BLOCKCHAIN

What is it & how to connect it in a business case.

Aaron Symanski, CTO, Change Healthcare

September 2017

CHANGE HEALTHCARE

Agenda

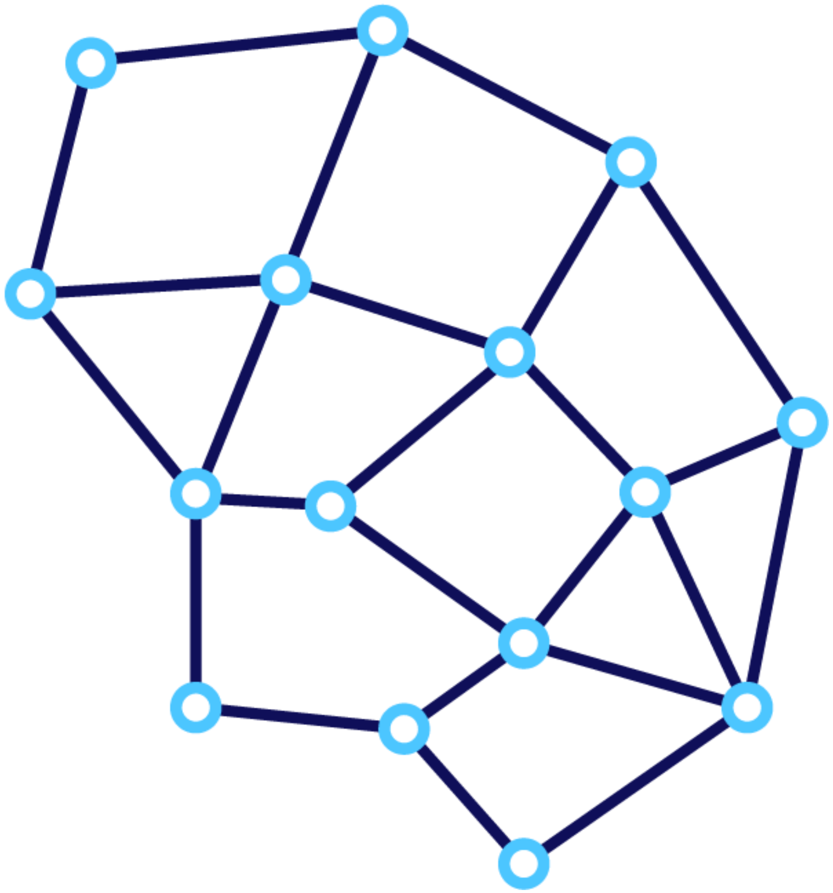
- Blockchain in my business case?
- Blockchain worthwhile calculation
- Legal Considerations
- Smart Contracts
- Summary

CHANGE HEALTHCARE

Blockchain in my business case?

CHANGE
HEALTHCARE

What is Blockchain?



Information Storage

Consensus Model

Associated with Blockchain

- Public Blockchains
- Permissioned Blockchains
- Private Blockchains
- Smart Contracts

Not Blockchain

- Interoperability
- Encryption of data
- Participant lists
- Speed (real-time)

CHANGE HEALTHCARE

What is Blockchain: Information Storage

It’s a list of transactions, grouped into Blocks, and locked immutably together forever.

Blockchain			
Block 0	Block 1	Block 2	Block 3
Sue pays Jill $100	Jill pays Milton $25	Pat pays Rowan $75	Pat pays Sue $110
Milton pays Pat $250	Milton pays Angel $25	Rowan pays Sue $150	Sue pays Angel $50
Rowan pays Angel $75	Pat pays Rowan $25	Angel pays Pat $125	Angel pays Milton $75
Null lock (origin block)	Crypto lock (hash) of Block 0	Crypto lock (hash) of Block 1	Crypto lock (hash) of Block 2

What is Blockchain: Consensus Model

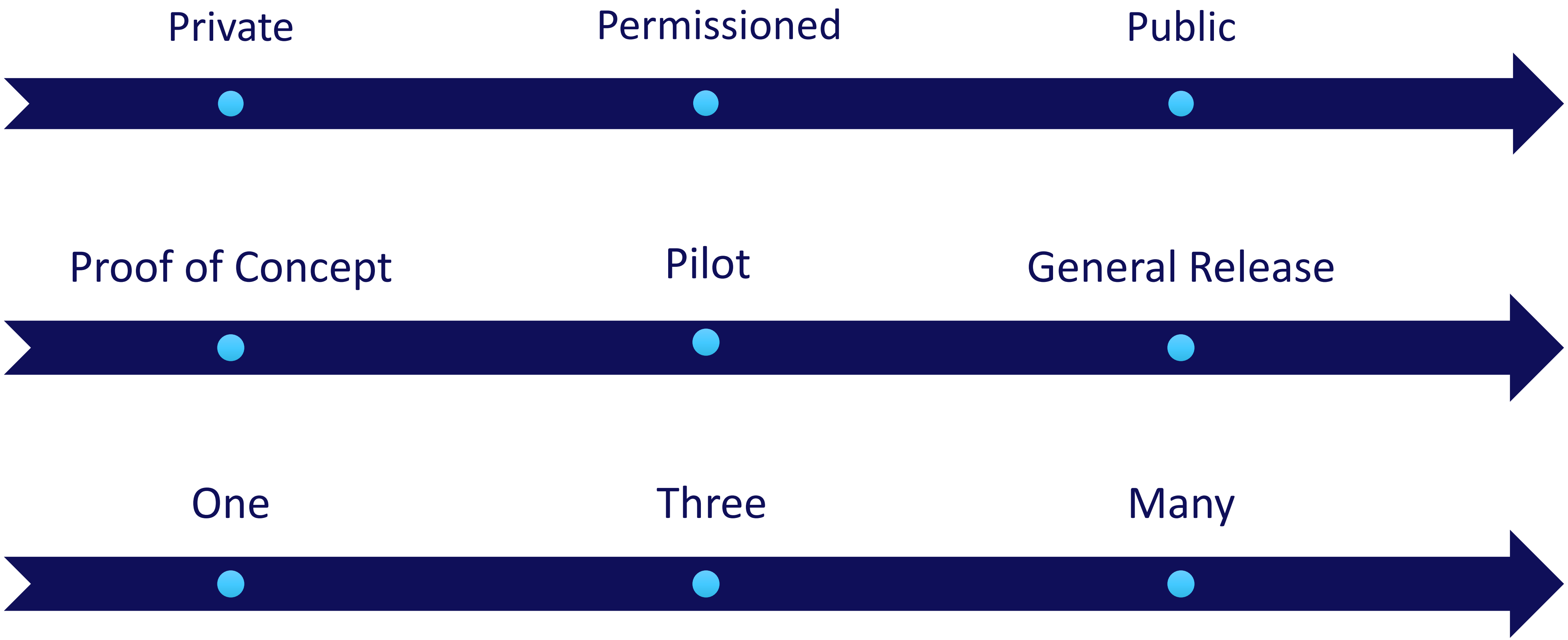
50% + 1: Majority rules

Trust Issues…

- Proof of Work (Bitcoin): compete to add by solving a puzzle
- Proof of Stake: more coins you own, better your odds
- Proof of Activity: combines Work + Stake
- Proof of Burn: Irretrievable "pay to earn"
- Proof of Capacity: The more storage, the better the odds
- Proof of Elapsed Time: Waiting to win (Intel)

CHANGE HEALTHCARE

Types of Blockchain Networks



CHANGE HEALTHCARE

Smart Contracts

Perfectly written contracts performing perfectly

Benefits:

- No humans at the wheel.
- Automatic execution of conditional financial transactions
- Encoded contracts can be tested before placing them onto the blockchain
- Survivability (DR/BR)
- Discoverability
- Aggregate exposure opportunity (for both parties)

Risks:

- No humans at the wheel.
- Automatic execution of conditional financial transactions
- Who pays the costs of running the smart contract?
- How does the network decide to stop running a smart contract?
- Can you verify the smart contract is unhackable?
- What if the participating entities do not exist when the contract executes?

Not Blockchain: Encryption, Participant Lists, Speed

Interoperability

- Blockchain is the storage.
- Blockchain is not the language of what is being stored.
- Agreeing on the descriptions, the nouns and verbs is interoperability.

Encryption:

- If the data stored in the transaction is encrypted, how can anyone know what was agreed? All we can agree is that all the encrypted information looked the same.
- Key management: once a key is provided to access encrypted data, it cannot be revoked. The Blockchain is immutable…

Participant Lists:

- If private or permissioned, you know the list
- If public, one can have many identities.

Speed:

- Bitcoin, with thousands of calculating nodes, tries to respond in under 10 minutes. Times are often higher, sometimes hours.

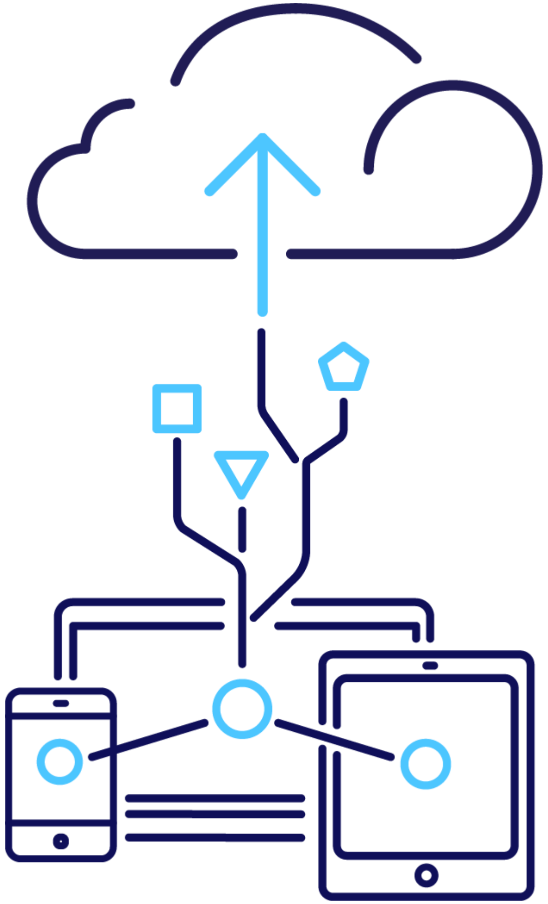
CHANGE HEALTHCARE

What makes Blockchain compelling?

We all want a future where information is:

- Immediately available
- Is identical everywhere it is stored
- Has a complete history
- Is immutable
- AND is under the control of the entity that ‘owns’ the data.

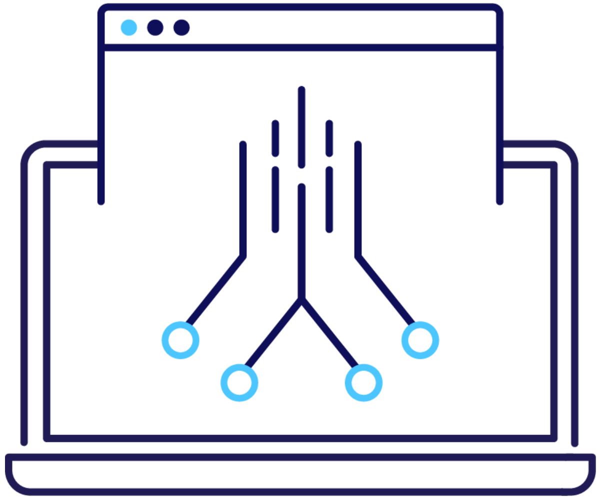
It’s the last item. That’s where Blockchain doesn’t bring an innate solution. Lots of innovation is occurring in the market…



CHANGE HEALTHCARE

Blockchain is innovating

- Protocols
- Storage
- Consensus Models
- Business Cases



What does Blockchain replace?

Trust

- Bitcoin is founded on the basis that no participant trusts another.
- Blockchain was created by Bitcoin to solve that issue.
- Everyone has an identical, cryptographically validated copy.
- Data only is added through a process that is so expensive to overwhelm that, simply, it is not worth the effort.

Where is Blockchain in use today?

Bitcoin

Original implementation. Bitcoin has had its growing pains with a recent ‘hard fork’ between its miners and ‘core’ teams as well as an expected new ‘hard fork’ in November as the network tries to coordinate upgrades in speed and functionality.

Ethereum

Strong newcomer. *Ethereum has become the front line for smart contract development, both directly and as a technology platform for other, new blockchains with modifications to solve some of the smart contract challenges*

Guernsey

Real, production, financial usage. Northern Trust and the Guernsey regulator are executing and monitoring private equity transactions.

Bitcoin and Blockchain by the numbers

White Paper Published
Oct 2008
Satoshi Nakamoto

One Coin
$4,524.63

Avg Block
8-10 min

Trans v. Mine
17.87%

274,530 Transactions/day

11 Crypto currencies with a market cap of > $1 Billion

900+
cryptocurrencies

81%
Miner geographic concentration

$35 and rising
cost per transaction

Sources: Wikipedia, Blockchain.info, buybitcoinworldwide.com/mining/pools

CHANGE HEALTHCARE

Section 2.0

Blockchain: evaluating utility

CHANGE HEALTHCARE

Factors

When considering Blockchain, ask the following questions:

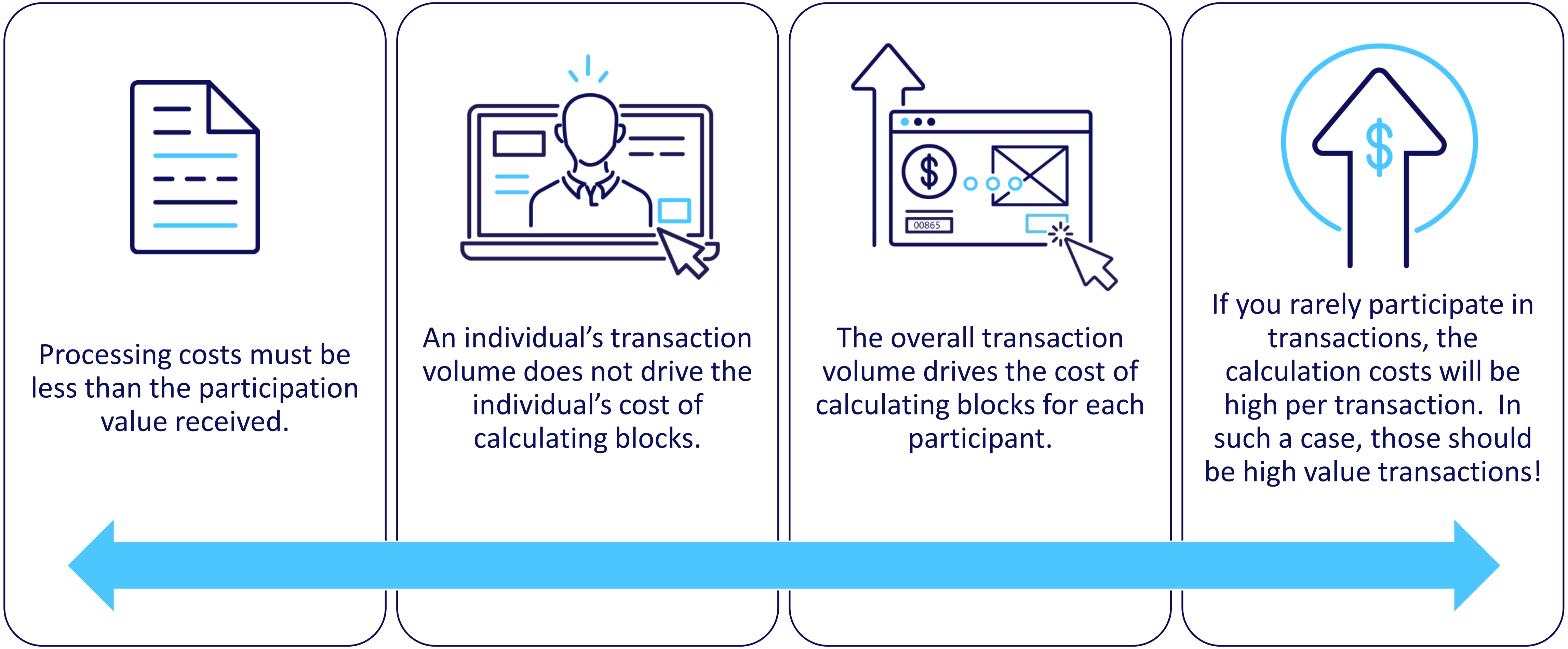
- How many participants?
- How is value shared across the participants?
- Are immutable records important?
- What is needed for speed and latency?
- Can the business model support the costs of consensus?
- Do we have an explicit trust model?

Participants in a Blockchain

Private:	Permissioned:	Public:
• If there is only one participant, all blockchain brings is a cryptographically locked chain of transactions. It's a mathematically proveable audit log. To avoid the situation of being accused of rewriting the chain in ones own favor, best practice would be to store a copy in escrow.	• External technology limits the participants.	• Any one can participate.

CHANGE HEALTHCARE

Value Shared across Blockchain participants



Processing costs must be less than the participation value received.

An individual's transaction volume does not drive the individual's cost of calculating blocks.

The overall transaction volume drives the cost of calculating blocks for each participant.

If you rarely participate in transactions, the calculation costs will be high per transaction. In such a case, those should be high value transactions!

CHANGE HEALTHCARE

Blockchain is immutable

If the business process actually ‘rewrites’ history, blockchain is not the right choice.

If the business process does not value history, blockchain is not the right choice.

If the business process stacks updates on top of the original record to show the history of modifications, blockchain is a candidate. Most processes are like this one.

Blockchain stores nouns. It records the history of verbs that occur to those nouns.

Blockchain Speed and Latency

Business processes that are sensitive to time should establish strong success criteria when considering Blockchain.

Speed and latency is affected by:

- Blockchain Protocols:
  (Hyperledger Fabric, Iroha, Sawtooth Lake; Ethereum; etc.)
- Consensus Models (PoW, PoET, etc.)
- Block size (2x)
- Block management (Segregated Witness: Segwit, Segwit2x)

Blockchain Consensus: the costs and choice

How much energy/power/compute will be required to balance the trust amongst the participants?

The largest trust difference is the driver.

Bitcoin assumes zero trust.

A permissioned Blockchain balances its trust with the process of receiving permission to participate.

Blockchain Trust is understood

For the consensus choice to be made, establishing the level of trust between **all current and future participants** is critical.

Changing a consensus model once a Blockchain is started is possible, but not recommended…

CHANGE
HEALTHCARE

Section 3.0

Legal Considerations

CHANGE
HEALTHCARE

Legal Considerations

A very new area of law is forming around Blockchain networks.

Consider the liability and risks of:

- Submitting a block containing an inaccurate transaction.
- Accepting a transaction from a bad actor to include in a block.
- Unintentionally submitting a bad transaction.
- Providing information to a Blockchain as an oracle that is later found to be invalid (intentionally or unintentionally).
- Calculating a block that contains a banned transaction (financial) between two parties.
- Eventual regulation that varies by (overlapping and/or nested) jurisdictions

CHANGE HEALTHCARE

Section 4.0

Smart Contracts

CHANGE
HEALTHCARE

Smart Contracts

- Large area of innovation. Goal of ‘automating’ transactions.
- Automatic transactions can have unintended consequences.
    - Participating entities can change over time.
    - Laws and regulations can change.
    - The Smart Contract code can be hacked (DAO 2016)
- Mathematically provable smart contracts are under development.
- Humans being good at predicting unintended consequences…
- Who pays for the never-ending running of the contracts?
- Who pays for the oracles (information injectors)?

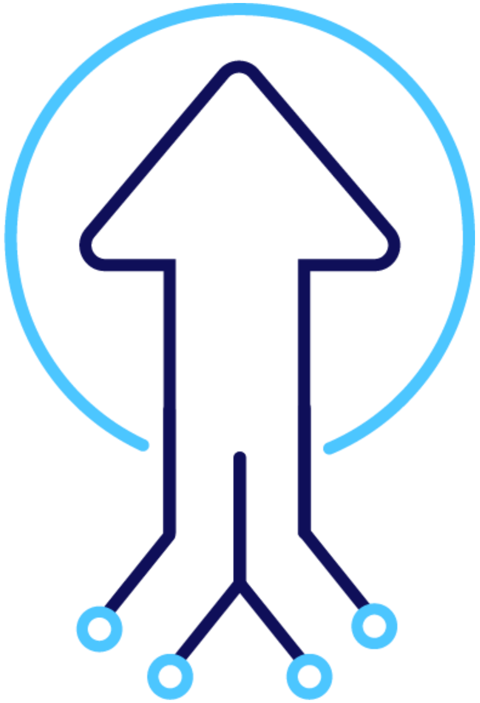
CHANGE HEALTHCARE

Section 5.0

Summary

CHANGE
HEALTHCARE

Summary



Blockchain outside of Bitcoin is in its early days.

Blockchain technology is widely available and innovating.

Blockchain in Production is the next step.

CHANGE HEALTHCARE

CHANGE HEALTHCARE