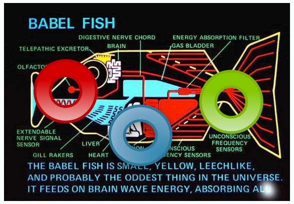
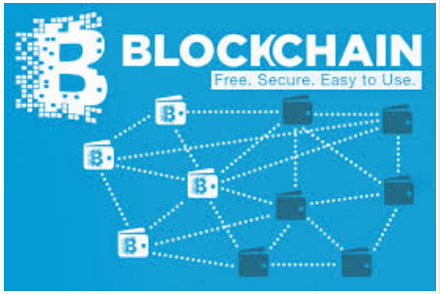

BABEL FISH
DIGESTIVE NERVE CHORD
ENERGY ABSORPTION FILTER
TELEPATHIC EXCRETOR
BRAIN
GAS BLADDER
OLFACTO
EXTENDABLE NERVE SIGNAL SENSOR
LIVER
GILL RAKERS
HEART
NSCIOUS
ENCY SENSORS
UNCONSCIOUS FREQUENCY SENSORS
THE BABEL FISH IS SMALL, YELLOW, LEECHLIKE,
AND PROBABLY THE ODDEST THING IN THE UNIVERSE.
IT FEEDS ON BRAIN WAVE ENERGY, ABSORBING ALL

IoT Babelchain
-
Proof of Understanding



How Machines learn to communicate

Benedikt Herudek (benedikt.herudek@gmail.com)
April2016
Linux Foundation
Open IoT

Abstract

- Having Machines talk to each other is of specific interest for the Internet of Things with the number of different devices and protocols

- This presentation suggests to solve this Problem (in IoT often referred to as the ‘Baskets of Remotes’ Problem) by following the Consensus Approach Bitcoin and Blockchain Technologies take:
  - Participants in a distributed Network can ’translate’ messages from one to another protocol with the help of Machine Learning Algorithms
  - Successful Translators will receive awards in a cryptocurrency like Miners in a Bitcoin Network get rewards for Executing Proof of Work
  - (partially) replace a Bitcoin Proof of Work by a proposed Consensus Mechanism Proof of Understanding

- The resulting System will:
  - translate Messages from different protocols into each other
  - arrange publicly verifiable agreements about these Translations on a Blockchain

- An open question is if we the resulting Blockchain will have the same string immutability feature as the Bitcoin Blockchain

Agenda

- The Problem: Disparate Protocols and Machine cant communciate
- Bitcoin versus ‘classical’ Integration Approach
- Bitcoin Blockchain Consensus approach applied to IoT Protocol Integration Problems
- Proof of Understanding
  - Format Handshake
  - Content Handshake
  - Action Handshake
- Translator Machine Learning (Mining Hash Power)
- Implementing Proof of Understanding
  - Smart Contract
  - Pre-req for Bitcoin Proof of Work
  - Replacing Proof of Work
- Proof of Understanding and the Blockchain Immutability Feature
- Comparing Bitcoin Blockchain and Proof of Understanding Blockchain (‘Babelchain’)
- Once again: What we claim & Why it all matters …

Machines can't (hardly) communicate !

The IoT Version

- Devices have different message Formats but need to be able to communicate, e.g. The iPhone needs to be able to take over from all remote controls and talk to the Samsung TV
- Devices can get connected via Software Solution in a centralized or distributed Cloud Solution
- Problem is increasing with number of devices and exposure to the end users who will not like large enterprises be able to account for the Integration effort between disparate protocols

The Enterprise Integration Version

- Consider the case of a CRM and Billing System and a Provisioning System in a Telecommunications enterprise.
  - Client order are taken in with the CRM Sy
  - stem, the order is send to the Provisioning System, The Billing System will be responsible to generate a bill to the
  - All three Systems (in fact there are many more) know the concept of a Client and of Products, but they have different ways of talking about them and their internal Data Models differ.

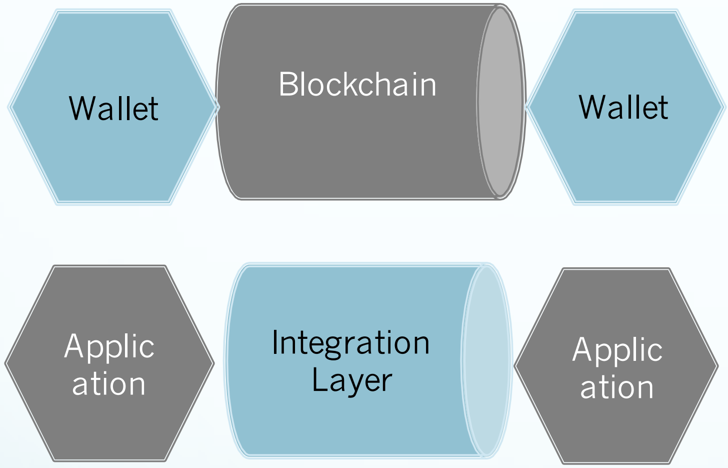
The 'Broken Trusted Middle Man' Solution

Suggest an Industry Standard or follow a Standard set by a large player
But:

- Large players dont stick to industry standards
- With the number of usecases, applications and devices, innovations and the globalized character of the internet industry standards are impossible to keep up

The ‘naïve’ way of copying Bitcoins Approach to integrate Endpoints

Bitcoin is able to integrate endpoints (wallets, miners) in a large distrubuted network seemlessly without any integration effort



Blockchain:

- Transactions (Blockchain) are **permanent** & **primary**
- Enpoints (Wallets) are **derived** & **ephemeral**

Conventional Systems

- Transactions (EBS) are **derived** & **ephemeral**
- Enpoints (Applications) are **permanent** & **primary**

- Following Bitcoin would mean to create a standard for handling transactions
- Even though Existing Systems often do not keep Transactions but the end points permanent, they use a similar approach
  - existing SOA Style (Microservices, API Industry) follow the same pattern in dictating a message exchange format.
  - often, these are Industry, Technollgy Vendor or Enterprise Standards

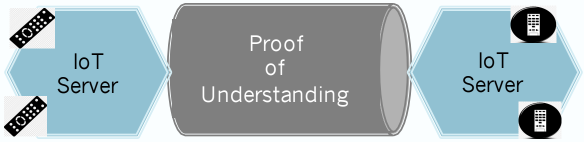
What can we learn from Bitcoin and Blockchains?

Bitcoin

How can machines securely come to an agreement about the status of transactions without resorting to a trusted third party ?

Internet of Things

How can machines come to an agreement about the meaning of a message without resorting to a trusted third party ?



IoT Server

Proof of Understanding

IoT Server

Miner's Hashing Power

Computing Power
Use the CPU power of a large distributed System

Predictive Machine Learning Capabilities

Rewards for Hashing Blockheaders

Incentives
Cryptocurrency reward chance on fulfilling certain

Rewards for Translating Messages

Immutable Transactions

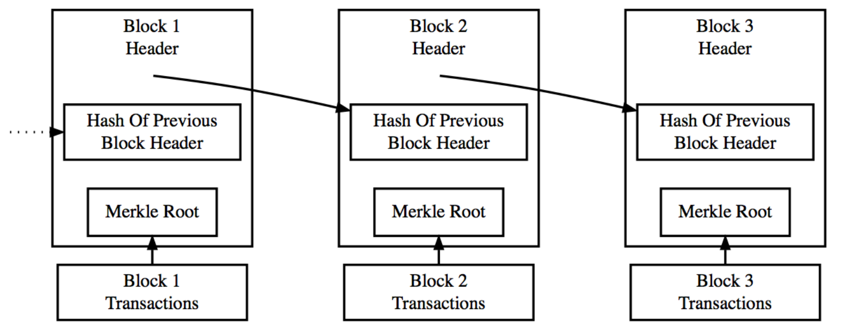
Consensus
Establish Consensus in a distributed (unmuteable) System

Common Language

Economics
Avoid the costs of a Centralized Datacenter, use a shared, distributed 'hardware' largely self organizing System

Proof of Work: create a shared & immutable bitcoin transaction ledger

- The “**previous block hash**” field is **inside** the **block header**
- When the parent is modified in any way (eg fraud), the parent’s hash changes and hence the child hash changes and so on
- The **cascade effect** would require that much computing power that deeper layers are practically **immutable**



Simplified Bitcoin Block Chain

With courtesy from the bitcoin book of Andreas Antonopoulos and documentation from bitcoin.org

4.Independent **selection**, by every node, of the chain with **the most cumulative computation demonstrated through proof of work**

Mining & Feeds align Miner’s (financial) with Network (immutable transaction ledger) interest

1.Independent **verification** of each **transaction**, by every full node, based on a comprehensive list of criteria

Mining via ‘ hash puzzles’

- process of hashing the block header repeatedly, changing one parameter (‘nonce’) , until the resulting hash matches a specific target
- The hash function's result cannot be determined in advance, nor can a pattern be created that will produce a specific hash value
- Hence, the only way to produce a hash result matching a specific target is to randomly modifying the input until the desired hash result appears by chance.

3.Independent **verification** of the new **blocks** by every node and assembly into a chain

2. Independent **aggregation** of transactions into new blocks by mining nodes, coupled with **demonstrated computation through a proof of work algorithm**

This is reminiscent of a common distinction in linguistics of syntax, semantics and pragmatics

‘Meaning’ for Machines: Syntax, Semantic, Pragmatics

Meaning is defined as a key value pair of **Format** & **Content** potentially triggering an **Action**:

Message **Format** like file with fields, XML messages, csv files, binary files

```
<body>
     <device> ...<device>
     <command> ...
             </command>
    <channel>  .</value>

  </body>
```

There are variable slots in which values with **Content** will go

TV
change
channel
12

Action in the real world or a digital form (photo, fingerprint of a machine state)

It can be verified by **humans** or **advanced machine algorithms**

Examples:

- (Digital fingerprint of) changed state in TV
- (picture of) Temperature measuring room on 20 degree

```
<ZAP_TV>

   <to>
    <receiver>TV in my chinese hotel
      room</receiver>
      <path> TV Cloud Server</path>
  </to>
  <from>
    <sender>my smart phone remote app
    </sender>
    <path> smart  phone Cloud Server</path>
  </from>
```

```
<body>
     <device> TV <device>
     <command>  change channel
             </command>
    <channel> 12</value>

  </body>
 </ ZAP_TV >
```

Format Handshake

There is an assumption here a Translator can make format suggestions ! Hang on a couple of slides !

Sender

1. A sender creates a message with content (key value pairs in potentially a hierarchical structure) and sends it to the Receiver

```
…
<device> TV<device>
    <command> change channel
          </command>
   <channel> 12</value>
…
```

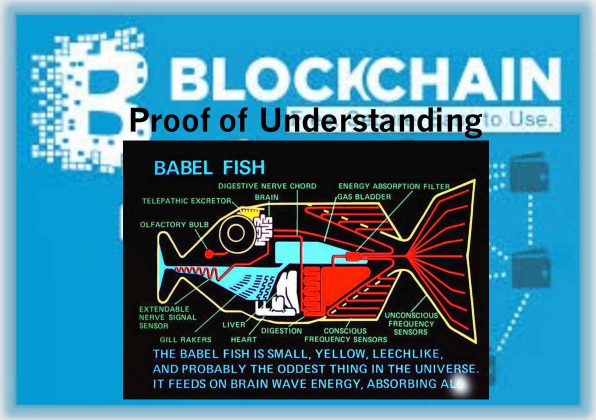
4. Sender & Receiver pick one message formats they 'believe' they would be able to understand.

Repeat Format Handshake

Failure

3. Translators offer different data formats and offer those to sender and receiver

```
…
<thing> … <thing>
    <action > …
          </action>
   <what_action>
… </what_action>
…
```


BLOCKCHAIN
to Use.
BABEL FISH
DIGESTIVE NERVE CHORD
ENERGY ABSORPTION FILTER
TELEPATHIC EXCRETOR
BRAIN
GAS BLADDER
OLFACTORY BULB
EXTENDABLE NERVE SIGNAL SENSOR
LIVER
DIGESTION
CONSCIOUS FREQUENCY SENSORS
UNCONSCIOUS FREQUENCY SENSORS
GILL RAKERS
HEART
THE BABEL FISH IS SMALL, YELLOW, LEECHLIKE, AND PROBABLY THE ODDEST THING IN THE UNIVERSE. IT FEEDS ON BRAIN WAVE ENERGY, ABSORBING ALL

Proof of Understanding

5. The Translator that generated the format that is first picked by both sender and receiver is marked for the part of the reward for the format translation.

Agreed Format

Receiver

2. Unless the Receiver ('believes to') understand the message, the message gets offered to the Babelchain Translators with a bounty

```
…
<device> TV<device>
    <command> change channel
          </command>
   <channel> 12</value>
…
```

4. Sender & Receiver pick one message formats they 'believe' they would be able to understand.

Success

Action Handshake

Content Handshake

See this as a confirmation that
the agreed message format is
understood by both in the same way

Sender:

3. The Sender will have to agree to the solution, if he doesn’t another message format has to be found and the format handshake round of the quiz will have to start

4. If Sender and Receiver agree on the correct assignment, then whoever of the Translators offered the correct solution will get marked for the Content part of the reward..

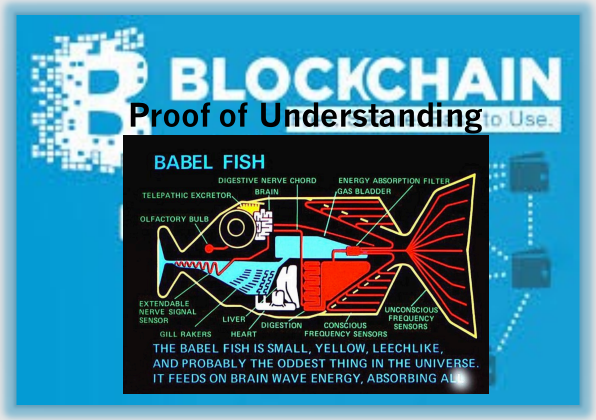
Repeat
Format Handshake

Failure

Content Hand-shake

1. Translators will compile all possible combinations of value assignments to the format.

```
...
<thing> TV<thing>
      <action > change channel
                 </action>
     <what_action>
12</what_action>
...
```


BLOCKCHAIN
to Use.
BABEL FISH
DIGESTIVE NERVE CHORD
ENERGY ABSORPTION FILTER
TELEPATHIC EXCRETOR
BRAIN
GAS BLADDER
OLFACTORY BULB
EXTENDABLE NERVE SIGNAL SENSOR
LIVER
DIGESTION
CONSCIOUS FREQUENCY SENSORS
UNCONSCIOUS FREQUENCY SENSORS
GILL RAKERS
HEART
THE BABEL FISH IS SMALL, YELLOW, LEECHLIKE,
AND PROBABLY THE ODDEST THING IN THE UNIVERSE.
IT FEEDS ON BRAIN WAVE ENERGY, ABSORBING ALL

Proof of Understanding

5. If no Action Handshake is mandated, rewards will get paid out

```
...
<thing> TV<thing>
      <action > change
channel
                 </action>
      <what_action>
12</what_action>
...
```

Agreed Content for Format

Receiver:

2. The Receiver will pick the combination, that ‘works for him’

4. If Sender and Receiver agree on the correct assignment, then whoever of the Translators offered the correct solution will get marked for the Content part of the reward..

Success

Transaction / Action Handshake (optionally)

Action Handshake

See this is a test, that there really was no misunderstanding during format & content handshake Humans could do it, if simple and we good, we automate it

Sender:

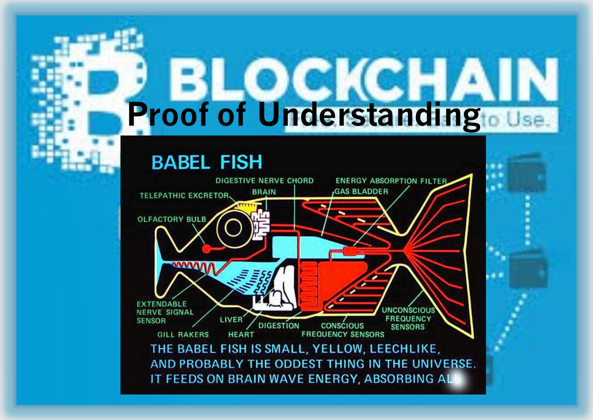
2. Receiver upon his or Senders initiative has to offer evidence of the action. Digital picture of a If the handshake is confirmed

Repeat Format / Content Handshake

Failure

Action Hand-shake

1.Sender or Receiver can choose to open this round before continuing.



Proof of Understanding

THE BABEL FISH IS SMALL, YELLOW, LEECHLIKE, AND PROBABLY THE ODDEST THING IN THE UNIVERSE. IT FEEDS ON BRAIN WAVE ENERGY, ABSORBING ALL

3.Evidence will be checked by machines or humans

4. Rewards will get paid to Systems marked during the Format and Content

Agreed Action on Content for Format

Receiver

- Actions handshake can reconfirm the format & Content Handshake but can be time-consuming (if humans check) or difficult for machines to undertake.
- It can typically be useful 1st time two systems handshake and messages can trigger significant and sensitive actions, like opening a banksafe or launching a rocket
- Choosing for this handshake wil depend on probability to fail (determined by sender or receiver) and the risk implied upon a misunderstanding

Success

Transaction

Machine learning algorithms (eg swiftspear) can create shakespeare sonnets when fed with existing one's

Translator

We can predict (something as profane, but nevertheless important) as machine message

- The Babelchain Data structure has to be designed such that it offers a **training set** of **success-** and **unsuccessful handshakes** with all relevant **features**
- Over such a training set Translators can create a **supervised logical or probabilistic regression learning algorithm** trying to **predict** message formats, contents. Participants typically would feed their Translators with all kinds of xml, csv and other technology and industry message exchange standards
- There needs to be a proper **balance** between what is made **public** on the blockchain to allow the network to learn and what successful Translators keep **private** for themselves
- **Translating will get easier**, hence Translators will need to receive other rewards eg for infrastructure services like delivering messages within time, similar to the bitcoin shift from miners benefiting from Mining rewards towards transaction fees

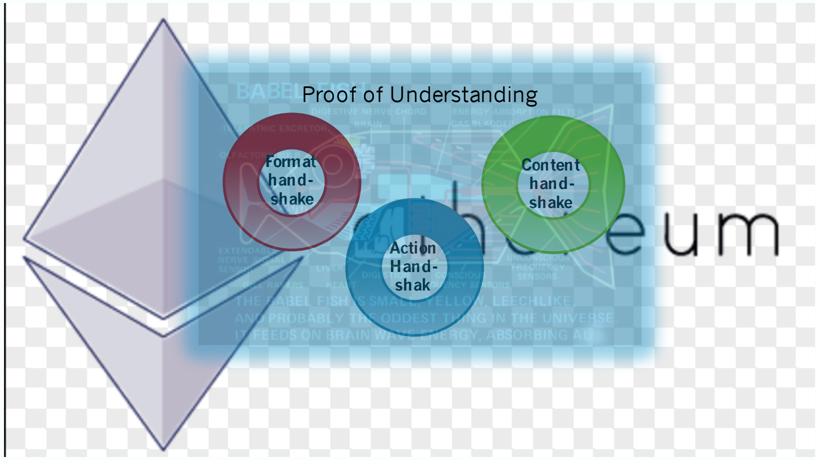
Message	Location Start Signal	Identity Sender	Identity Receiver	Feature n	S ACK Format	R ACK Format	S ACK Content	R ACK Content	S ACK Action	R ACK Action	Format Handshake	Content Handshake	Action Handshake
… <device> TV<device> <command> change channel </command> <channel> 12</value> …	Hotel, front of TV	GUEST	TV Hotel	…	yes	yes	yes	yes	yes	yes	<<device>>; <<command>>;<<value_command>>	TELEVISION; ADJUST_CHANNEL;12	-
… <device> Themostat<device> <command> adjust temparaturechannel </command> <channel> 20</value> …	Hotel, front of thermostat	GUEST	Thermostat Hotel	…	yes	no	-	-	-	-	THERMOSTAT; ADJUST_CHANNEL;12		
… safe; OPEN …	Hotel, front of sage	UNKNOWN	Safe Hotel	…	?	?					?		

Implementing Proof of Understanding

	Description	Energy Waste	Goods & Bads
Smart Contract	• write out a competition, a **bounty smart contract** • where anyone solving the translation task will get a cryptocurrency award like ethereum paid out	**High**: • as high as the hosting blockchain e.g. ethereum • No smart reuse of the work translators do	+ Ideal for prototyping - Low scalability
Prereq for Proof of Work	• whoever generated a valid proof of understanding (there can be several) can start the proof of work • **Hashing puzzle and finding a nonce will include the agreed message, hence proof of work can be started only after proof of understanding** • Agreed Message will be signed by sender and receiver, so anyone in the network can check	**Smarter, not lower:** • Machine work will be used for a useful task • Combined work overall would be similar to bitcoin blockchain	+ Re-use proven Bitcoin approach to make the Blockchain immuteable + high scalability - Energy consumption and waste as high as Bitcoin ***- To be clarified, how the effort of proof of understanding can be measured and how proof of work difficulty target could be adjusted dynamically***
Replace Proof of Work	• In any **transaction system** between connected parties **having a common terminology is a pre req** to make useful transactions. • With the size and amounts of usecases in IoT the **‘one agreed transactio data format’ strategy of Bitcoin will not be feasible.**	**Smarter and lower:** • Machine work will be used for a useful task • Effort for Translation will decrease with the learning effect	+ high scalability + use of machine work to cover 2 goals: translation & immutability - ***To be clarified how Blockchain Immutability will be achieved, even more with learning effect and decreased work*** - ***Potentially smart combination of machine work with consent sender & receiver to message reverts***

Proof of Understanding as a Smart Contract

Bob



Alice

Approach: write out a competition, a bounty smart contract, where anyone solving the task will get ethereum paid out

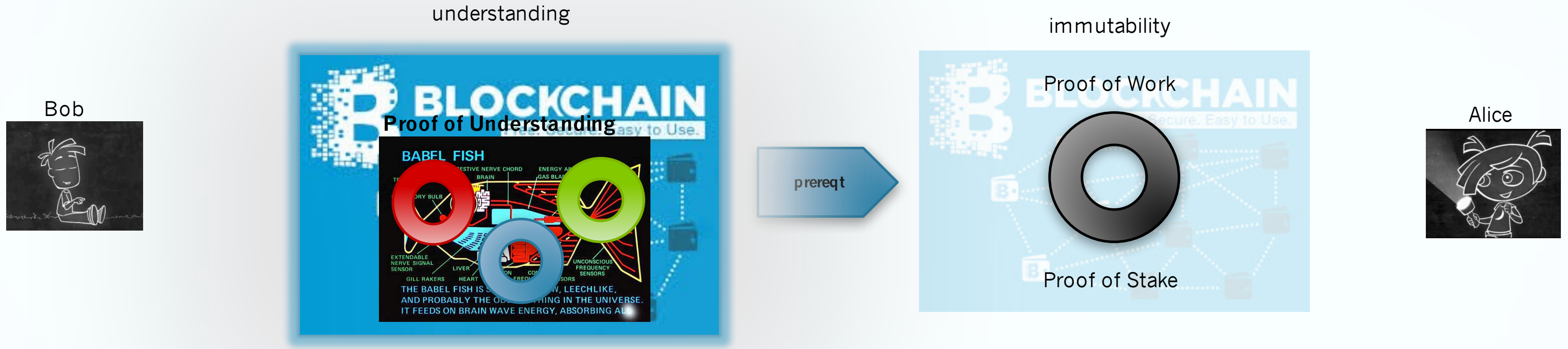
Questions:

- Does a general purpose Blockchain like ethereum scale to the IoT size?
- Could a Proof of Understanding ‘help’ creating consensus eg instead of Proof of Stake ?
- Can a smart contract serve as a prototyping platform ?

Github pseudocode: https://github.com/Benudek/babelchain/blob/master/proofofunderstanding

Ethereum Solidity compiler: http://chriseth.github.io/browser-solidity/

Proof of Understanding as prereq for existing Proof of X Mechanims



understanding

immutability

Bob

Proof of Understanding

prereqt

Proof of Work

Proof of Stake

Alice

BLOCKCHAIN
BABEL FISH
THE BABEL FISH IS SMALL, YELLOW, LEECHLIKE,
AND PROBABLY THE ODDEST THING IN THE UNIVERSE.
IT FEEDS ON BRAIN WAVE ENERGY, ABSORBING ALL

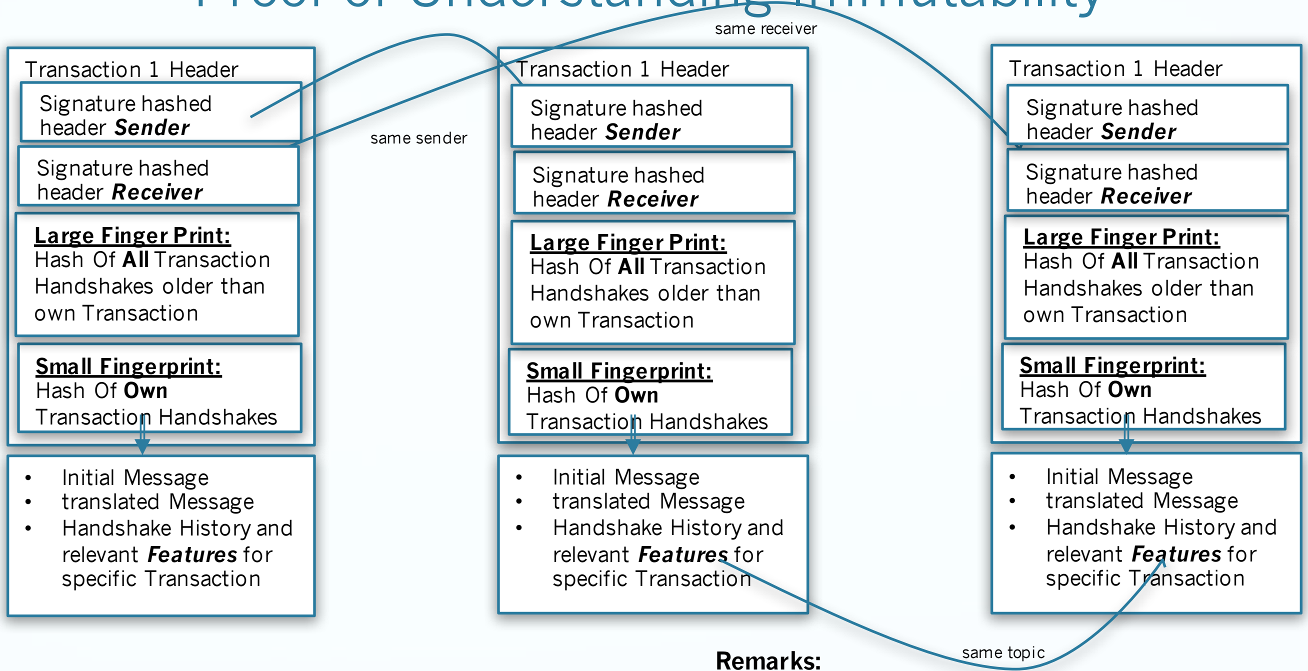
Combine with ‘**Proof of Work**’ style:

- have Translator not only find Translations but also hash them against a difficult target
  - Proof of Understanding Message will be signed by sender and receiver
  - Only who generated a valid proof of understanding can start the proof of work,
  - fingerprint of the agreed message is part of the blockheader for which to find a nonce to meet the difficulty target
- Revising a handshake will require re-do of computationally expensive Hash – against – difficulty - targets like in bitcoin

Combine with **Reputation**, **Trustability** and ‘**Proof of Stake**’ Systems:

- Have not only sender and receiver agree to handshakes but have also other ‘trustable’ network members like eg very successful **Translators sign and approve translations**
- **Trustability** or **Reputation** is defined via the amount of **currency won** as it indicates that a member is very knowledgeable about correct Translations
- Members additionally **holding a large amount of the cryptocurrency** hold a **financial stake** in the network and have interest to avoid fraud

Proof of Understanding Immutability



Transaction 1 Header

Signature hashed header ***Sender***

Signature hashed header ***Receiver***

Large Finger Print:
Hash Of **All** Transaction Handshakes older than own Transaction

Small Fingerprint:
Hash Of **Own** Transaction Handshakes

- Initial Message
- translated Message
- Handshake History and relevant ***Features*** for specific Transaction

Transaction 1 Header

Signature hashed header ***Sender***

Signature hashed header ***Receiver***

Large Finger Print:
Hash Of **All** Transaction Handshakes older than own Transaction

Small Fingerprint:
Hash Of **Own** Transaction Handshakes

- Initial Message
- translated Message
- Handshake History and relevant ***Features*** for specific Transaction

Transaction 1 Header

Signature hashed header ***Sender***

Signature hashed header ***Receiver***

Large Finger Print:
Hash Of **All** Transaction Handshakes older than own Transaction

Small Fingerprint:
Hash Of **Own** Transaction Handshakes

- Initial Message
- translated Message
- Handshake History and relevant ***Features*** for specific Transaction

Cascade Effect :

A Blockchain representing 'Conversations' between Senders & Receivers would take:

- **small fingerprint**: hash fingerprints of their own Handshake Negotiations
- **large fingerprint**: Handshake Negotiation history existing at the time of their handshake

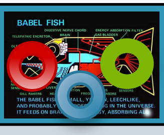
Changing a transaction, handshake will trigger:

- **weak immutability**:
  - Re-do **translation** work, unless same format / content / action accepted
  - Re-ask **consent** from senders and receivers if handshakes are adjusted
  - Header needs to get **hashed**, optionally against a difficulty target
- **strong immutability:** Change of Handshake will change the Large Fingerprint of all younger Transactions
  - Re-do **all translation** work, unless same format / content / action accepted
  - **all those Senders Receivers** will need to sign the Header again
  - **All their Headers** need to get hashed, optionally against a difficulty target

Remarks:

- Usage of a hash **against a difficulty target** can be necessary to rule out the possibility that (all affected) sender & (all affected) senders conspire to revert transactions on expense of a 3rd party affected in the real world but not part of the digital transaction
- The larger the network, the less likely it is all will 'cheat'. Usage of a hash against a difficulty target can therefore be useful especially in the **network startup phase** when the network is small and the cascade effect hence neglectable
- Note **neither** Blocks of Transactions **nor Transactions** (C pays B) **depend** on previous Transactions (B pays A)
- There is an **indirect link** via the **history of handshakes** (the training set), which can be used to create a cascade effect (see below)
- Transactions in a Blockchain representing Conversations between Machines are **loosely coupled** along ***Senders*** & ***Receivers*** or ***topics*** (training set ***features***) like in a social network

Comparing Proof of Work and Proof of Understanding

	Bitcoin Proof of Work	Babelchain Proof of Understanding 
Purpose	Create an unmuteable Blockchain for Financial Transactions	Create common message formats to allows machines to communicate
Quiz	Find a value for the nonce that results in a block header hash that is less than the difficulty target	Find a format (content, Action) which sender and receiver approve
Deterministic	Yes, for any input (arbitraty length) egSHA 256 will produce always the same fixed length output	No, sender and receiver could agree on different formats for the same messages asked on different times as long as they both believe the format will work for them
Predictable timeframe	Yes, statistically	*For many messages probably yesy statistically, but there will be non-translatable messages*
Can it fail ?	Statistically not	Yes, sender and receiver could never reach an agreed message format (content / action)
Money supply	decreasing	constant, never ending
Hard to find solutions	Yes, depending on difficulty target	Case by Case. Will generally get easier with the learning effect of the network. There can always be very hard or untranslatable messges.
Easy to verify solution	Yes, feature of hash function	Yes, sender & receiver have to agree and sign the message, which can be verified
Quiz Difficulty adjusting over time	no	Yes, network learning effect implies that translation will get easier. There can always be very hard or untranslatable messages.
Difficulty of winning reward	Increasing (money supply decreasing and quiz difficuty unchanged)	*Decreasing (learning effect and constant money supply). This raises the question, how to reward Transators for (too) easy translations over time*
Payer	Mining Reward: Bitcoin network Transaction Fee: the Sender of Bitcoin	Translation Reward: Sender (try claiming part from Receiver) Transaction Fee: Sender (try claiming part from Receiver)
Cheating possible	no	Yes, senders and receiver might pass on more features outside the network to preferred translators
Immutability	Yes	'weak immutability' per default as sender and receiver need to agree to changes 'strong immutability' depending on either combination with existing proof of work / proof of stake or smart usage of training sets to cause a

Why ?

- **Computers are 'no good' at understanding concepts** and translating them into each other. This is a problem in many areas of IT like Cloud API's, Enterprise Integration
- With the **size of IoT** and the exposure of devices to normal consumers (Baskets of Remotes) the problem will get larger

Why **Blockchains**?

- Bitcoin shows us that **Transactions** can get safely handled **without any central 'trusted Middle man'** solutions
- Blockchains promise **economical advantages** for large volume, long living, low margin devices over centralized cloud solutions

Why **Proof of Understanding** ?

- Any **Transaction System** has to solve the question of a **common data format** either by **enforcing** (Bitcoin and e.g. most Integrations patterns like SOA and alikes) or **negotiating** (Babelchain)
- Proof of Understanding can make more **efficient usage of Machine work** by (partially) replacing Proof of Work, while keeping the Blockchain unmutability feature

Why **not some Middleware ?**

- **Middleware & ESB's** are **permissioned** with Identity & Access Management. They typically have a centralized data exchange format
- Blockchains with Consensus Mechanisms can be **permissionless** (open & distributed) and **negotiate Message Exchange Formats**.