Molde University College
Specialized University in Logistics

MANUFACTURING NETWORK 4.0

Blockchain Technology

Bjørn Jæger
Associate professor / Leader of the SCM-IS Research Group
Molde University College

Guest Lecture

- Introduction
- Blockchain Technology: Encryption Principles
- Blockchain applications in Supply Chain

Blockchain

Open, Public, Permission less, Global

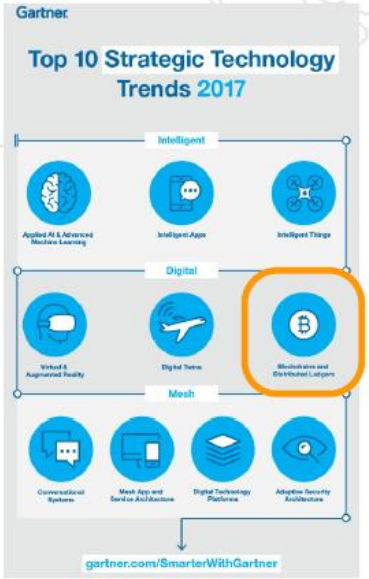
bitcoin

The most secure data network in the World!

100,0 % up-time since Jan 3rd 2009!

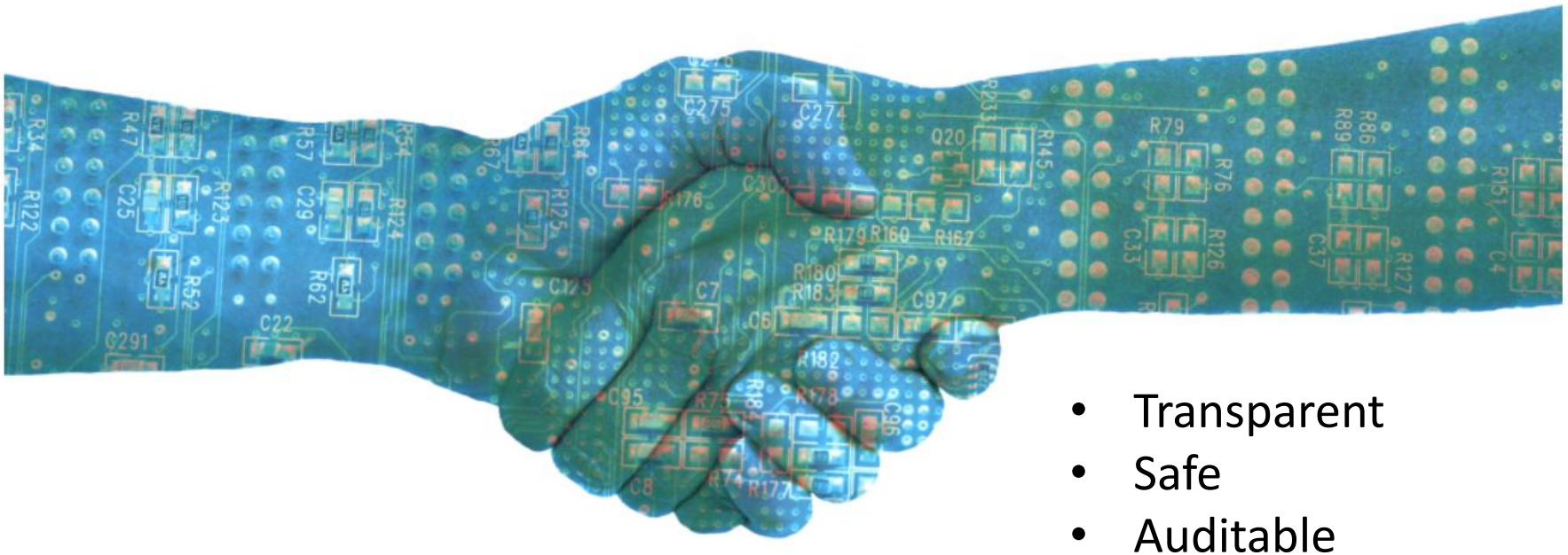
Gartner:

«Blockchain to fundamentally change the society in which we live»



Blockchain

- A distributed ledger technology
- A new way to record and transfer data



- Transparent
- Safe
- Auditable
- Resistant to outages.

Invention: Paper by Nakamoto

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

https://bitcoin.org/bitcoin.pdf

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

https://bitcoin.org/bitcoin.pdf

Example to illustrate

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main

I.e. how money is exchanged without banks

Exchange money via a bank
Initial situation

Bjørn **Deodat** **Student**

Ledger in Bank

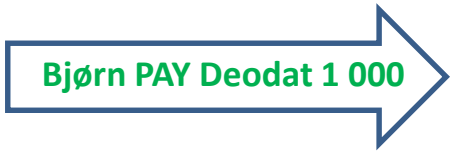
Bjørn Bjørn's bank account 9710 33 2314
Balance: 10 000

Deodat Deodat's bank account 9710 33 2314
Balance: 10 000

Student Student's bank account 9710 33 2314
Balance: 10 000

… Exchange money

Bjørn **Deodat** **Student**



Ledger in Bank updated

Bjørn Bjørn's bank account 9710 33 2314
Balance: 9 000

Deodat Deodat's bank account 9710 33 2314
Balance: 11 000

Student Student's bank account 9710 33 2314
Balance: 10 000

… Exchange money without a bank -- with Blockchain Initial situation

Bjørn

Bjørn's Ledger

Bjørn's Balance: 10 000

Deodat's Balance: 10 000

Student's Balance: 10 000

Deodat

Deodat's Ledger

Bjørn's Balance: 10 000

Deodat's Balance: 10 000

Student's Balance: 10 000

Student

Student's Ledger

Bjørn's Balance: 10 000

Deodat's Balance: 10 000

Student's Balance: 10 000

… Exchange money: No bank involved!

Bjørn

Deodat

Student

The transaction is broadcast to all participants

Bjørn's Ledger

Bjørn's Balance: **9 000**

Deodat's Balance: **11 000**

Student's Balance: 10 000

Deodat's Ledger

Bjørn's Balance: **9 000**

Deodat's Balance: **11 000**

Student's Balance: 10 000

Student's Ledger

Bjørn's Balance: **9 000**

Deodat's Balance: **11 000**

Student's Balance: 10 000

Blockchain = Distributed Ledger

Ledger in Bank

Distributed Ledger among all members of a blockchain

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

https://bitcoin.org/bitcoin.pdf

Hash

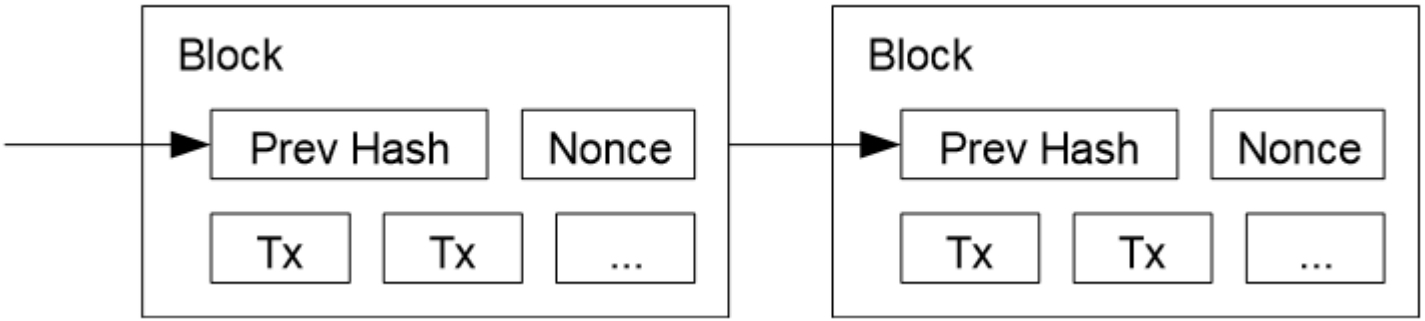
What is a hash?

- It is a function that returns a value of a specific length.
  - So whether the input is "Hi" or "Hello" or "This is an even longer piece of data", the hash function will return the same length of output, and that output will always be the same size, and the output will always be the same for a given input.
- The other aspect of a hash function is that it is "one way".
  - It is very easy to put input into the hash function and get output, but it's basically impossible to get some hash output and determine from that what the input was.

What is a hash?

- It is a function that returns a value of a specific length.
  - So whether the input is "Hi" or "Hello" or "This is an even longer piece of data", the hash function will return the same length of output, and that output will always be the same size, and the output will always be the same for a given input.
- The other aspect of a hash function is that it is "one way".
  - It is very easy to put input into the hash function and get output, but it's basically impossible to get some hash output and determine from that what the input was.

A blockchain
From the paper by Nakamoto



Hash: number representing a block
Nonce: part of timestamp for proof-of-work
Tx: Transactions in a block

A block in a blockchain

Bjørn's Ledger

Bjørn PAY Deodat 1 000

Deodat's Ledger

Transaction, T new:

From Bjørn (Bjørn's Public BankID)

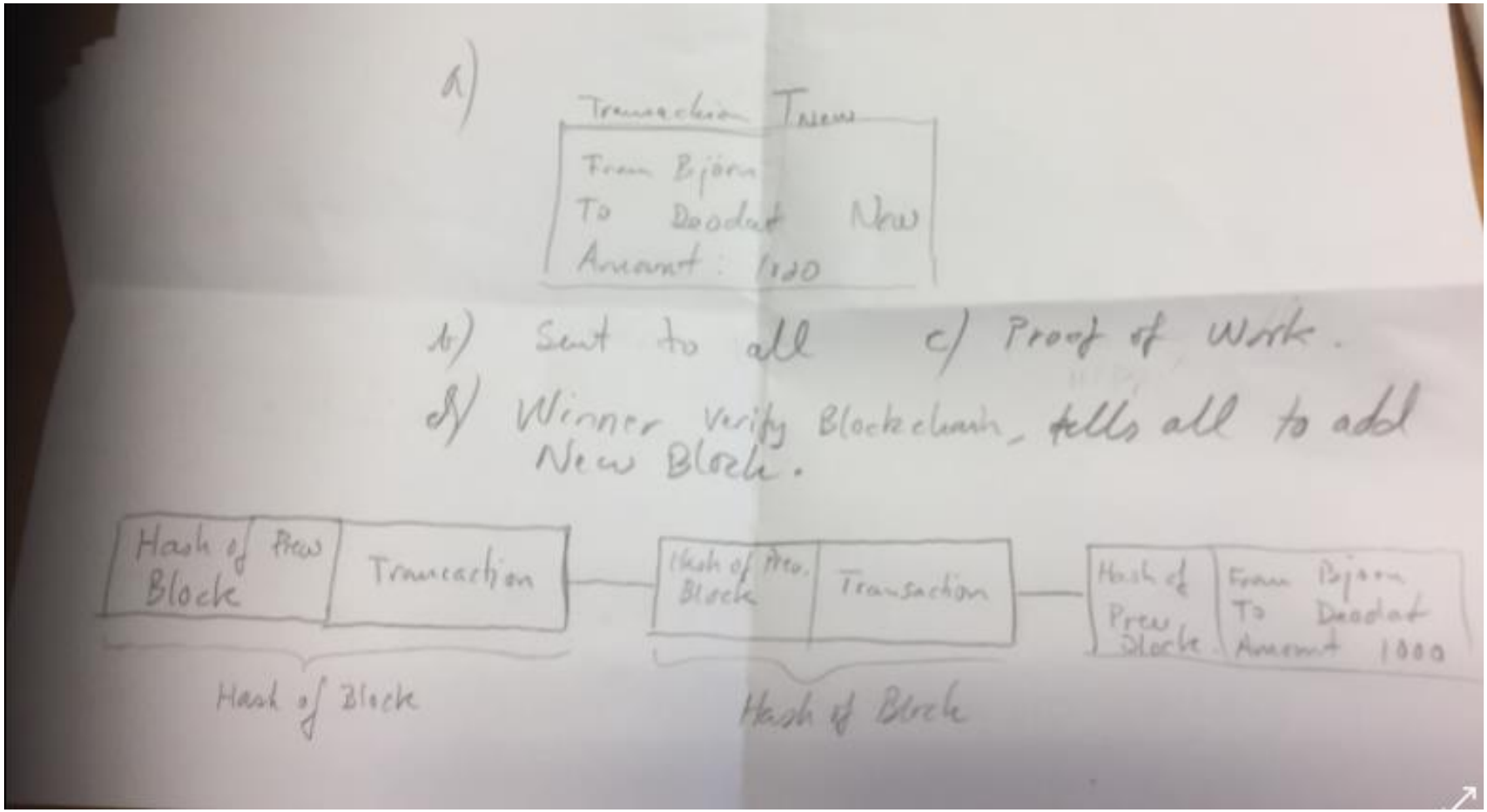
To: Deodat (Deodat's Public BankID)

Amount: 1 000

Draw example on blackboard in class …

a) Transaction
b) Send to all
c) Compete by Proof-of-work
d) Winner verify entire blockchain, tells all to add new block

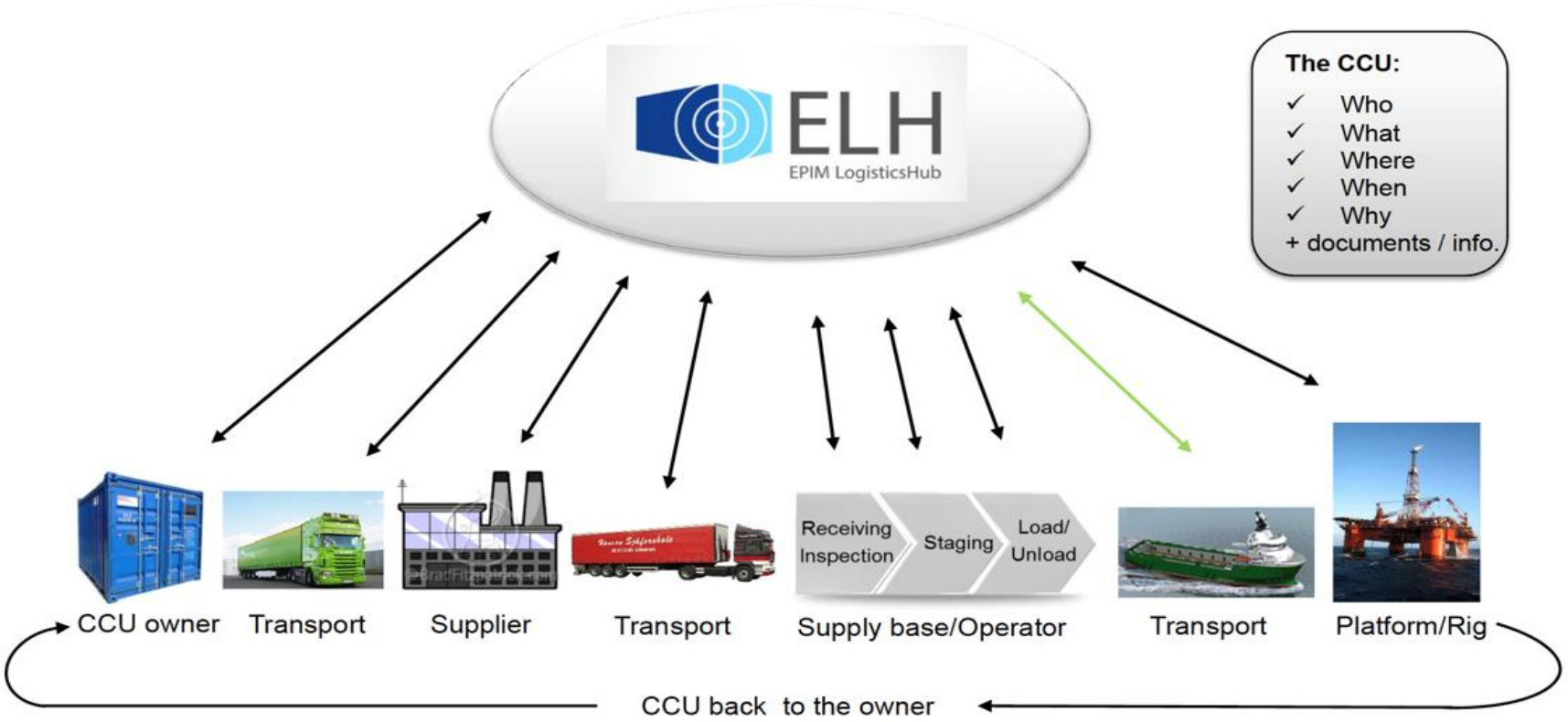
On the boad …


a)
Transaction T NEW
From Björn
To Deodat Nkw
Amount: 1000
b) Sent to all
c) Proof of Work.
d) Winner verify Blockchain, tells all to add New Block.
Hash of Prew Block
Transaction
Hash of Block
Hash of Prev. Block
Transaction
Hash of Block
Hash of Prew Block
From Björn
To Deodat
Amount 1000

Blockchain applications in Supply Chains

Sharing event data in Supply Chains
Traditional way

- Track cargo containers in the supply chain
- LogisticsHub in Oil & Gas (https://epim.no/elh/)
- **All events in ONE DATABASE**

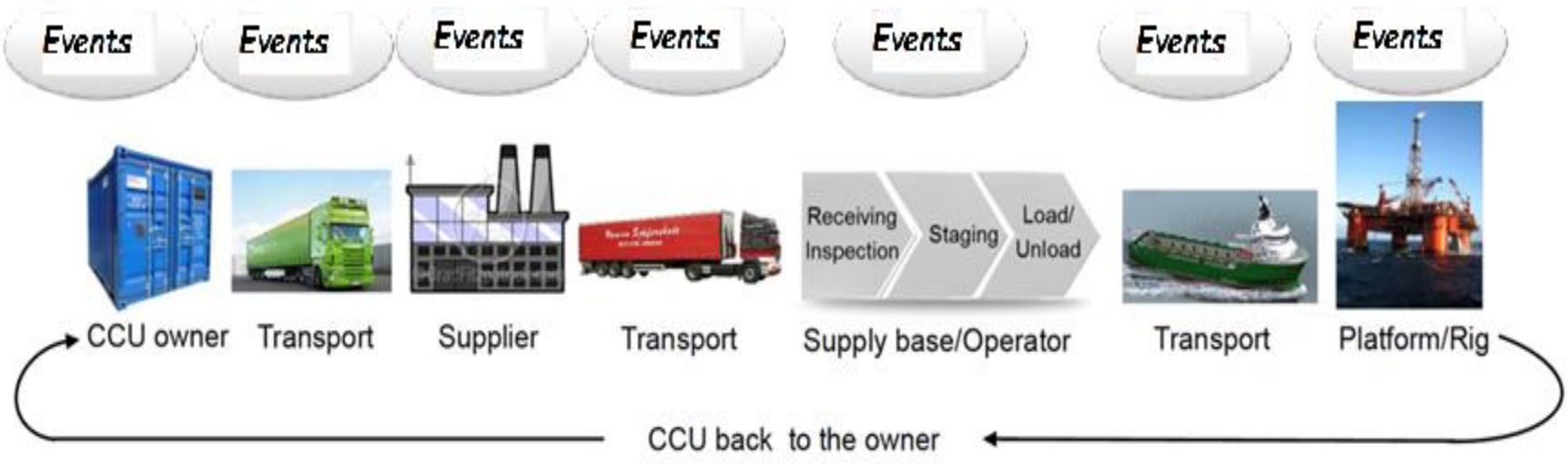


… Sharing event data in Supply Chains

Using a Blockchain

Suggested by researchers Engelenburg et.al

Blockchain with copies of event-log distributed to all members



- **Each company has all the events**
- **Events are encrypted by the company owning the event**
- **The owner send a Decryption Key to the ones with access**

AkerBP

- Aker-BP are testing out Blockchains to get payment if goods are delayed
- Time Received and Time Sent are entered in a blockchain by each actor in the supply chain
- If it is delayed, the one(s) responsible can be charged

Smart Contract Example

- Suppose you rent an apartment from me.
- You can do this through the blockchain by paying in cryptocurrency.
- You get a receipt which is held in our virtual contract;
- I give you the digital entry key which comes to you by a specified date.
- If the key doesn't come on time, the blockchain releases a refund.
- If I send the key before the rental date, the function holds it releasing both the fee and key to you and me respectively when the date arrives.
- The system works on the If-Then premise and is witnessed by hundreds of people, so you can expect a faultless delivery.
- If I give you the key, I'm sure to be paid. If you send a certain amount in bitcoins, you receive the key.
- The document is automatically canceled after the time, and the code cannot be interfered by either of us without the other knowing since all participants are simultaneously alerted.

Thank You!