OLIVER WYMAN

Blockchain applications in Insurance
2018 Annual Fall SEAC Meeting

November 15, 2018

Jeff Guo
Acknowledgement to Helen Duzhou

MARSH & McLENNAN COMPANIES

Agenda

1 What is a Blockchain?

2 Mechanics of Blockchain

3 Current use cases

4 Is it time for Insurance to adapt?

Section 1

What is a Blockchain

Why should actuaries be excited about Blockchain?

What is a Blockchain?

Industries are excited about the key properties of immutability… but be careful what you read!

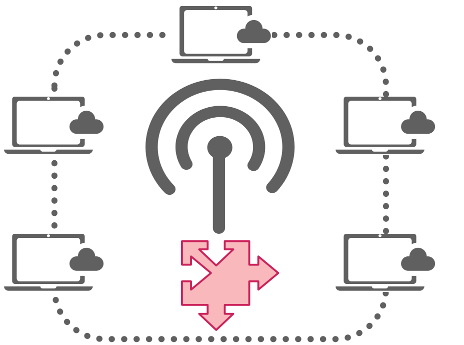
> *A blockchain is a decentralized and distributed database with the ability to efficiently retrieve accurate and secure information at one point in time.*

Key properties

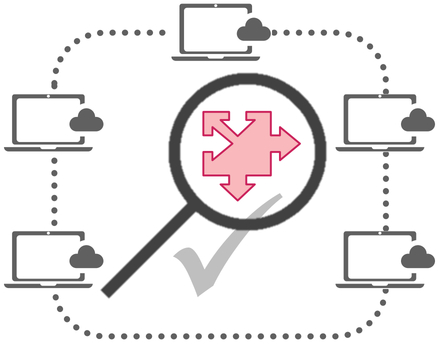
1. **Immutability**
2. **Decentralization**
3. Anonymity

What is a Blockchain?

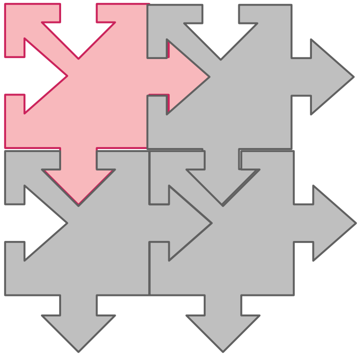
In simplest terms, Blockchain works like…



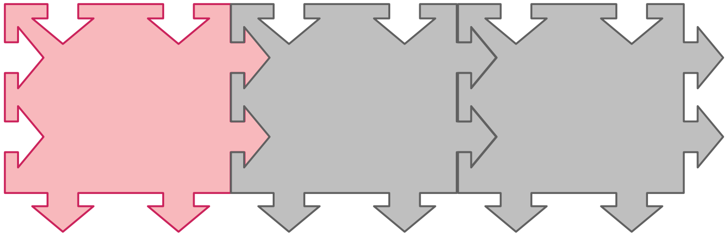
1 **Broadcast:** A transaction is submitted and broadcasted to all participants on the network



2 **Validation:** participants use algorithms to confirm that the submitted transaction is valid



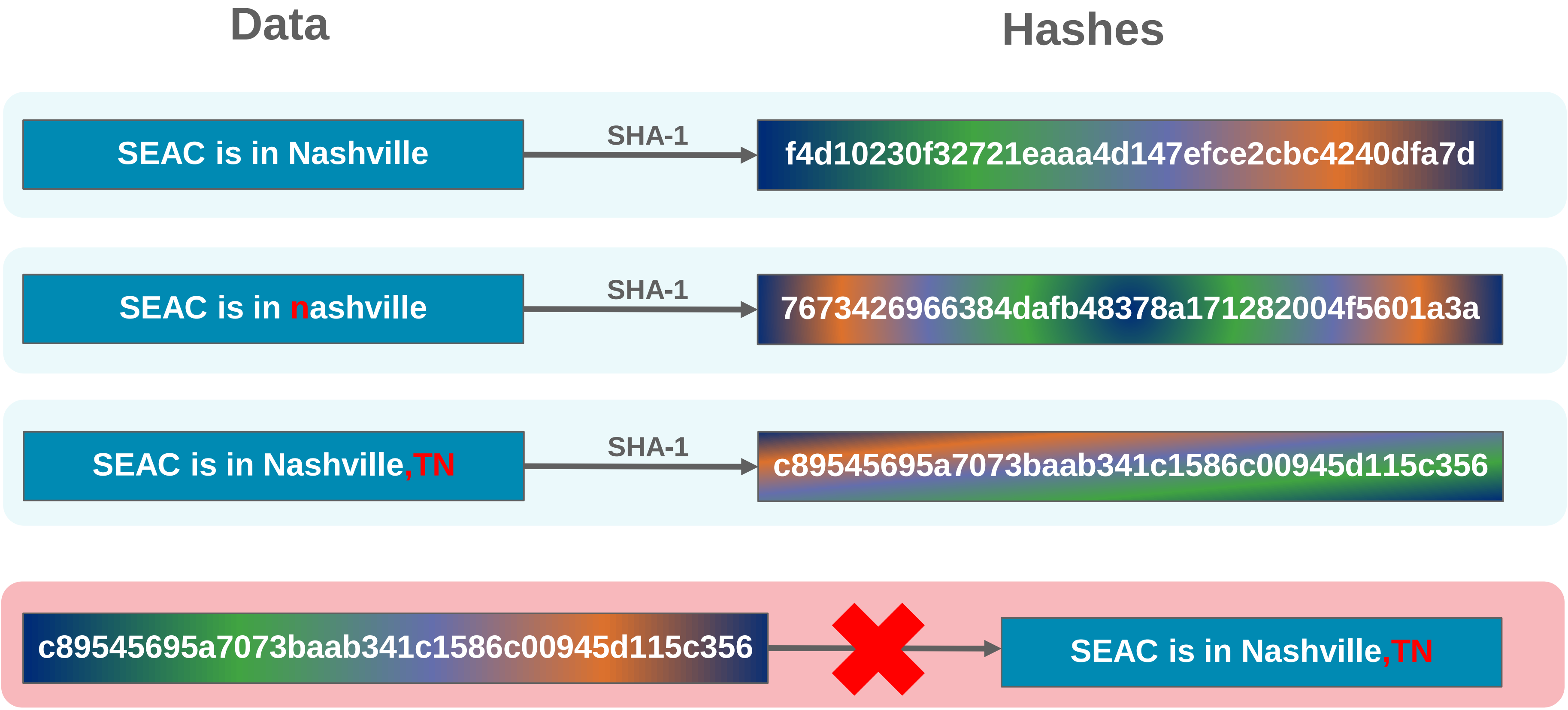
3 **Block formation:** the verified transaction is combined with other verified transactions to form a block



4 **Hashing:** the block is attached to the previous chain of blocks (‘hashing‘) in a manner that is both permanent and immutable

What is a Blockchain?

What is a cryptographic hash function?



Data

Hashes

SEAC is in Nashville → SHA-1 → f4d10230f32721eaaa4d147efce2cbc4240dfa7d

SEAC is in nashville → SHA-1 → 7673426966384dafb48378a171282004f5601a3a

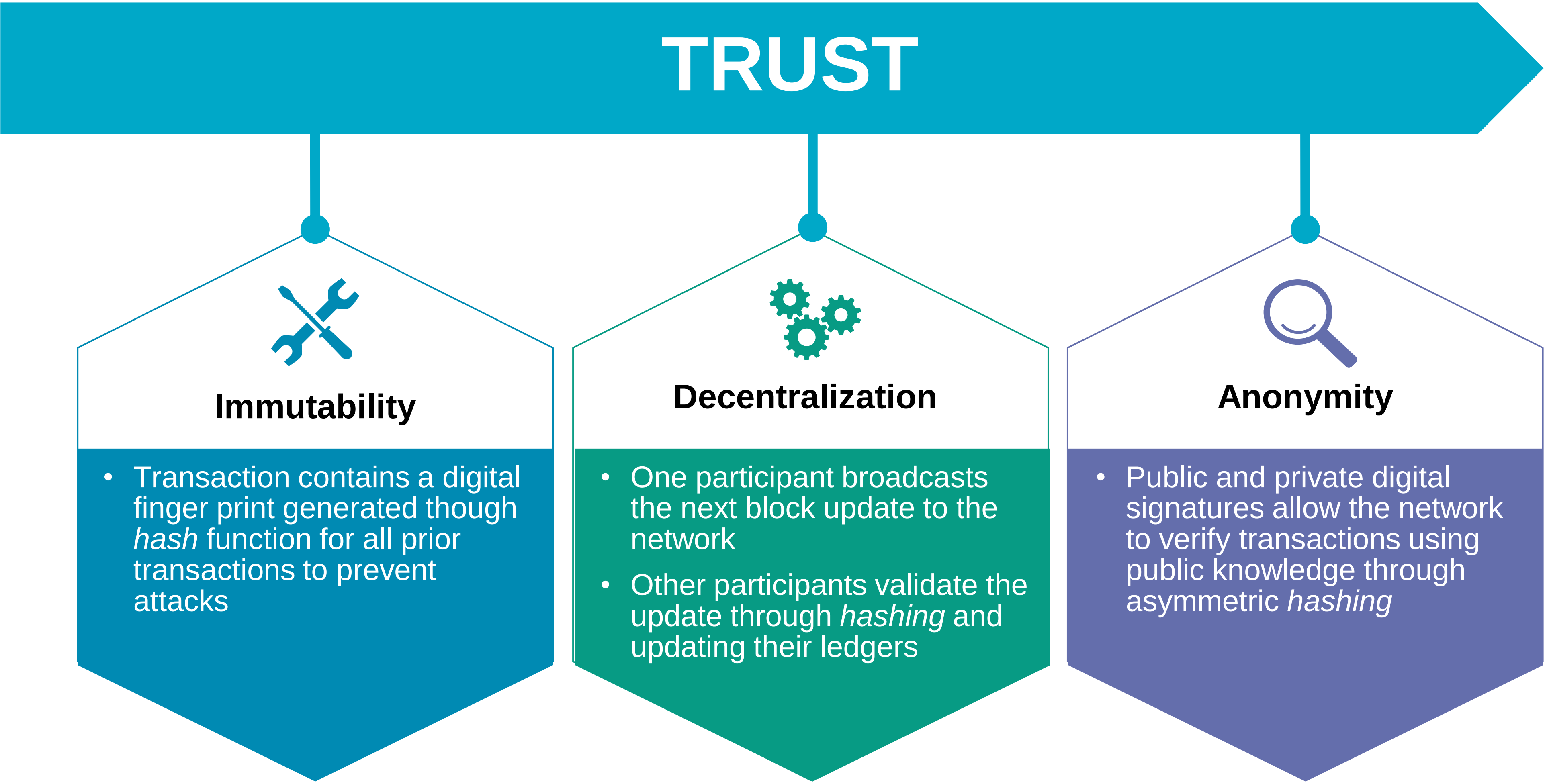
SEAC is in Nashville,TN → SHA-1 → c89545695a7073baab341c1586c00945d115c356

c89545695a7073baab341c1586c00945d115c356 → ✗ → SEAC is in Nashville,TN

Small differences in the input data result in very different hash output and unkown input data can not be reconstructed

What is a Blockchain?

How does Blockchain achieve these key properties?



TRUST

Immutability

- Transaction contains a digital finger print generated though *hash* function for all prior transactions to prevent attacks

Decentralization

- One participant broadcasts the next block update to the network
- Other participants validate the update through *hashing* and updating their ledgers

Anonymity

- Public and private digital signatures allow the network to verify transactions using public knowledge through asymmetric *hashing*

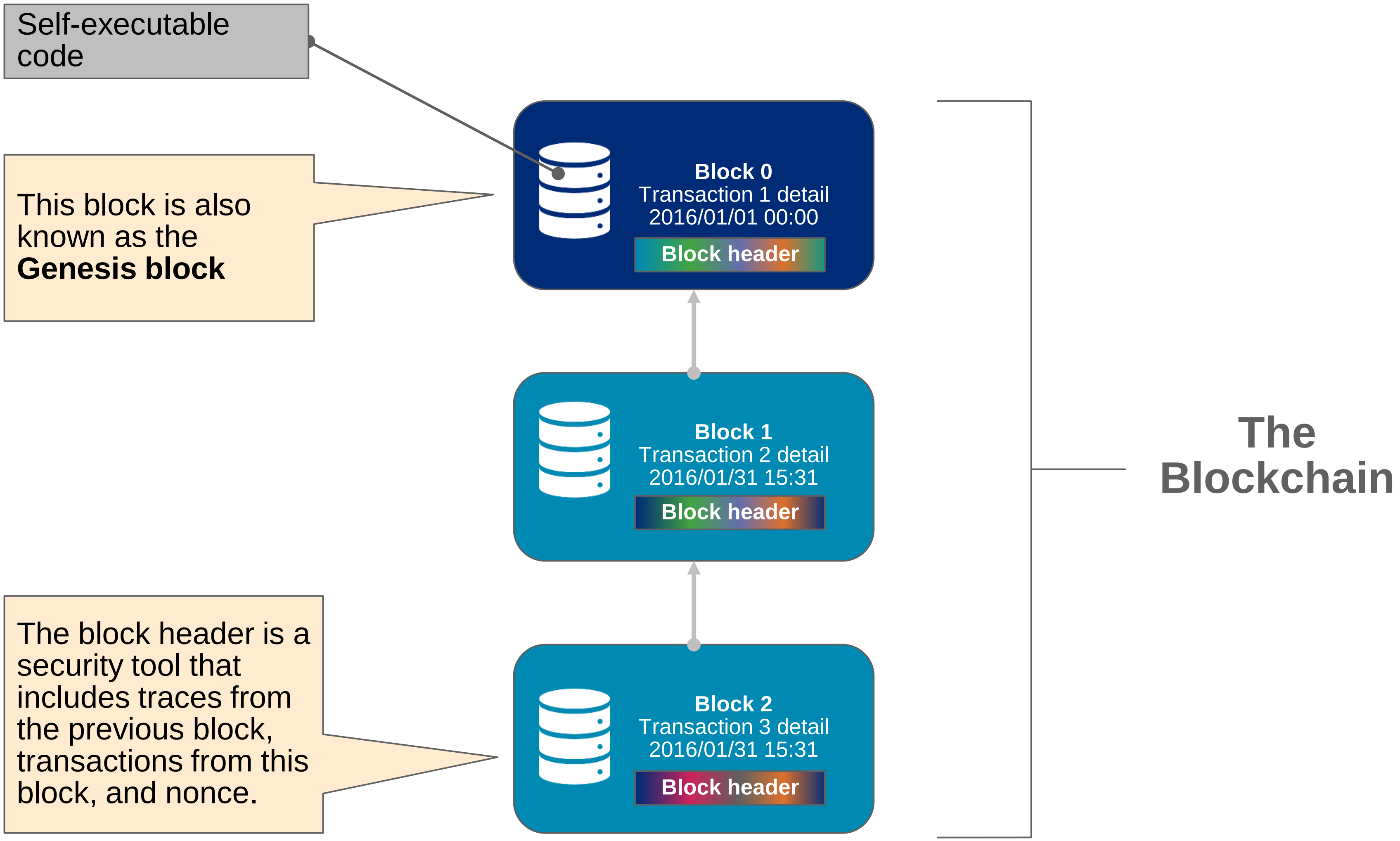
All key features of Blockchain rely on cryptographic hashes that is impossible to reconstruct unknown inputs

Section 2

Mechanics of Blockchain

Mechanics of Blockchain

A blockchain is made up of blocks, that each point to the preceding parent



Self-executable code

This block is also known as the **Genesis block**

The block header is a security tool that includes traces from the previous block, transactions from this block, and nonce.

Block 0
Transaction 1 detail
2016/01/01 00:00
Block header

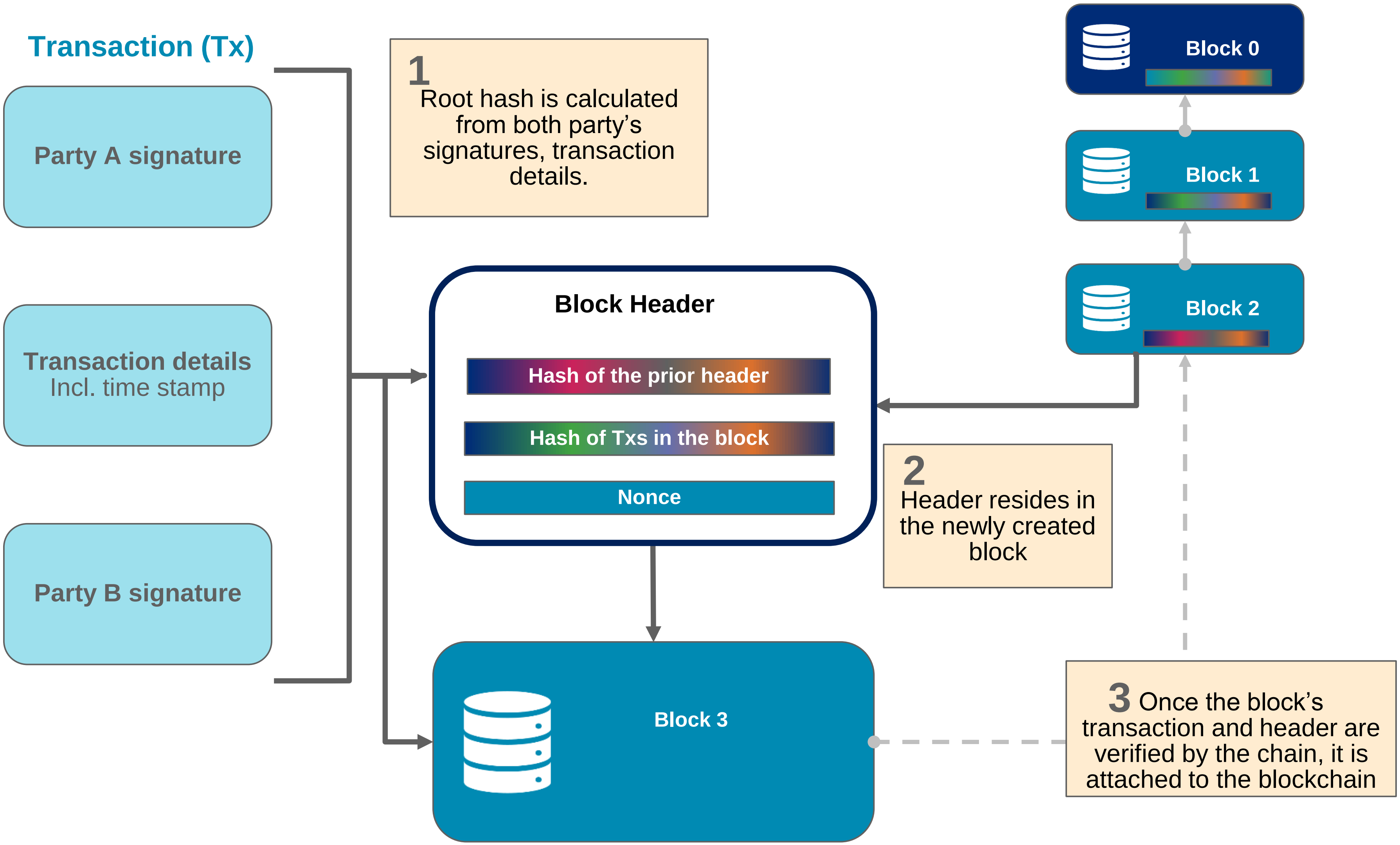
Block 1
Transaction 2 detail
2016/01/31 15:31
Block header

Block 2
Transaction 3 detail
2016/01/31 15:31
Block header

The Blockchain

Mechanics of Blockchain

To add transactions to a blockchain, cryptographic hashes are calculated for the new block, which is verified by the rest of the network



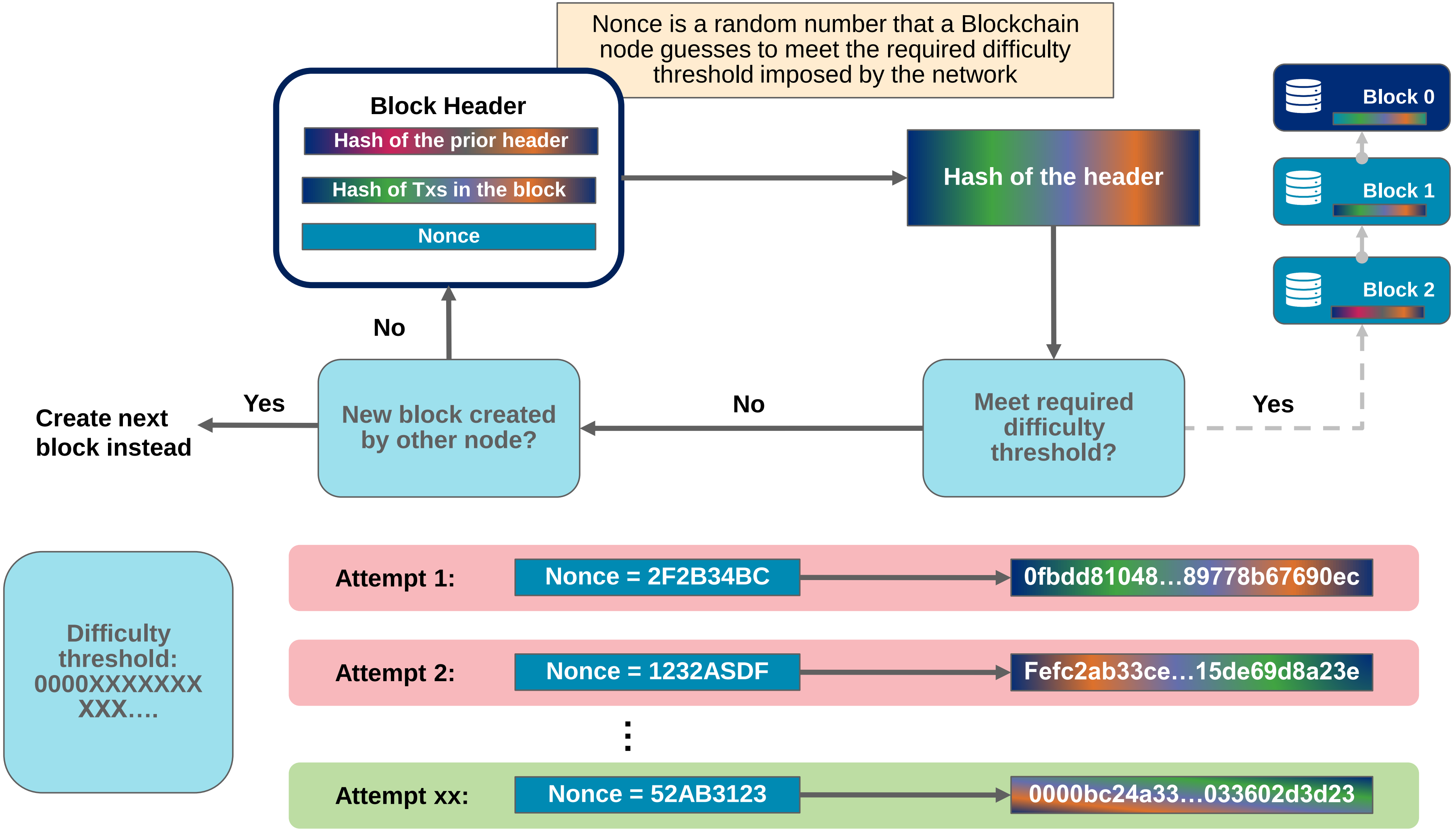
1 Root hash is calculated from both party's signatures, transaction details.

2 Header resides in the newly created block

3 Once the block's transaction and header are verified by the chain, it is attached to the blockchain

Mechanics of Blockchain

The iterative process, called “mining”, creates collective memories by distributing the chance to update based on the computation power



Nonce is a random number that a Blockchain node guesses to meet the required difficulty threshold imposed by the network

Block Header

Hash of the prior header

Hash of Txs in the block

Nonce

Hash of the header

Meet required difficulty threshold?

No

New block created by other node?

No

Yes

Create next block instead

Yes

Block 0

Block 1

Block 2

Difficulty threshold: 0000XXXXXXXXXX….

Attempt 1: Nonce = 2F2B34BC → 0fbdd81048…89778b67690ec

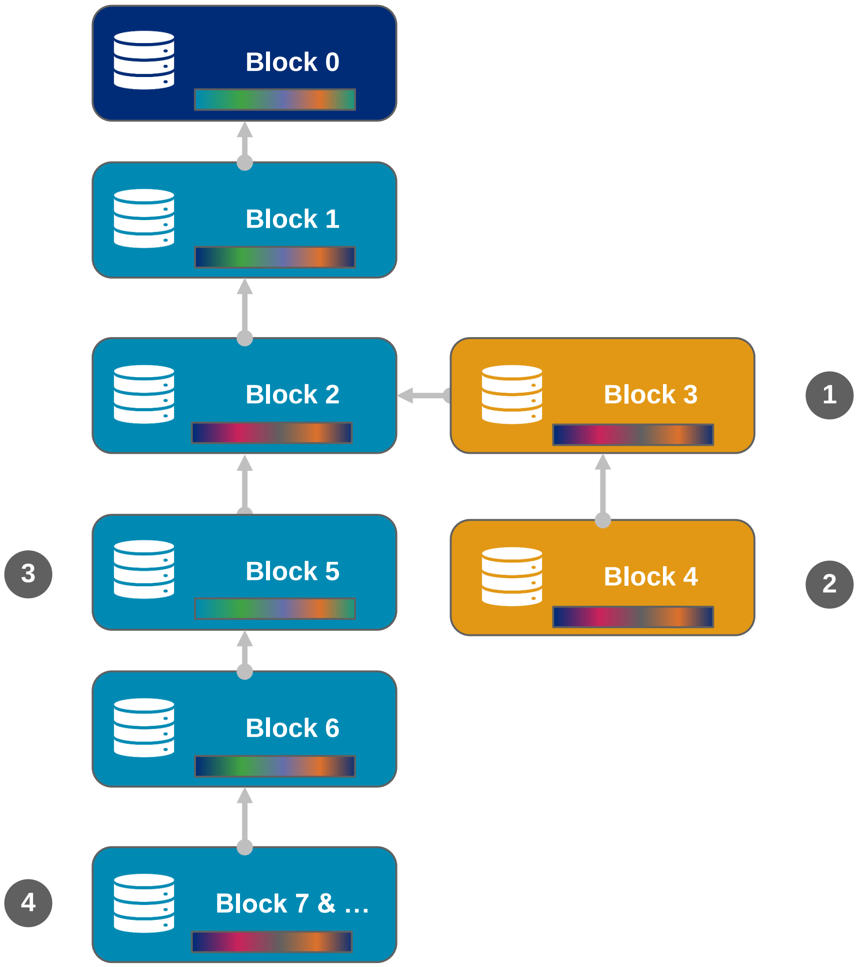
Attempt 2: Nonce = 1232ASDF → Fefc2ab33ce…15de69d8a23e

⋮

Attempt xx: Nonce = 52AB3123 → 0000bc24a33…033602d3d23

Mechanics of Blockchain

Case study: how Blockchain prevents fraudulent transactions through collective memories of the network



1. Helen's Henchmen Inc. created a fraudulent transaction **(Block 3)** by sending 10 coins that she does not own to Corporate Jeffery Limited.

   With the 30% total computation power, Helen and Jeffery were able to get her block verified and appended to Block 2 at 30% chance.

2. Corporate Jeffery then trades the 10 coins back to Helen's Henchmen which was verified again at 30% chance. **(Block 4)**

3. Due to the distributed network, there are 70% chance for people to verify the right chain

   They append verifiable blocks to Block 2. **(Block 5)**

4. With several iterations, Block 3 and 4 become part of the orphaned chain, which eventually gets truncated from everyone's memory. **(Block 6 and onwards)**

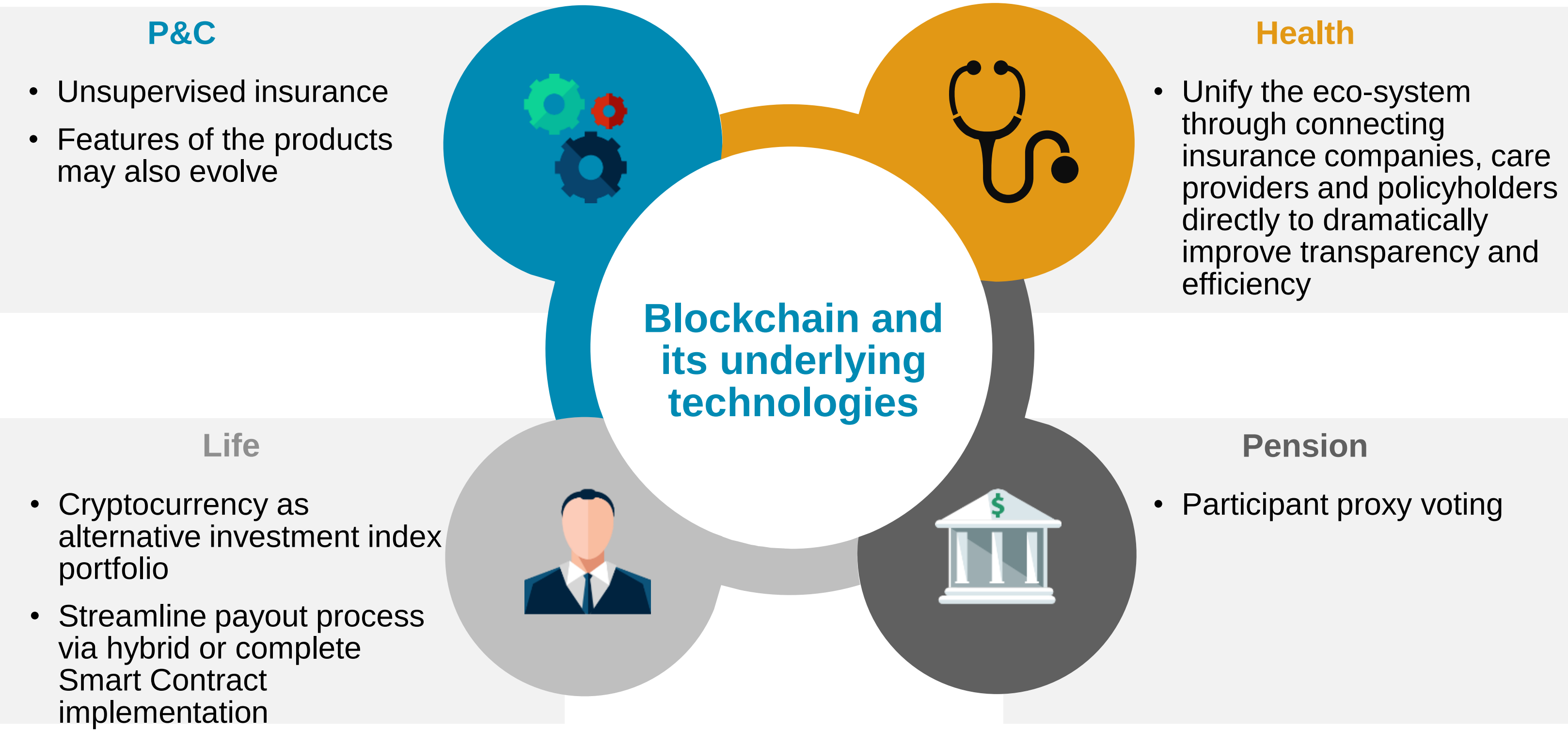
Section 3 | Current use cases of Blockchain

Insurance applications for Blockchain

Several start-ups have sprung up to take advantage of these opportunities

Example	Description	Use Case
Fraud detection	• Easily validated "fingerprint“ through encrypted and immutable nature	Blockverify Everledger
Smart contracts	• Contracts can be written as code in the blockchain • The code will self-execute once a triggering event is met, without the need for third-party intervention • Regulators can use the blockchain to understand market activity while maintaining anonymity of the individual players	Etherisc Edgelogic
Real time insurance quotes	• As the blockchain updates itself continuously, it can self-regulate the appropriate insurance premium at all time • These insurance quotes also pave the way for developing tailored products which addresses each customer's unique concerns.	Safeshare Global
Optimize existing systems	• An insurer today has to validate their customers against that of the service providers, which produces a higher chance of error. A shared ledger lowers the cost of validation and identifies the policy holder • A drawback with blockchains today is the amount of time it takes to validate a transaction	Credits (*)

Insurance applications for Blockchain
10-year outlook



Blockchain and its underlying technologies

P&C

- Unsupervised insurance
- Features of the products may also evolve

Health

- Unify the eco-system through connecting insurance companies, care providers and policyholders directly to dramatically improve transparency and efficiency

Life

- Cryptocurrency as alternative investment index portfolio
- Streamline payout process via hybrid or complete Smart Contract implementation

Pension

- Participant proxy voting

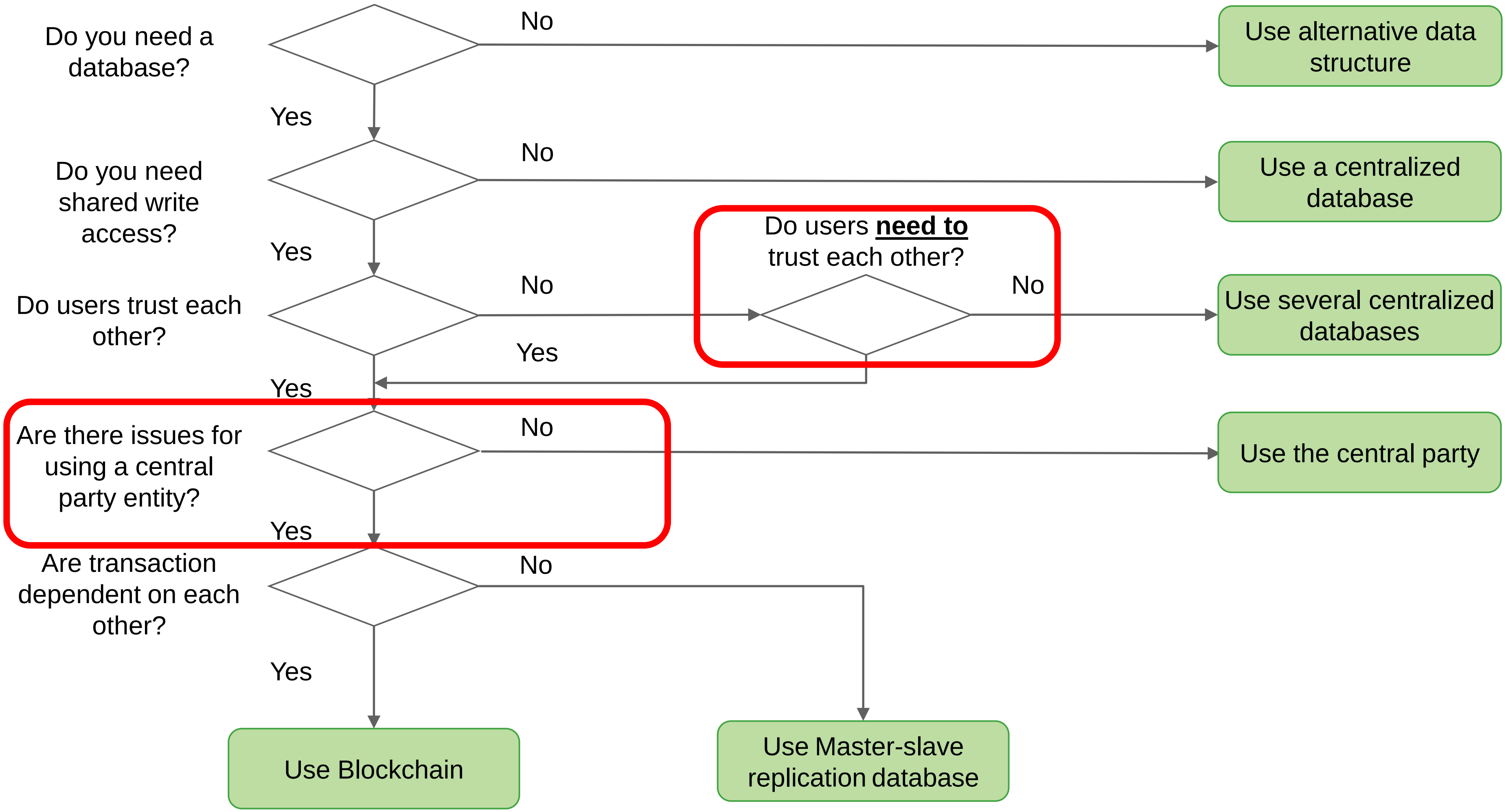
As insurance evolves, blockchain can allow for multiple insurers or even individuals to participating in risk pooling for reinsurance.

Blockchain has great potentials in the insurance industry

Section 4 Time to adapt?

Time to adapt?

Do you even need a Blockchain? More likely than not, existing technology already has solutions for insurers' issues on hand



Do you need a database?
No
Use alternative data structure
Yes
Do you need shared write access?
No
Use a centralized database
Yes
Do users trust each other?
No
Do users **need to** trust each other?
No
Use several centralized databases
Yes
Yes
Are there issues for using a central party entity?
No
Use the central party
Yes
Are transaction dependent on each other?
No
Use Master-slave replication database
Yes
Use Blockchain

Time to adapt?

Insurers face frictional costs in implementing Blockchain technology

Issue	Description
Complex legacy system	Insurance companies have complex legacy systems that are impossible or very hard to move onto the blockchain
Scalability	Consensus-based validation and continuous replication becomes data-intensive and has high storage requirements relative to the databases that we currently use
First-mover cost	There are considerable up-front costs to first-players of the blockchain who have to develop the market, such as the technical standards on how to manage a blockchain
Technology innovation	Cryptographic hash is fundamental for Blockchain's security. Modern cryptographic algorithms can take centuries to break by using a traditional deterministic computer but will be rendered essentially useless by matured quantum computing technology
Regulatory changes	Blockchain is currently not desirable as a public ledger of insurance details due to changes in regulations

Questions

Q&A