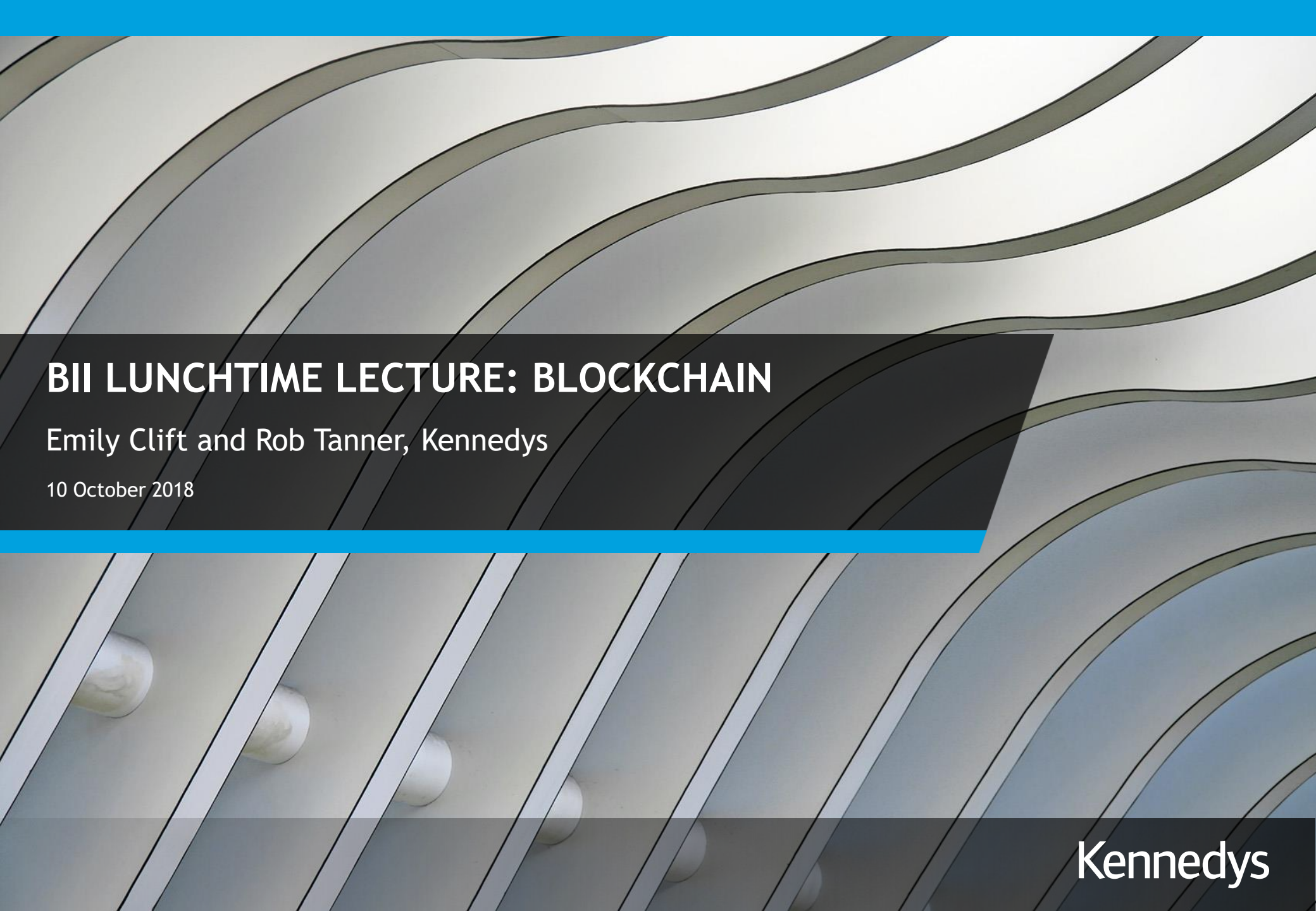


BII LUNCHTIME LECTURE: BLOCKCHAIN

Emily Clift and Rob Tanner, Kennedys

10 October 2018

Kennedys

Outline

Basic principles of blockchain technology	3
Examples	5
The Future	9
Questions?	12

BASIC PRINCIPLES OF BLOCKCHAIN TECHNOLOGY

Kennedys

A (very) basic introduction to Blockchain Technology

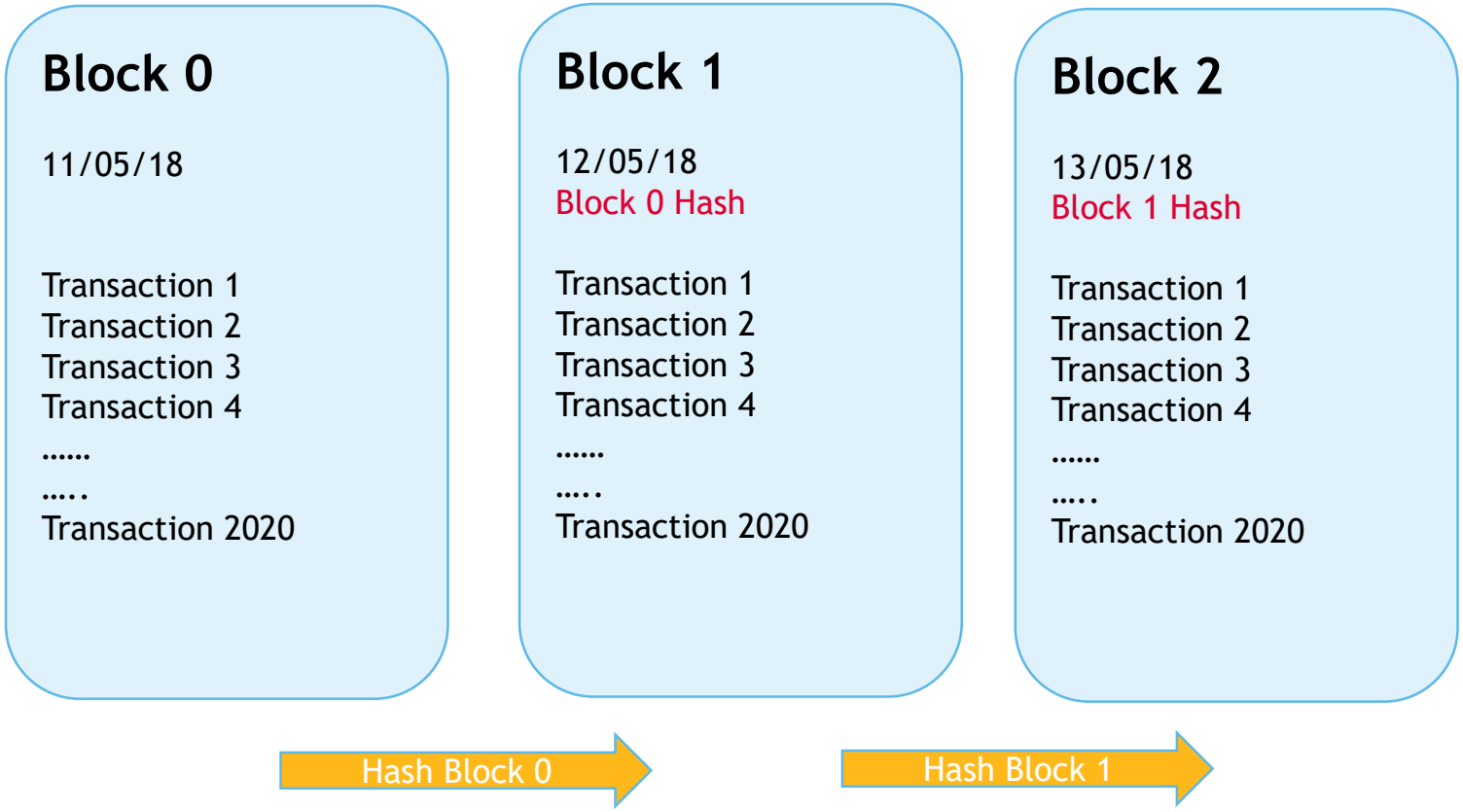
Blockchain is a (i) Decentralised (ii) Distributed (iii) Immutable ledger of (iv) transactions. Think of a digital version of a old paper accountant's ledger.

As there is no 'central authority' (ie: Bank), the system is said to be 'decentralised'.

Each computer (node) on the network has a copy (distributed) of a 'write only' (immutable) list of transactions which can represent any form of data.

The most common example is BitCoin which is both a currency and a system of transfer of cryptocurrency which operates on a 'blockchain' model.

Example chain of blocks



How does it work?

Each transaction is posted into a communal ‘pot’ of transactions which are then collated into a ‘block’ and ‘mined’. It is this process of mining which ensures the security of the block chain at the cost of computational expense.

Each block contains a number of objects:

(i) The hash value of the previous block

(ii) The nonce value of the current block

(iii) The list of transactions (whatever they may be)

(iv) The hash of the current block (the ‘Digital Signature’)

This contents ensures consistency, implies trust and the security of the Blockchain technology.

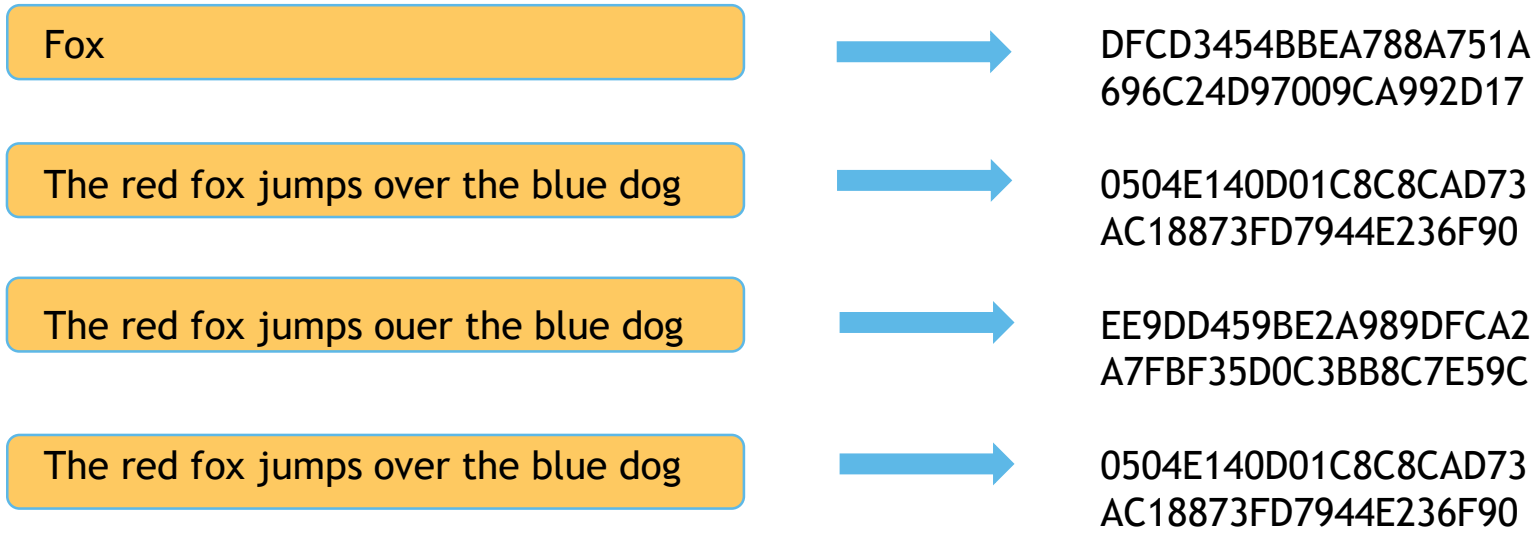
Hashing and the nonce value

Hashing is the exercise of taking data (of any length) and converting it into a seemingly random string of characters of a fixed length. In the case of Bitcoin, SHA256 is used, and so the 'hash value' is a string of 256 0's and 1's or, alternatively, a string of 64 hexadecimal characters (0-9, A-F)

This string of characters is based solely on the data input into the hashing algorithm. As such, the hash value for 'Kennedys' would be different to the hash value for 'kennedys'.

The exercise of mining is to find the nonce value which, when added to (i) the string representation of the list of transactions; and, (ii) the hash of the previous block; that are then put through the hashing algorithm, gives a hash value meeting certain criteria. This 'digital signature' verifies the contents of the block.

Hashing: one way encryption



https://passwordsgenerator.net/sha1-hash-generator/

Security

This form of hashing is computationally expensive and, as time goes on, the ‘difficultly’ of the hash criteria will increase. Blockchain technology works (at present) on a proof-of-work concept, which makes it quick to check the nonce value, but potentially slow to calculate.

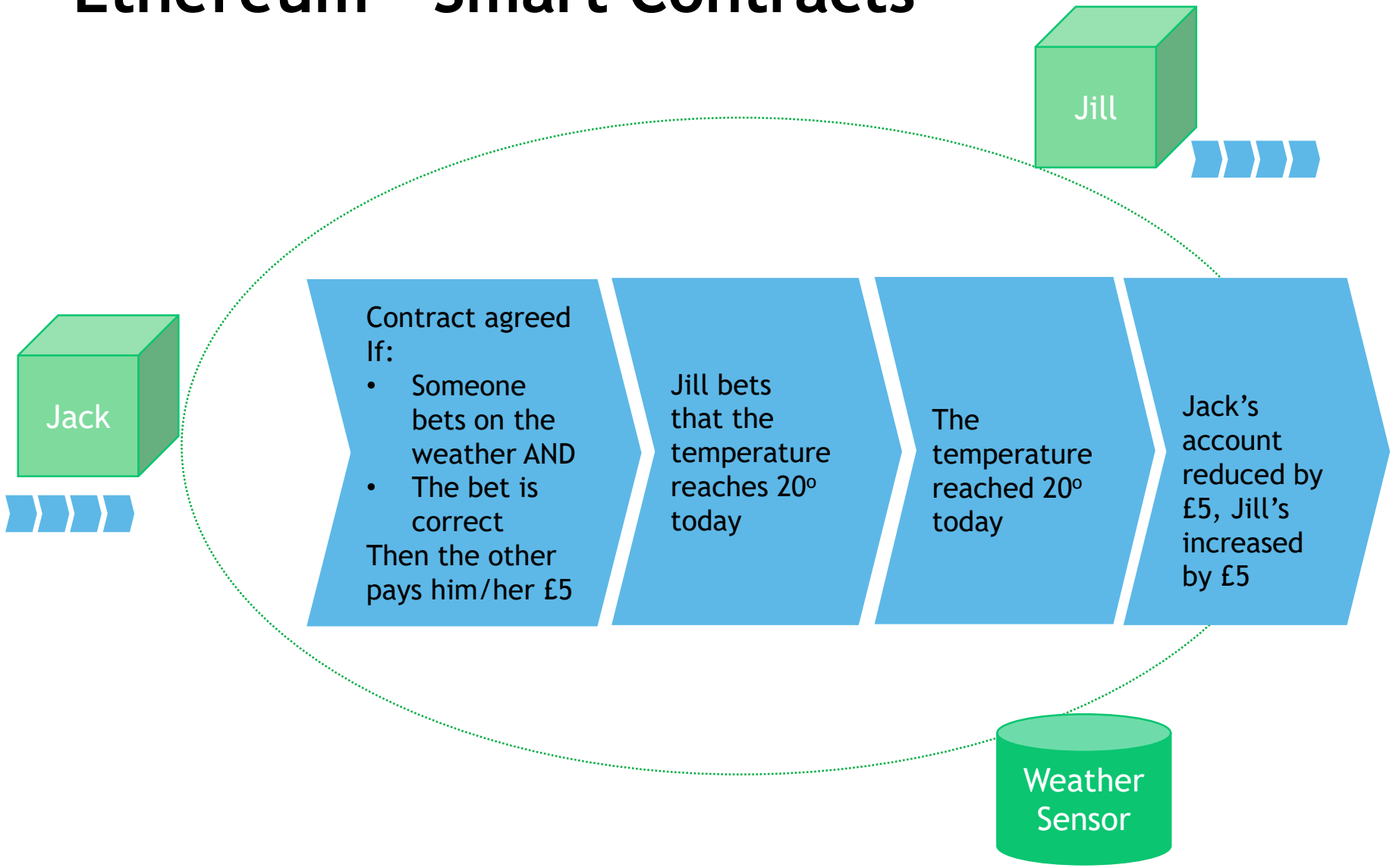
This provides 2 aspects of security:

1. In order to ‘alter’ a transaction, you will need to recalculate the nonce values for every subsequent block in the chain; and,
2. To maintain this ‘fork’ you will need to have 51% or more of the computing power on the network to outstrip the mining of any subsequent blocks by the other nodes.

EXAMPLES

Kennedys

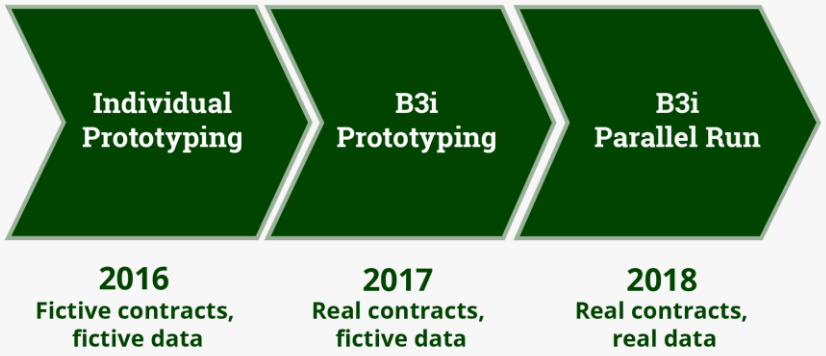
Ethereum - Smart Contracts



B3i

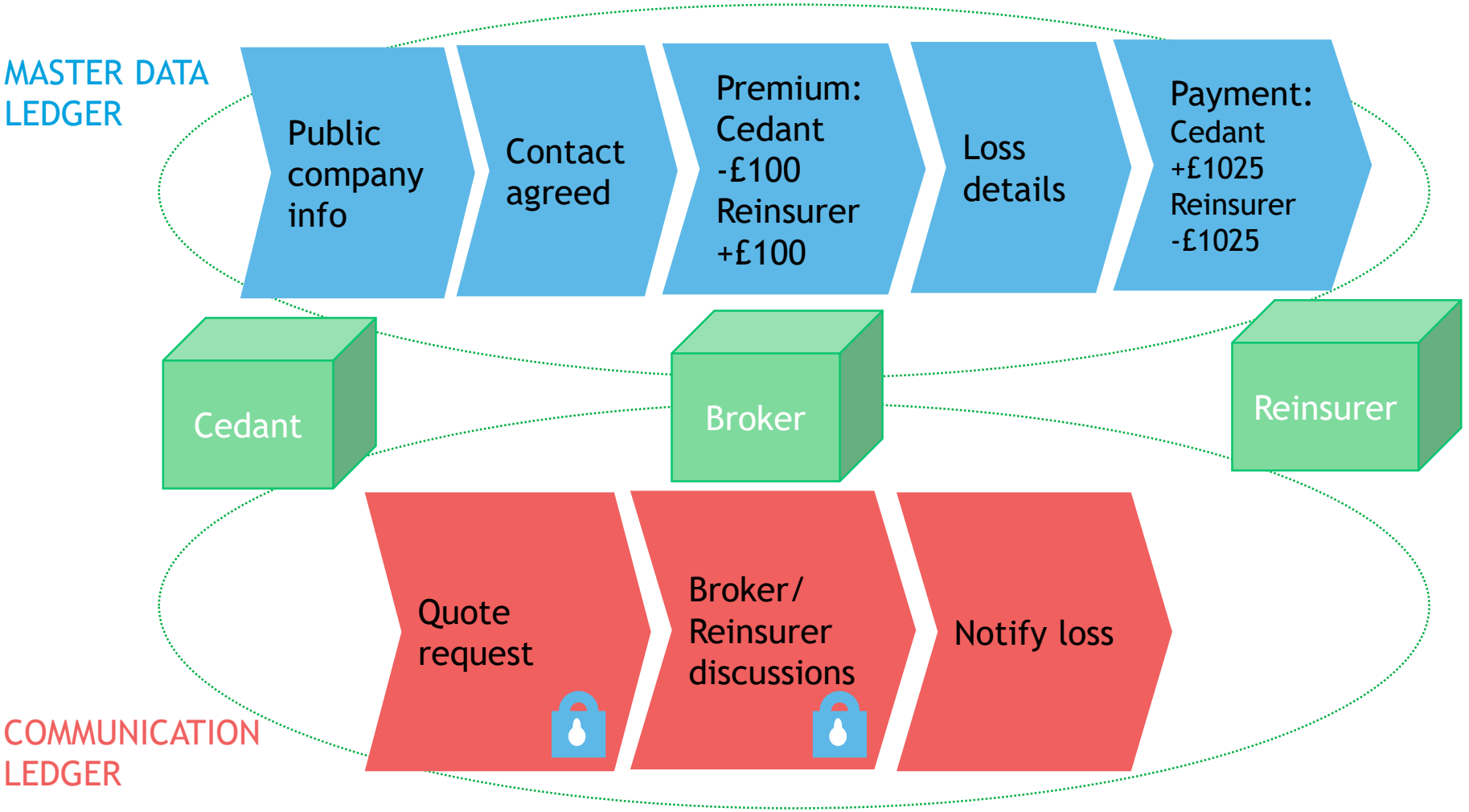
Blockchain Insurance Industry Initiative

- 15 founding members
- Prototype: Property Cat XOL contract
- B3i Services AG incorporated March 2018
- Deployment late 2018



B3i website: https://b3i.tech/about-us.html

B3i



Kennedys

Insurwave

Commercial launch: May 2018

- Developers:
  - EY (Ernst & Young)
  - Guardtime (blockchain developer)
  - Microsoft (Azure cloud)
  - ACORD (data standardization)
- Participants:
  - A.P. Møller-Maersk (shipping firm)
  - Willis Towers Watson
  - XL Catlin
  - MS Amlin

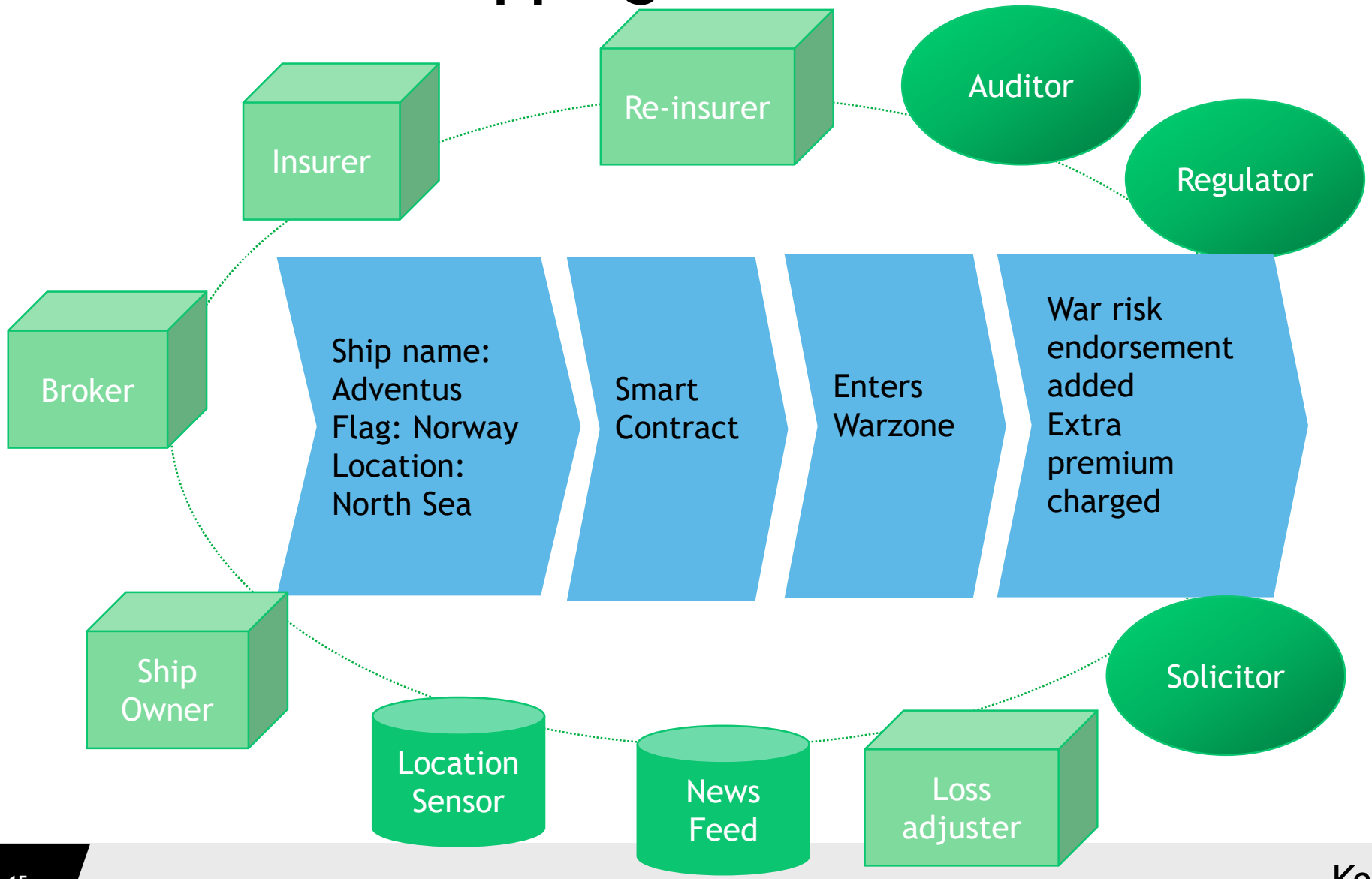
“

Insurwave enables:

- *Claims to be paid in hours, not years*
- *Premiums to be agreed and settled in seconds*
- *Shippers to track assets and share data with brokers and insurers*
- *Brokers to focus more on servicing clients and less on administration*
- *Insurers to track their exposures in near real-time*

”

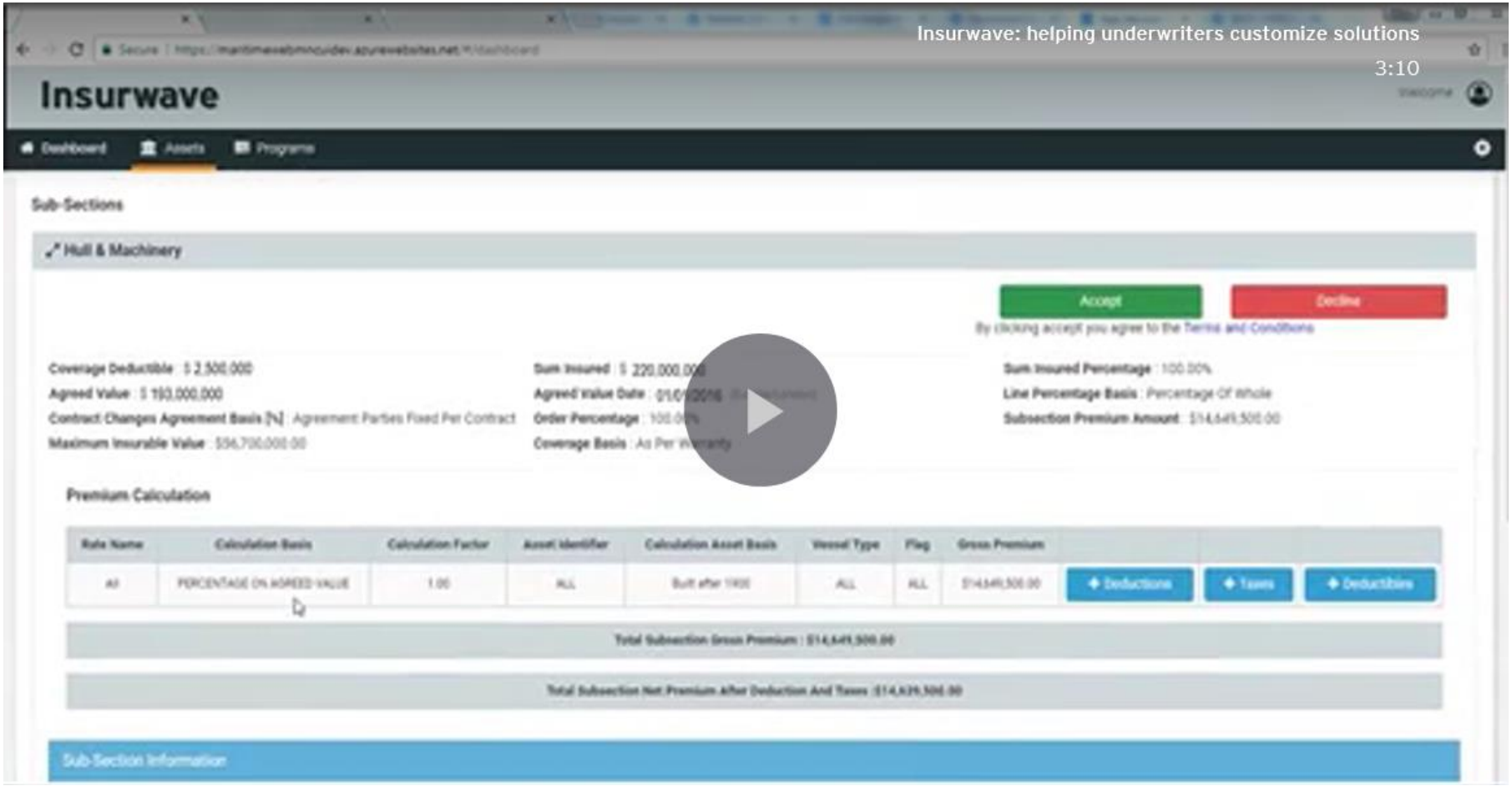
Insurwave: shipping



Kennedys

Insurwave

Underwriter view: live contract endorsements, risk data etc



www.ey.com

Kennedys

THE FUTURE

Kennedys

Benefits

Decentralisation.

There is no central authority required to provide the trust or validation for any transaction. Trust is implied in the network through consensus.

Consensus

Everyone is looking at the same data in real-time on similar, and (perhaps) eventually on the same platform.

Transparency

The blockchain is shared amongst all nodes on the network which all parties being able to able to see the contents of the blocks, ensuring transparency.

Increased speed of decision making

Contracts administered on a ‘smart’ basis often require little, if any, human input in order to be activated. The previous weather example uses ‘index linked’ contracts which are activated on digital notification from an outside data source (an Oracle).

Benefits

Immutability

The ledger is, to all intents and purposes, write only and so the accuracy of any transaction written into the ledger is assumed eradicating uncertainty.

No single point of failure

As the ledger is distributed throughout the network, there is no one single point of weakness. If one node ‘drops’ the rest remain with no break in service.

Trust

The integrity of the ledger is implied through consensus on the Blockchain. This does away with the need for a trusted third party to validate, or ensure, the legitimacy of any transaction or block. This allows for trust relationships between parties where no trusted intermediary may exist to validate the transaction opening up new markets.

Commonality or consensus of terminology

This allows for better data analytics without the need to ‘clean’ or ‘filter’ data prior to analysis and/or reporting.

Disadvantages

Scalability

As more transactions are added to the network, the ability to run a ledger query will take longer and longer as no running ‘balance’ is calculated with each block. A balance search effectively loops through all blocks to calculate a balance at that time.

Speed / Response time

As the rate of transactions out-pace the computational resource, transactions which carry a higher reward payment for mining will become prioritised, leaving a residual backlog of ‘low yield’ transactions.

Space

As the transaction list grows, as does the ledger requiring increasing storage space on each node on the network to maintain the decentralised and distributed nature of the system.

Smart Contracts

As the ledger is immutable, any errors in the contracts are fixed in place. Accordingly, a new contract correcting the error will need to be added but the incorrect contract will remain in place. If there are flaws or vulnerabilities within these contracts, this will be open to exploitation permanently.

The future of Blockchain in insurance

What are Kennedys thinking and doing?

Blockchain claims data integration for fraud detection;
Subrogated recoveries management via claims matching on a shared ledger

What are other people doing or thinking of doing?

Chatbots (Spixii) to improve customer experience;
Peer-to-Peer (P2P) insurance based on pooled groups of insurance types (Friendsurance and So-Sure) which rewards policyholders at the end of the year if no claims are made;
On-Demand insurance (Cover2Go)
Internet of Things (IOT, think FitBit and wearables) based data analysis for claims processing or premium calculations;
Identify verification without the need to repeatedly produce extensive documentation;
Catastrophe swap and bonds based on on/off blockchain P2P agreements;
Automation of claims processing via smart contracts (Flight insurance policies)

QUESTIONS?

Thank you for attending today's seminar

Emily Clift
Insurance Division
Emily.clift@kennedyslaw.com
0121 214 8015

Rob Tanner
Liability Division
Robin.tanner@kennedyslaw.com
0121 214 8045

Kennedys


@KennedysLaw


linkedin.com/company/Kennedys


facebook.com/KennedysTrainees

kennedyslaw.com

Kennedys