SATURN 2018

14th Annual SEI Architecture Technology User Network Conference

MAY 7–10, 2018 | PLANO, TEXAS

Blockchain is the answer – What was the question again?

Harald Wesenberg

Specialist IT

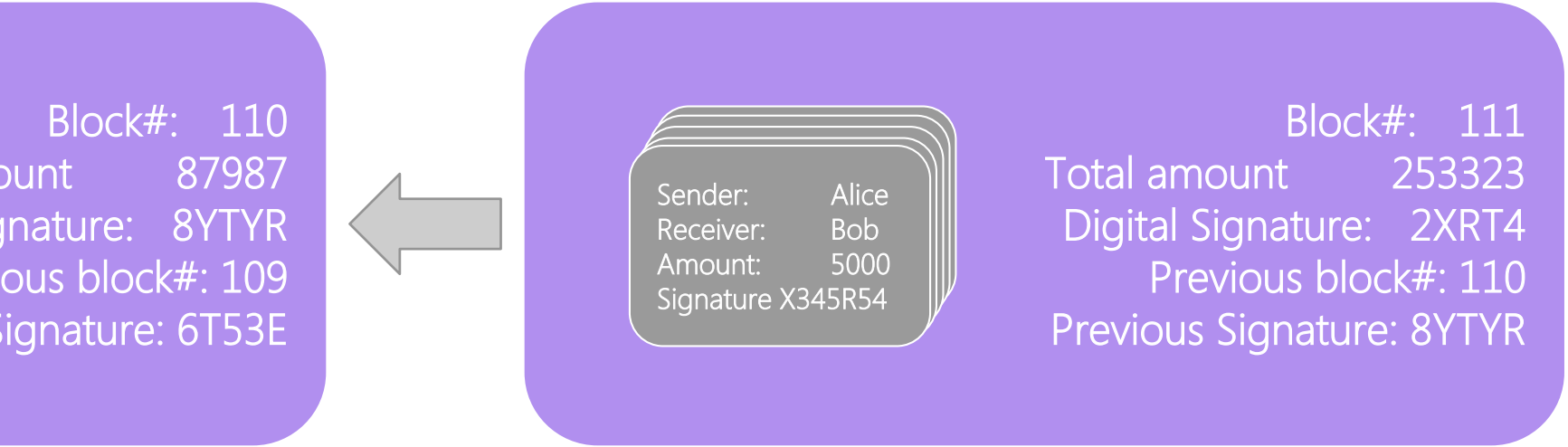
Statoil

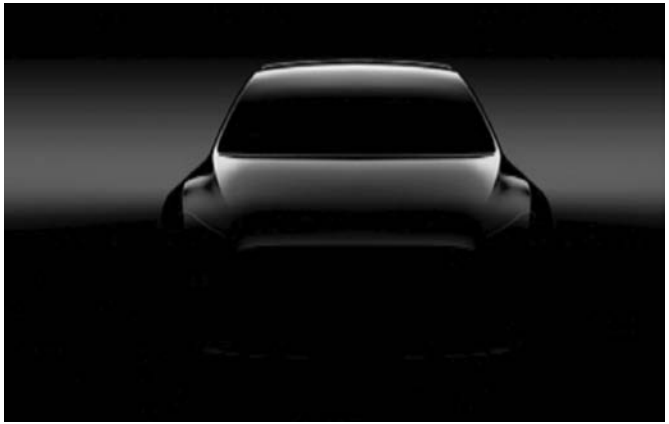
Bitcoin

Digital currency and wallet
Started in 2009
Directly between users
No "central bank"

Blockchain creates trust between unknown parties without the use of intermediaries or central authorities

A chain of **transactions** grouped into **blocks**



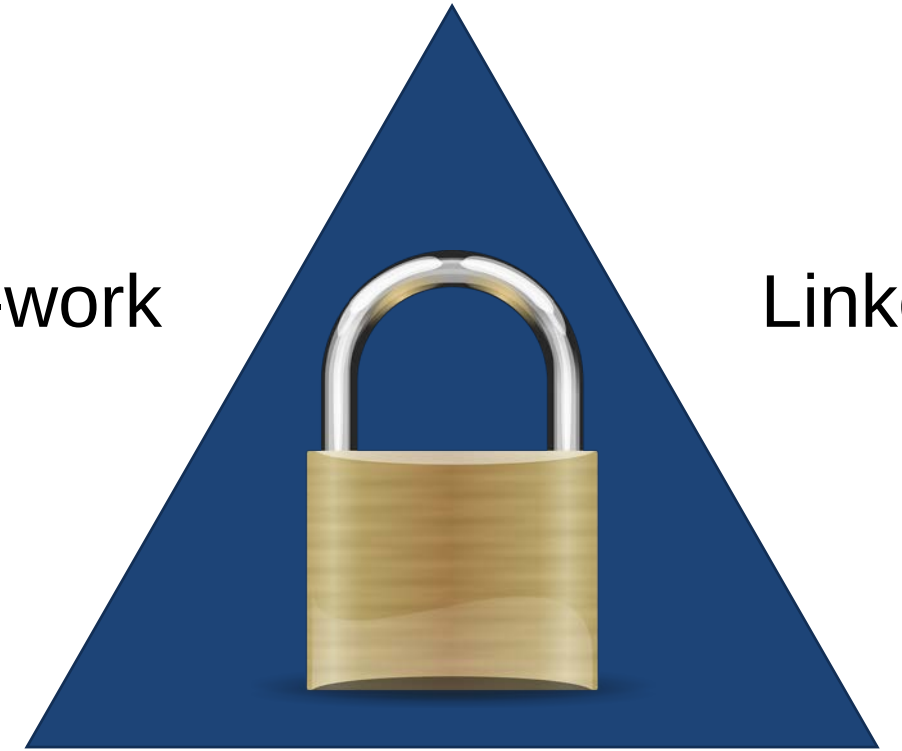


What they promise

100 years

What they can deliver

Proof-of-work



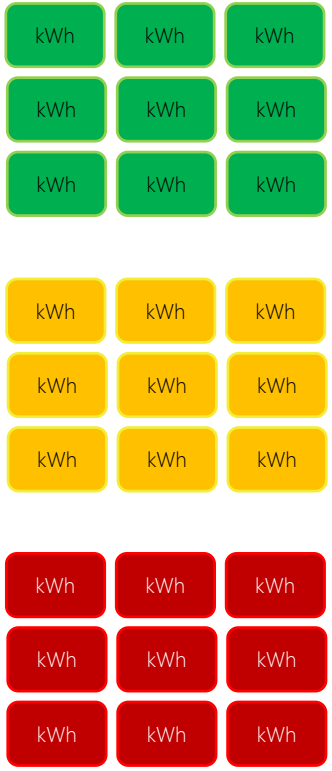
Linked chain

Consensus

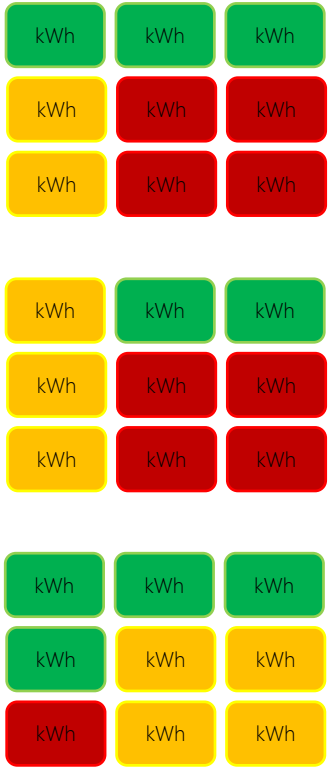
Blockchain is the answer – what was the question again?

Usage in the energy industry

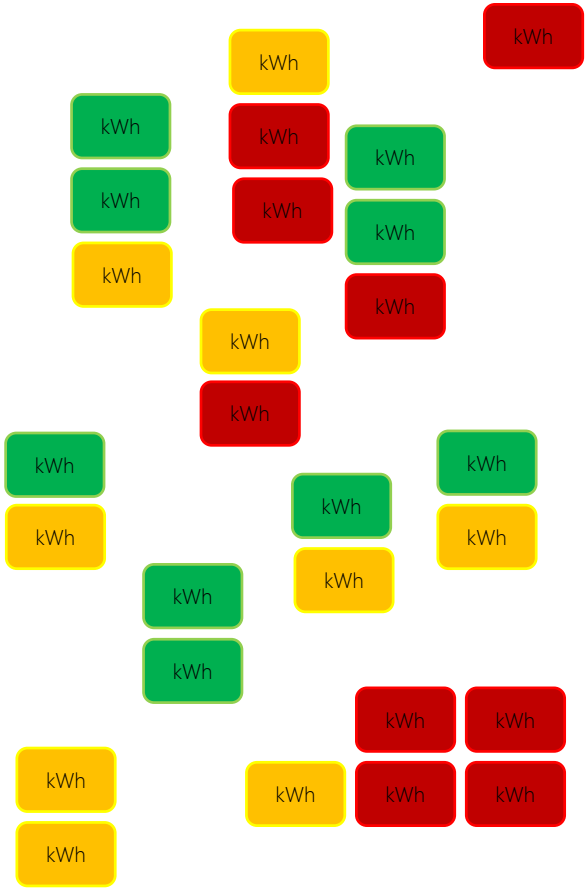
Certificate of origin



Production

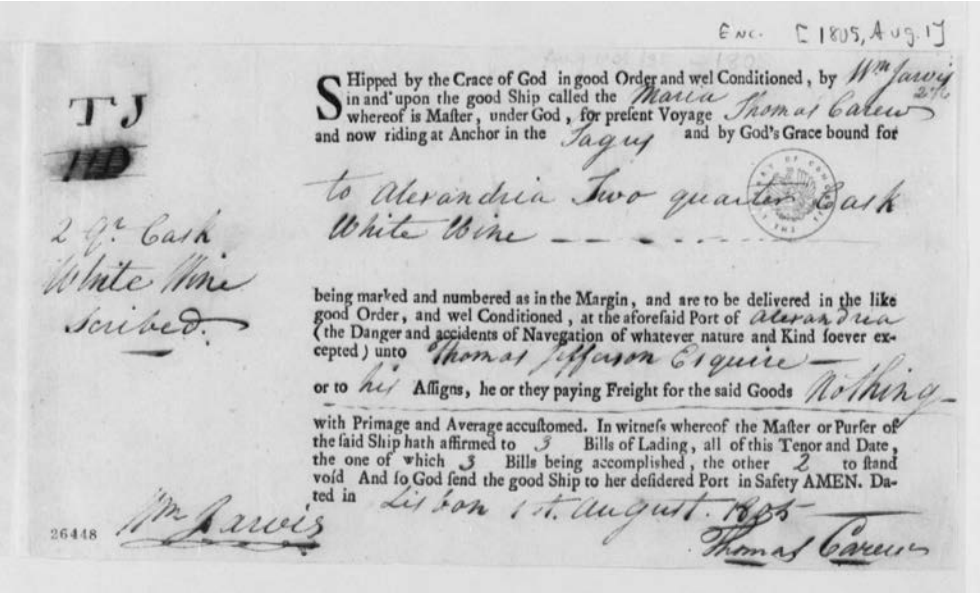


Transmission



Consumption

Oil cargo ownership



ENC. C 1805, Aug. 17

TJ

2 Qr. Cask White Wine Scribed.

SHipped by the Grace of God in good Order and wel Conditioned, by Wm Jarvis &c. in and upon the good Ship called the Maria Thomas Carew whereof is Master, under God, for present Voyage and now riding at Anchor in the Tagus and by God's Grace bound for to Alexandria Two quarter Cask White Wine

being marked and numbered as in the Margin, and are to be delivered in the like good Order, and wel Conditioned, at the aforesaid Port of Alexandria (the Danger and accidents of Navegation of whatever nature and Kind soever excepted) unto Thomas Jefferson Esquire or to his Assigns, he or they paying Freight for the said Goods Nothing with Primage and Average accustomed. In witness whereof the Master or Purser of the said Ship hath affirmed to 3 Bills of Lading, all of this Tenor and Date, the one of which 3 Bills being accomplished, the other 2 to stand void And so God send the good Ship to her desidered Port in Safety AMEN. Dated in Lisbon 1st. August 1805

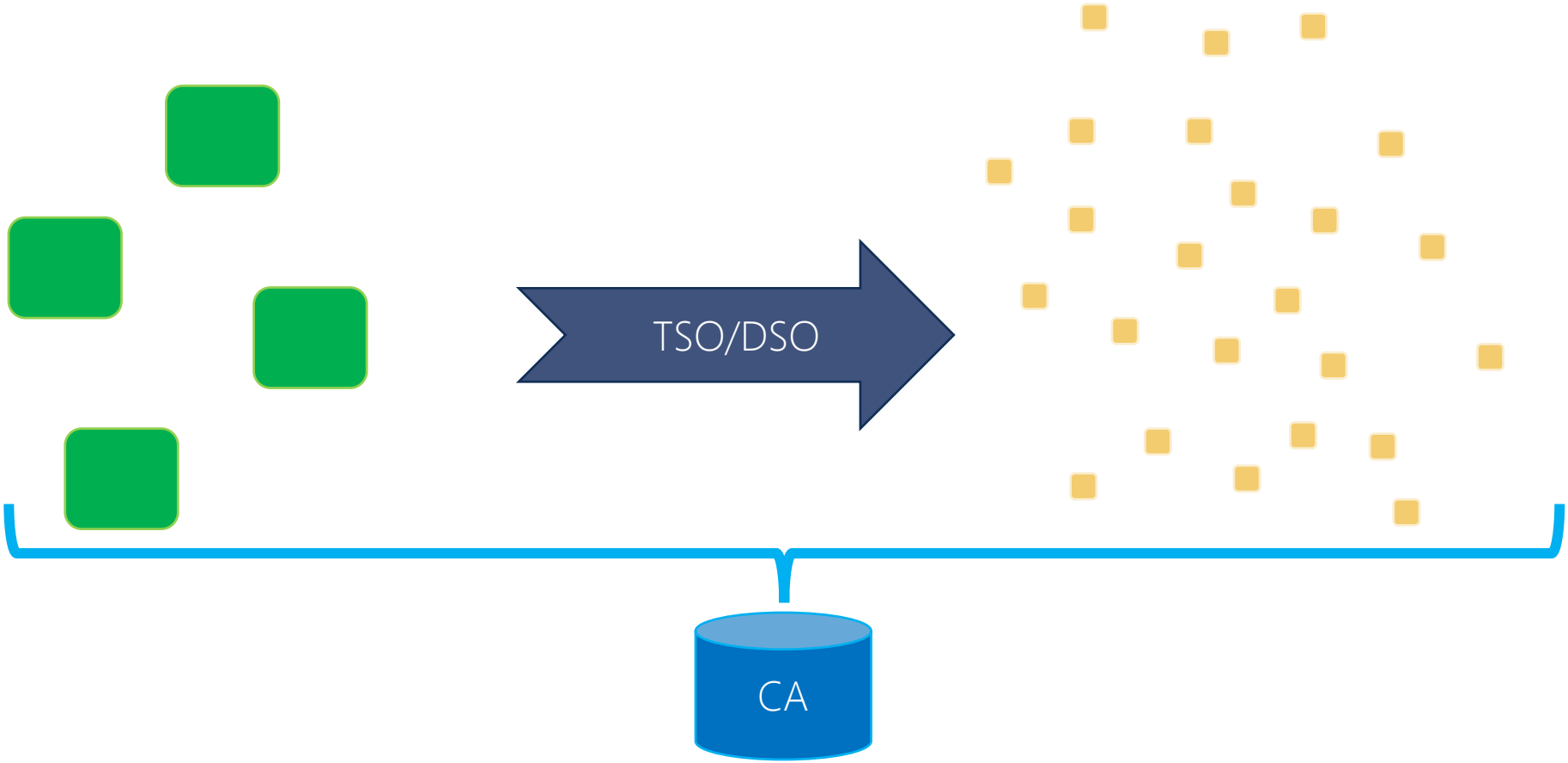
26448 Wm Jarvis

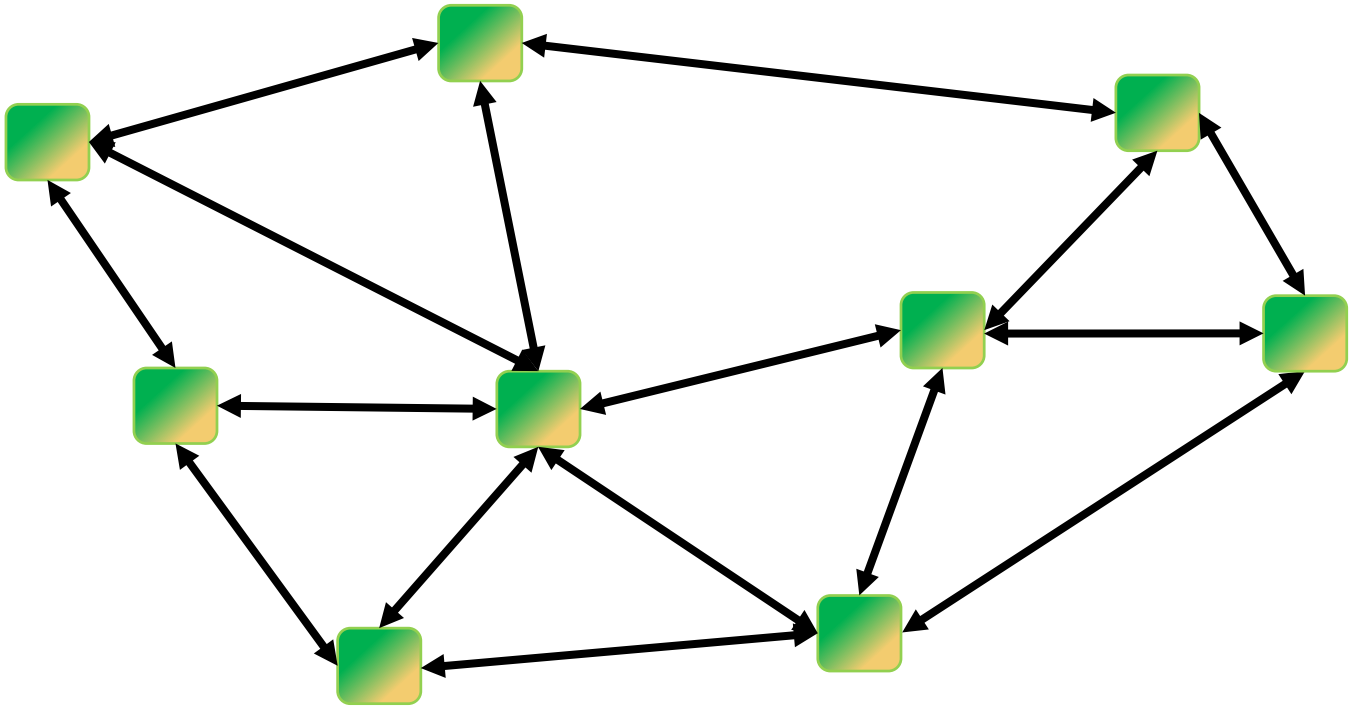
Thomas Carew

Bill of lading

Holder owns cargo
Physical document shipped around the world
Avoids double spending – maintain chain of ownership
Cumbersome and expensive

The machine network





Blockchain is the answer - what was the question again?

Evaluating blockchain proposals

1. Trusted transactions
2. Transparency
3. Central authority
4. Non-repudiation
5. Smart contracts/behavior
6. Timing and performance

1. What is the trusted transaction?

Blockchains are in its essence based around trusted transactions. Identifying the underlying trusted transactions is key in evaluating blockchain suitability.

a. **Very suitable**: Transaction chains between multiple counterparties that can be represented as financial transactions using cryptocurrencies and crypto wallets. E.g. certificates of origination
b. **Very suitable**: Information exchange chains between multiple counterparties where the information can be digitally signed, e.g. bills of lading
c. **Somewhat suitable**: One-sided publications of information on events

2. What is the transparency?

Blockchains are built to be transparent as part of the trust model.

a. **Very suitable**: Transactions that are public
b. **Somewhat suitable**: Transactions that are private, but where a digital representation (hash) of the transaction can be made public
c. **Not suitable**: Transactions where neither information itself, or knowledge of the existence of the transaction can be made public

3. Use of central authority

Blockchains are built to provide trust without a central authority.

a. **Very suitable**: Transactions where the central authority today is not fully trusted
b. **Very suitable**: Transactions where the use of a central authority is costly, time consuming or cumbersome
c. **Not suitable**: Transactions where the removal of the central authority does not provide any added value

4. Non-repudiation

Blockchains are built to provide trust by enforcing non-repudiation.

a. **Very suitable**: Transactions where we worry about counterparties repudiating their prior transactions
b. **Very suitable**: Publication of information where we need to be prove that a transaction happened at a given time and with a given content
c. **Not suitable**: Transactions where we neither worry about repudiation or proving the timing of a transactions

5. Smart contracts

Blockchains have the ability to add behavior using code. The code and resulting behavior poses a serious security risk, and must be evaluated carefully against security vulnerabilities.

a. **Very suitable:** Transactions with simple behavior using a handful of transaction states in a closed graph based on open source code
b. **Somewhat suitable**: Transactions with semi-complex behavior or simple transactions with behavior based on proprietary/closed source code
c. **Not suitable**: Transactions with complex behavior or non-simple transactions based on proprietary/closed source code

6. Timing/performance

Blockchain is (currently) based on complicated consensus algorithms that takes time and effort to complete. This means that there is a delay from a transaction is published until it is verified, as well as a delay on the number of transactions per second. Currently the delay is about one hour with a restriction of 7-15 transactions/second in most major blockchain implementations.

a. **Very suitable:** Long running transactions with low volume with no requirements for immediate verification
b. **Not suitable**: Transactions with high volume (>5 transactions/sec) or where immediate verifications is required.

Q&A