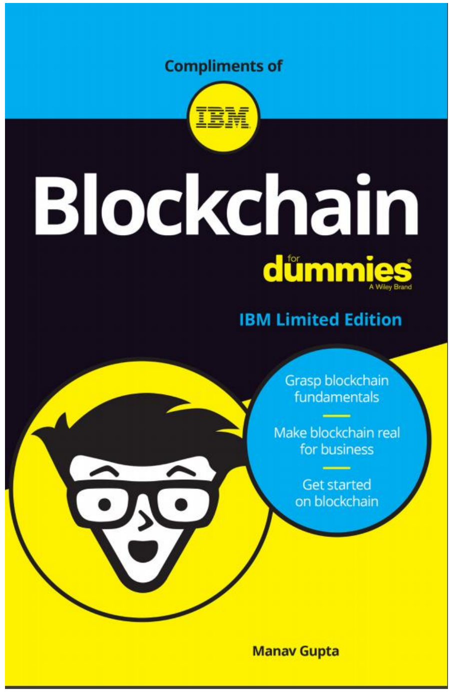
- Anybody can become a miner.

- The additions to the ledger are maintained through competition – until a new block is added to the ledger, it is not known which miner will create the block.

- The issuance of bitcoins is decentralized – bitcoins are issued as a reward for the creation of a new block.

- Anybody can create a new bitcoin address (a bitcoin counterpart of a bank account) without needing any approval.

- Anybody can send a transaction to the network without needing any approval, the network merely confirms that the transaction is legitimate.


Compliments of
IBM
Blockchain
for dummies
A Wiley Brand
IBM Limited Edition
Grasp blockchain fundamentals
Make blockchain real for business
Get started on blockchain
Manav Gupta

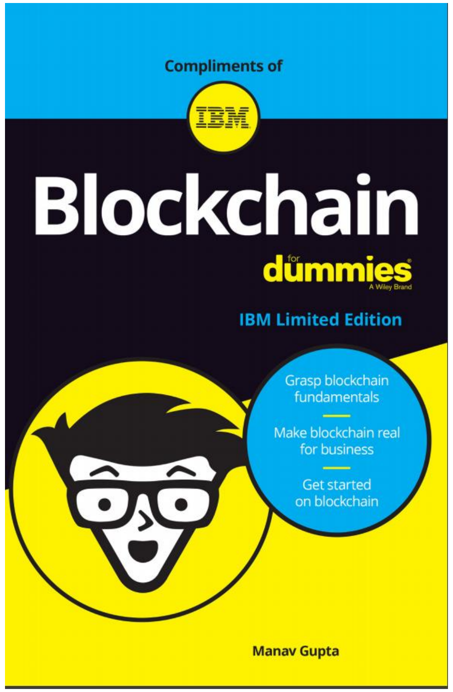
Hyperledger

Hyperledger is a Linux Foundation open-source, collaborative effort to create blockchain technology suitable for the enterprise.

Hyperledger Fabric

Hyperledger Fabric is a blockchain framework implementation and one of the Hyperledger projects hosted by The Linux Foundation with a modular architecture and pluggable, interchangeable services using container technology.

- Support a wide variety of industry use cases with different requirements
- Comply with statutes and regulations that exist today
- Support verified identities and private and confidential transactions
- Support permissioned, shared ledgers
- Support performance, scaling, auditability, identity, security, and privacy
- Reduce costly computations involved in proof of work


Compliments of
IBM
Blockchain
for dummies
A Wiley Brand
IBM Limited Edition
Grasp blockchain fundamentals
Make blockchain real for business
Get started on blockchain
Manav Gupta

Unlike other blockchain implementations like Bitcoin or Ethereum, Hyperledger Fabric fulfills all four key elements of a blockchain for business:

» Permissioned network: Collectively defined membership and access rights within your business network

» Confidential transactions: Gives businesses the flexibility and security to make transactions visible to select parties with the correct encryption keys

» Doesn’t rely on cryptocurrencies: Doesn’t require mining and expensive computations to assure transactions

» Programmable: Leverages the embedded logic in smart contracts to automate business processes across your network

Download the latest version for Windows

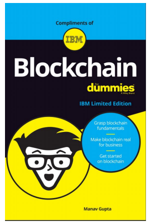
https://www.python.org/downloads/

What are hash functions

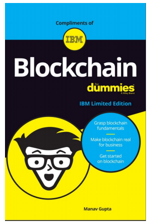
https://learncryptography.com/hash-functions/what-are-hash-functions

Developing APIs is hard - Postman makes it easy

https://www.getpostman.com/



You can find the latest blockchain technology use case examples at www.ibm.com/blockchain/for-business.html



For guidance on how to set up a blockchain network and start coding, see “IBM Blockchain 101: Quick-start guide for developers” at http://ibm.biz/QuickStartGuide

Simple blockchain implementation based on Python:
https://hackernoon.com/learn-blockchains-by-building-one-117428612f46

Simple blockchain implementation based on Node.js:
https://github.com/fshaikh/Blockchain

A Practical Introduction to Blockchain with Python
http://adilmoujahid.com/posts/2018/03/intro-blockchain-bitcoin-python/

A mini blockchain application in pure Python:
https://github.com/satwikkansal/ibm_blockchain

https://www.ibm.com/developerworks/cloud/library/cl-develop-blockchain-app-in-python/cl-develop-blockchain-app-in-python-pdf.pdf

https://tradecryptolive.net

https://blockexplorer.com

Python test kode PoW:

```
import hashlib
proof=0
last_proof=5
guess = f'{last_proof}{proof}'.encode()
guess_hash = hashlib.sha256(guess).hexdigest()
while guess_hash[:4] != "0000":
    proof +=1
    guess = f'{last_proof}{proof}'.encode()
    guess_hash = hashlib.sha256(guess).hexdigest()
    print(guess_hash)
    print(proof)
```