ValidityLabs

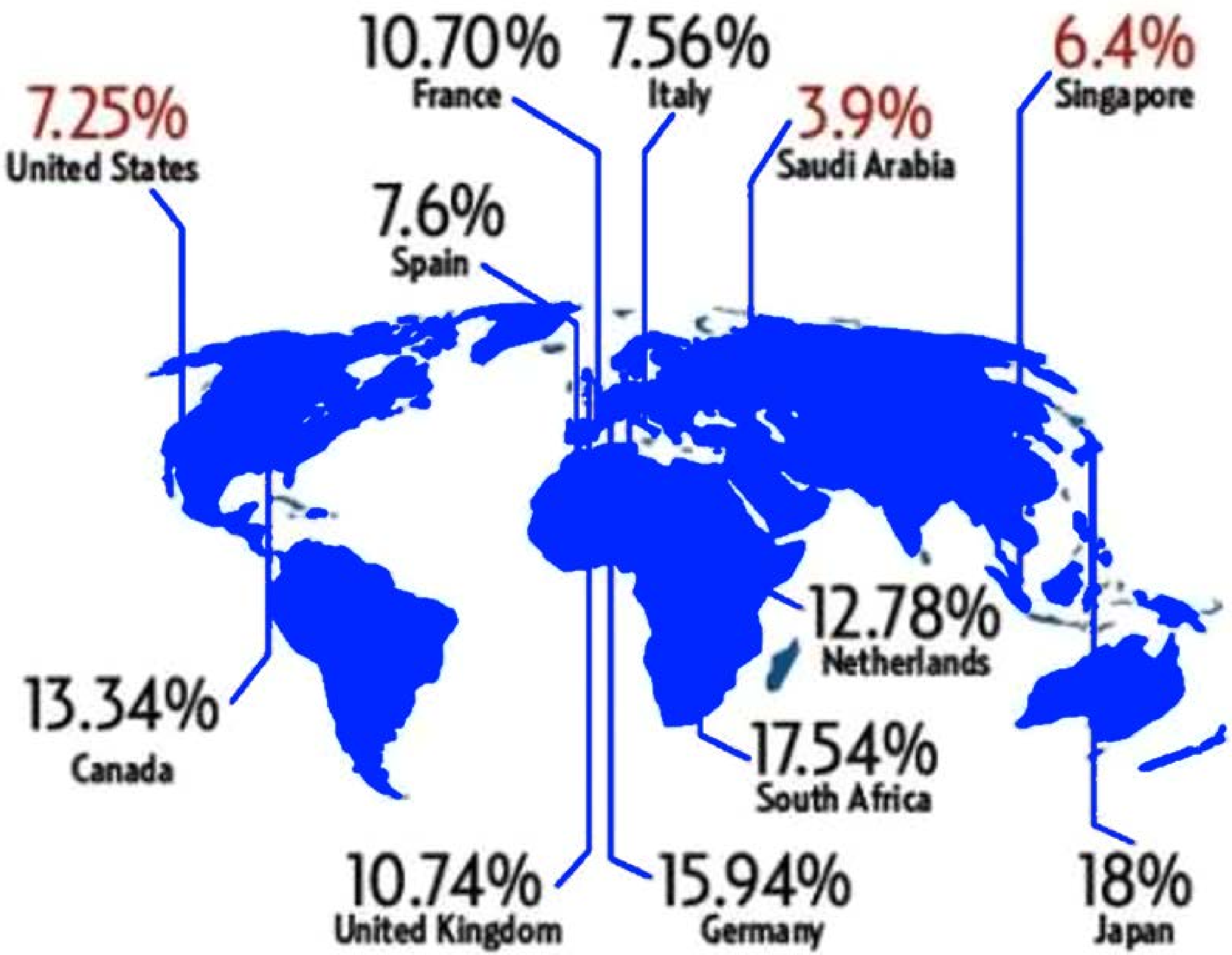
Blockchain & Smart Contracts

Introduction

Dr. Sebastian Bĉrgel

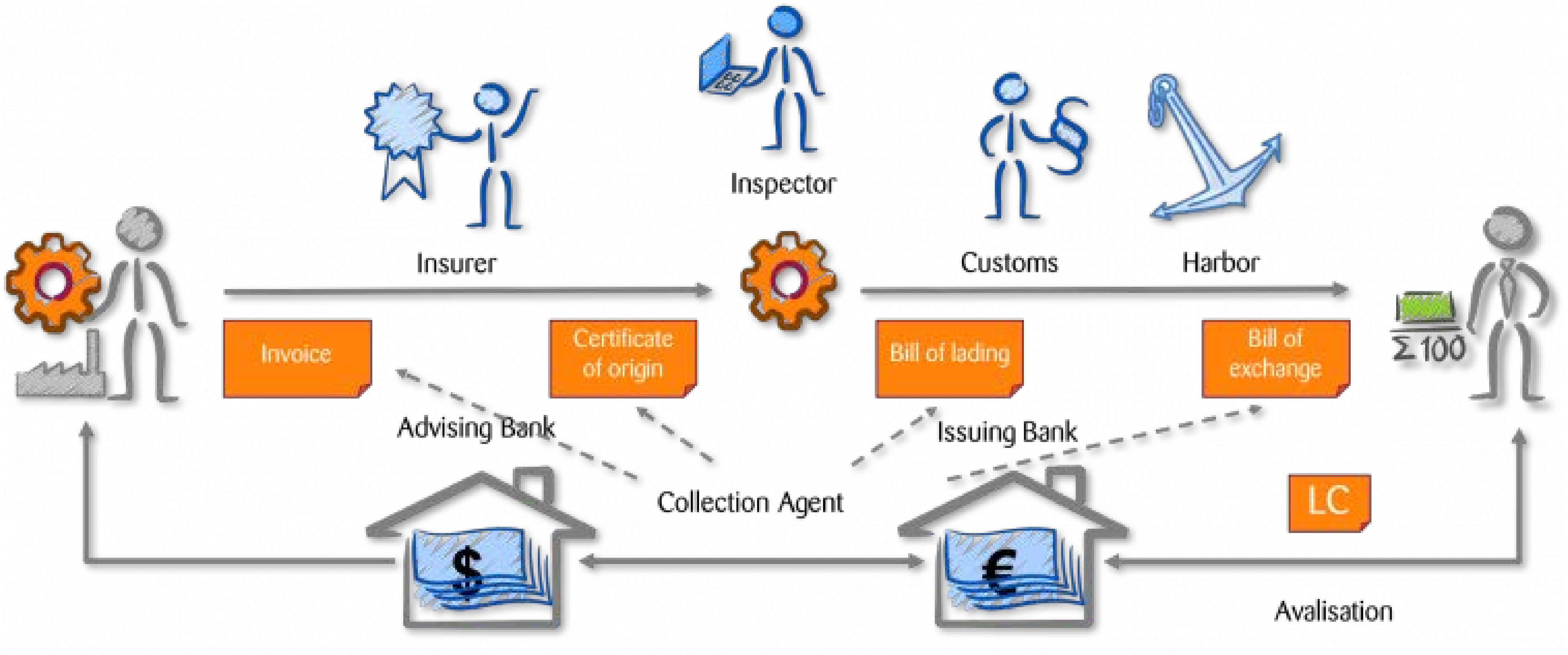
Does the following make sense…?

The remittance costs per $200 dollars sent from



ValidityLabs

State-of-the-Art Trade Finance (2017)



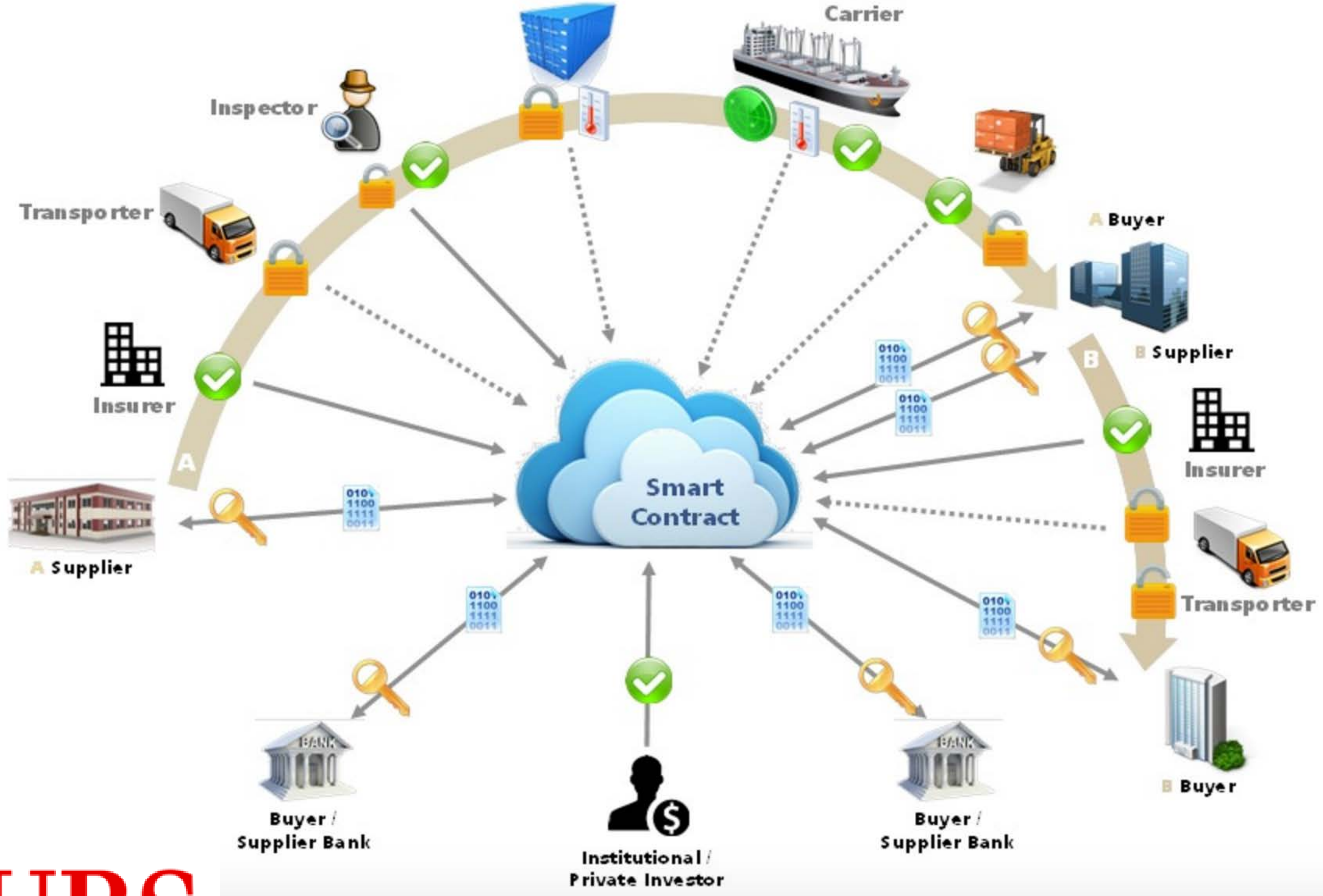
ValidityLabs

zühlke empowering ideas

http://blog.zuehlke.com/en/how-the-blockchain-can-disrupt-trade-finance/

a letter of credit can weigh 500 grams and comprise 36 documents

Beat Bannwart, UBS



UBS Project «Batavia», SIBOS 2016, Geneva

Neue Zürcher Zeitung

Märkte und Meinungen

Bitcoin ist als Währung Unsinn

Virtuelle Währungen

Die mediale Euphorie zieht die Betrüger an

Digitale Revolution

Blockchain – das überschätzte Wesen

Kryptowährungen

Bitcoin-Märchen ohne Happy End?

Bitcoin-Unfälle

Der Mythos «virtuelle Währung» bröckelt weiter

ValidityLabs

ValidityLabs

The blockchain will be to banking, law and accountancy as the internet was to media, commerce and advertising.

Joichi Ito, Director MIT Media Lab

ENABLING DISRUPTION IN:

- Banking
- Legal services
- Organization management
- Internet of Things
- Supply chain management
- …any marketplace

ValidityLabs

THIS REQUIRES KNOWLEDGE IN:

- Applied computer science
- Cryptography
- Current financial systems
- Current legal systems
- Game theory

GEDANKENEXPERIMENT

Aim: Log financial transactions

From	To	Value
1	2	15
3	1	10
2	3	20
3	2	200
2	1	10
1	3	50
2	4	20

PROBLEM: MUTABILITY

No inherent security against:

Hacked database

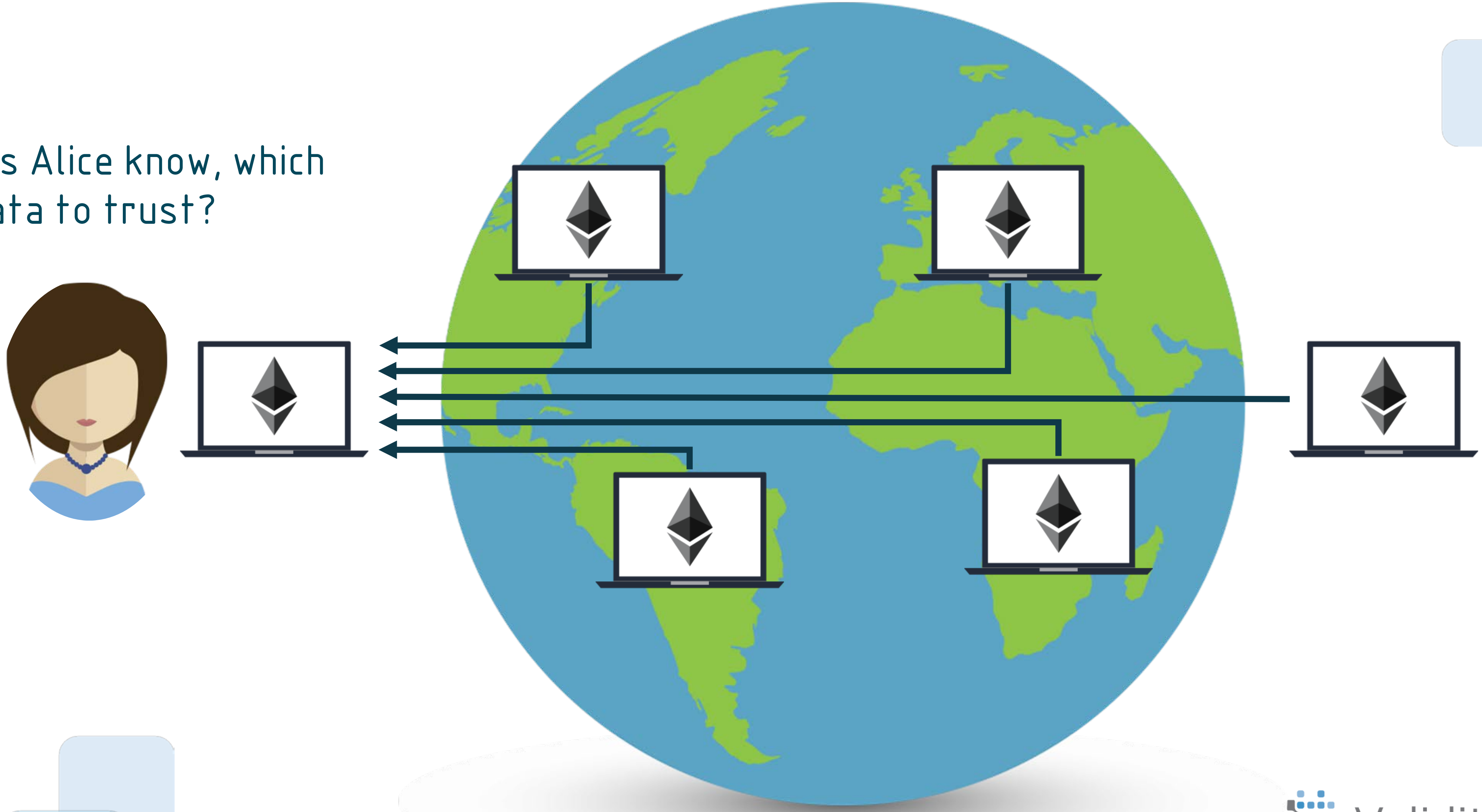
Rogue admin

From	To	Value
1	2	15
3	1	~~10~~ 5000
2	3	20
3	2	200
2	1	10
1	3	50
2	4	20

ValidityLabs

P2P NETWORK

How does Alice know, which data to trust?



BATCH PROCESSING

From	To	Value
1	2	15
3	1	10
2	3	20
3	2	200
2	1	10
1	3	50
2	4	20

ValidityLabs

BATCH PROCESSING

From	To	Value
1	2	15
3	1	10
2	3	20

From	To	Value
3	2	200
2	1	10

From	To	Value
1	3	50
2	4	20

CHAIN THE BLOCKS

ValidityLabs

Block number – 1		
From	To	Value
1	2	15
3	1	10
[illegible]	3	20

Digital root of block:

1 + 2 + 1 + 5 +

3 + 1 + 1 + 0 +

2 + 3 + 2 + 0

= 21

2 + 1

= 3

CHAIN THE BLOCKS

Block number – 1		
From	To	Value
1	2	15
3	1	10
	3	20

2 / Digital root of previous block – 3		
	To	Value
	2	200
	1	10

Digital root of block:

3 +

3 + 2 + 2 + 0 + 0 +

2 + 1 + 1 + 0

= 14

1 + 4

= 5

CHAIN THE BLOCKS

ValidityLabs

Block number – 1		
From	To	Value
1	2	15
3	1	10
2	3	20

Block number – 2 / Digital root of previous block – 3		
From	To	Value
3	2	200
2	1	10

Block number – 3 / Digital root of previous block – 5		
From	To	Value
1	3	50
2	4	20

LET'S CHEAT AGAIN!

ValidityLabs

Block number – 1		
From	To	Value
1	2	15
3	1	~~10~~ 5000
2	3	20

Block number – 2 / Digital root of previous block – 3 (actually 7!)		
From	To	Value
3	2	200
2	1	10

Block number – 3 / Digital root of previous block – 5 (actually 9!)		
From	To	Value
1	3	50
2	4	20

LET'S CHEAT PROPERLY!

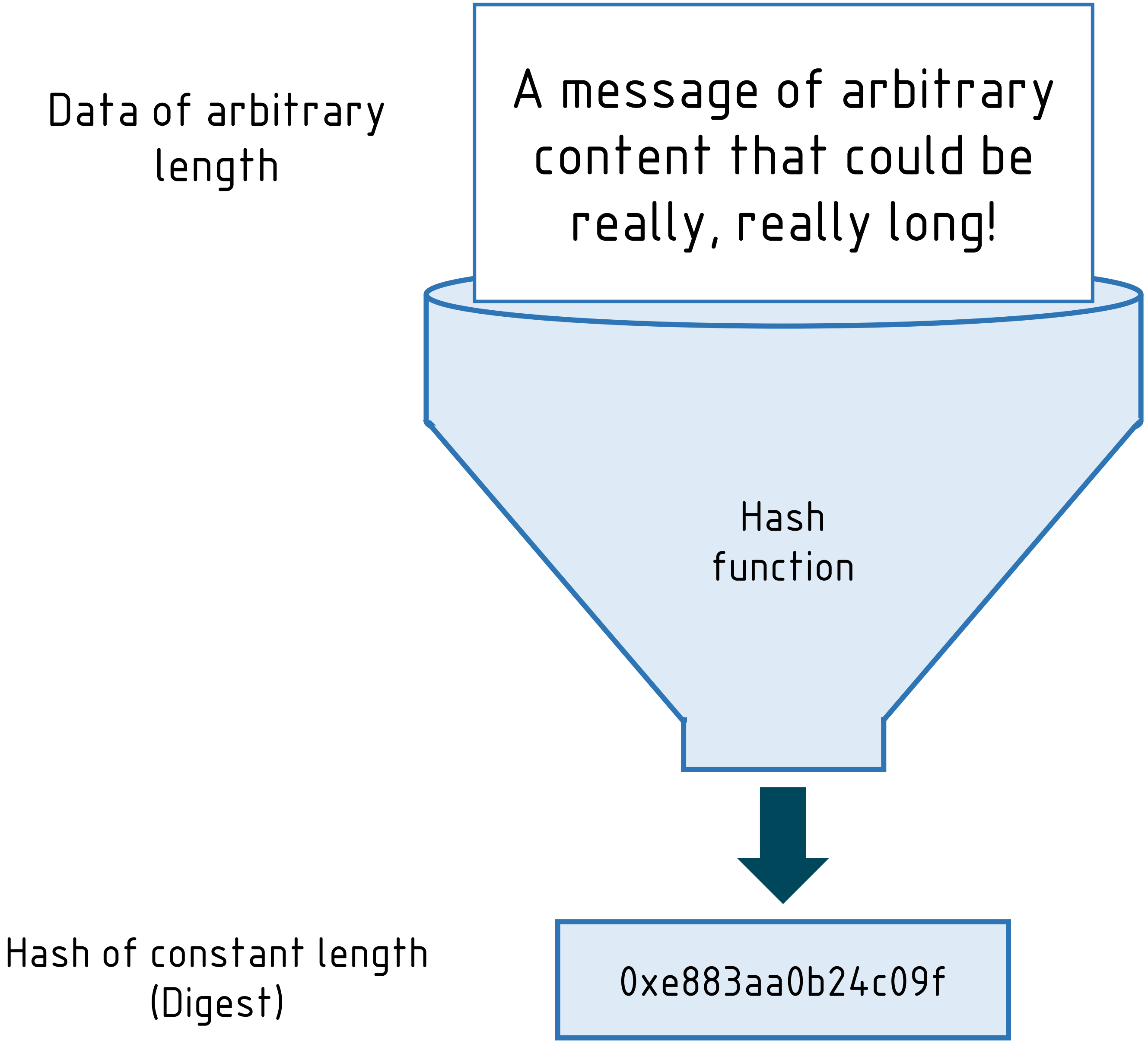
ValidityLabs

Block number – 1		
From	To	Value
1	2	15
3	1	~~10~~ 10000
2	3	20

Block number – 2 / Digital root of previous block – 3 (unchanged!)		
From	To	Value
3	2	200
2	1	10

Block number – 3 / Digital root of previous block – 5 (unchanged!)		
From	To	Value
1	3	50
2	4	20

HASHES



http://www.xorbin.com/tools/sha256-hash-calculator

ValidityLabs

AN ANALOGY

Human

Finger print

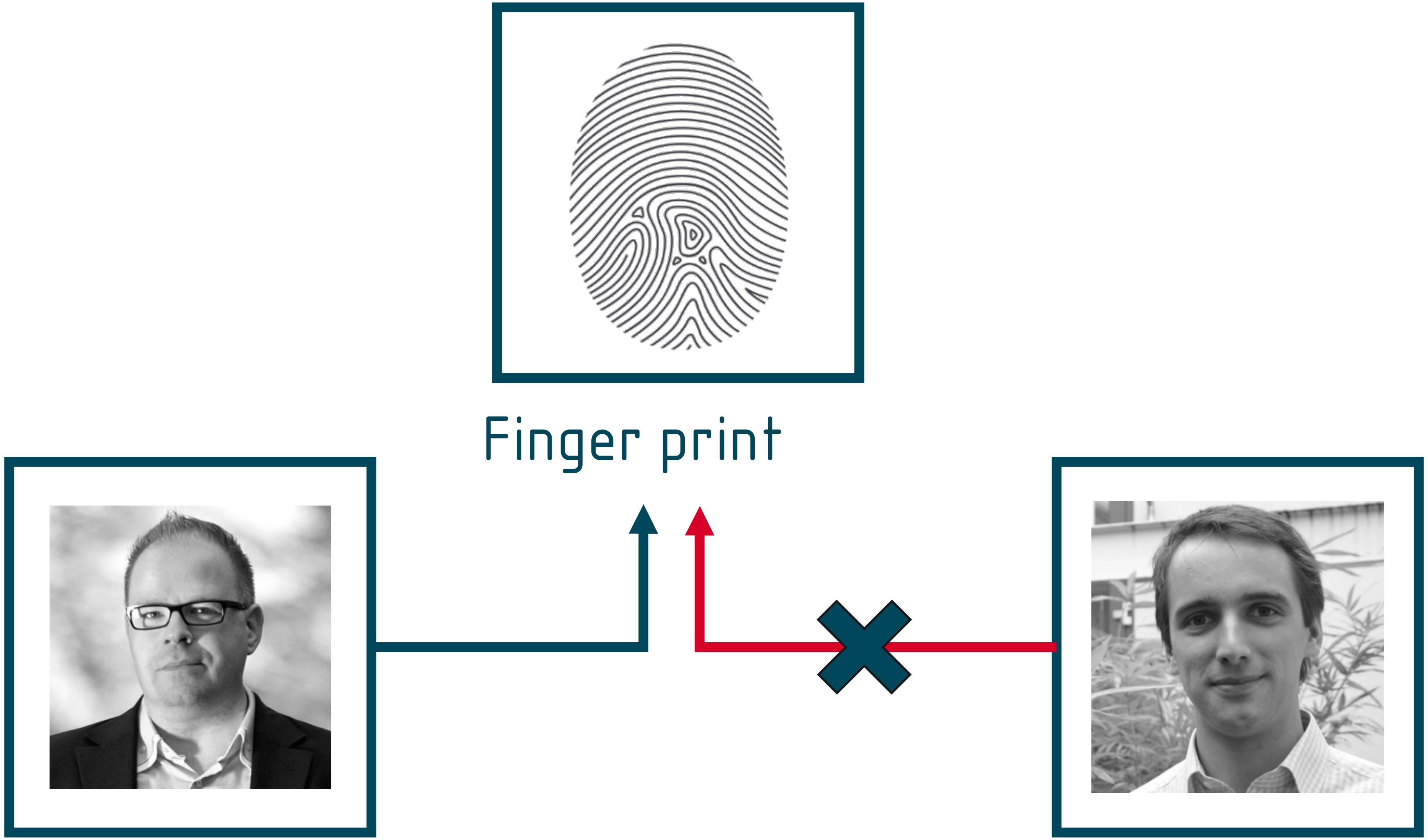
Data

Input!

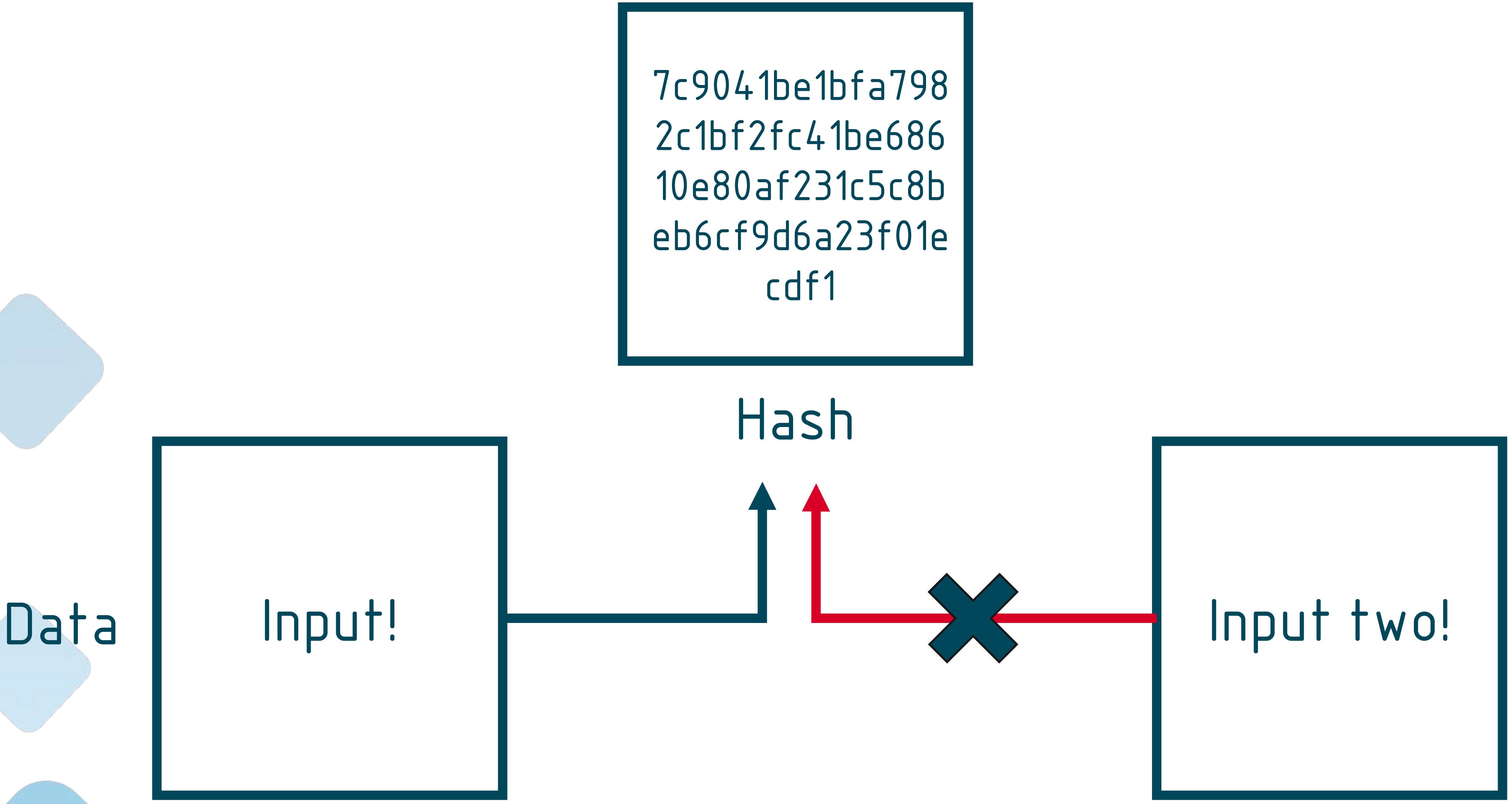
7c9041be1bfa798
2c1bf2fc41be686
10e80af231c5c8b
eb6cf9d6a23f01e
cdf1

Hash

COLLISION RESISTANCE



COLLISION RESISTANCE



HASH FUNCTIONS IN A BLOCKCHAIN

Block number – 1		
From	To	Value
1	2	15
3	1	10
2	3	20

Block number – 2 / previous block hash – 3eb571a...		
From	To	Value
3	2	200
2	1	10

Block number – 3 / previous block hash – a97b130...		
From	To	Value
1	3	50
2	4	20

HASH FUNCTIONS IN A BLOCKCHAIN

ValidityLabs

Block number – 1		
From	To	Value
1	2	15
3	1	~~10~~ 10000
2	3	20

Block number – 2 / previous block hash – 3eb571a... (actually 8a428c...)		
From	To	Value
3	2	200
2	1	10

Block number – 3 / previous block hash – a97b130... (actually fb196d...)		
From	To	Value
1	3	50
2	4	20

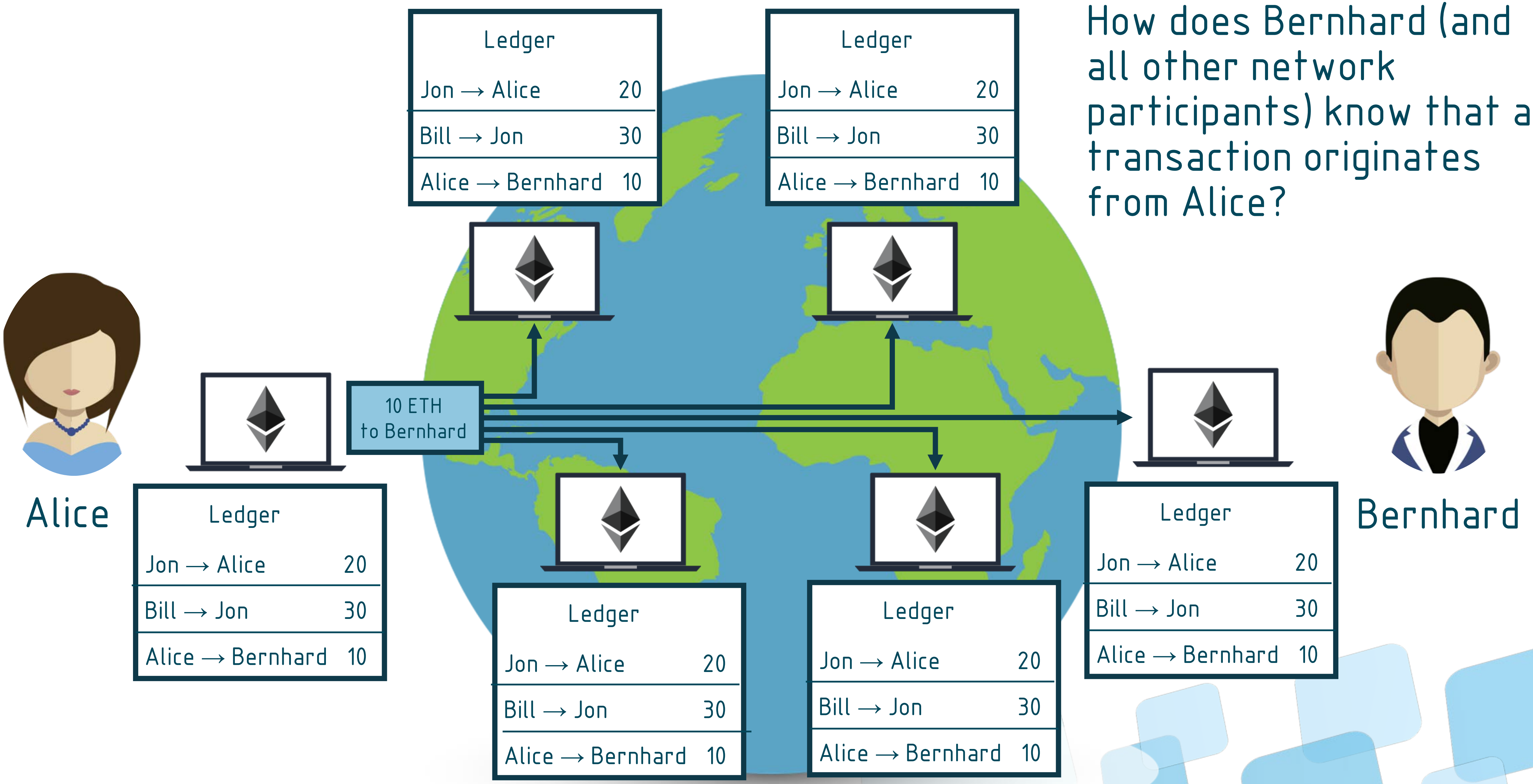
INHERENT VALIDITY:

Changes in one block
invalidate
all following blocks

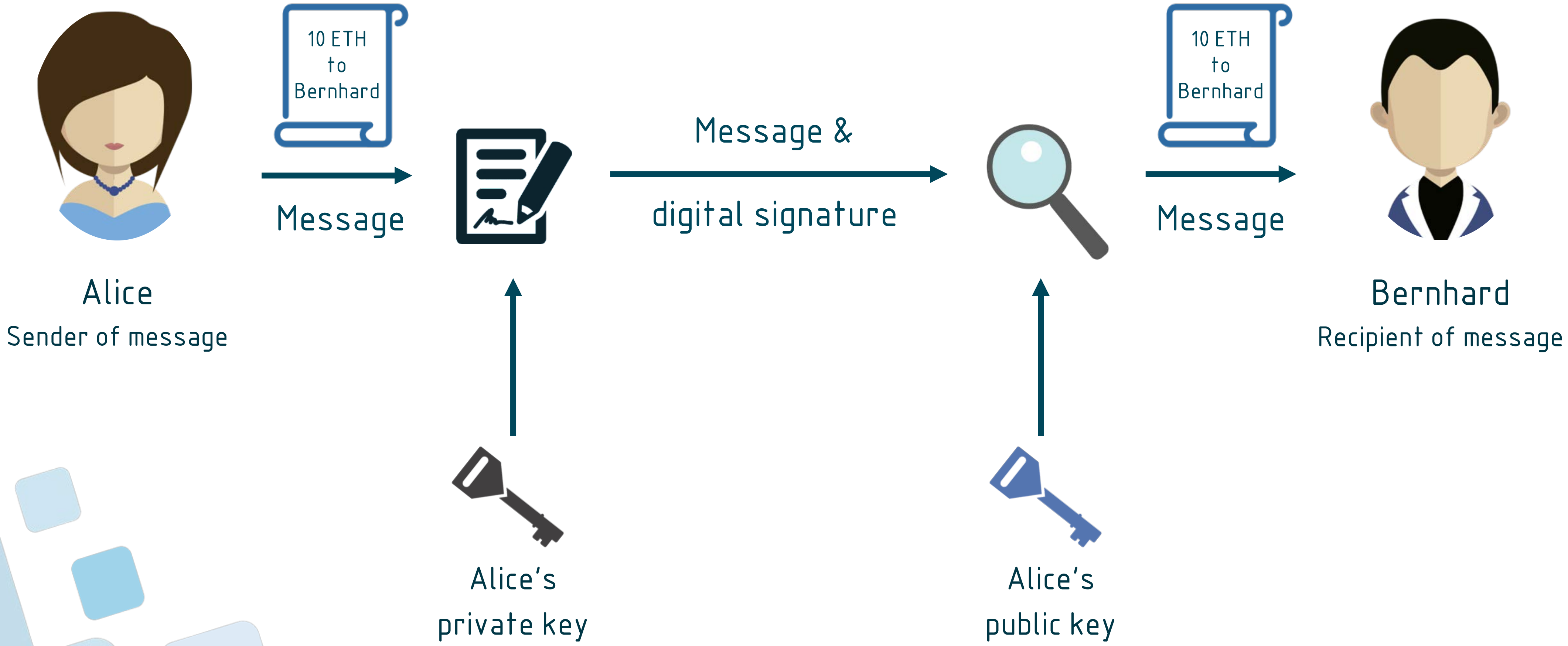
ValidityLabs

BLOCKCHAIN + P2P NETWORK

How does Bernhard (and all other network participants) know that a transaction originates from Alice?



DIGITAL SIGNATURES



https://kjur.github.io/jsrsasign/sample-ecdsa.html

SIGNATURES IN A BLOCKCHAIN

Block number – 2 / previous block hash – 3eb571a...			
From	To	Value	Signature
3	2	200	0x810a12b...
2	1	10	0x3c9012c...

But: Where is the public key with which we can validate a signature?

Public key = address

And: Where does the public key come from?

ValidityLabs

SIGNATURES IN A BLOCKCHAIN

Block number – 2 / previous block hash – 3eb571a...			
From	**To**	**Value**	**Signature**
0x1d0954...	0x826507...	200	0x810a12b...
0x826507...	0xf91a47...	10	0x3c9012c...

EC(‾GEHEIM')

EC(‾Passwort123!')

EC(‾S3B4$T14N')

EC = **Elliptic curve**, a complex one-way function

ValidityLabs

CONSENSUS

What do we include in a block?

Who declares a new block?

...the first one to solve a computational challenge:

"Find a hash of block content that matches some property"

CONSENSUS

"Find a hash that starts with N zeros"

Block content	Nonce	Hash
1121531102320	0	0xad816e3...
1121531102320	1	0x9a6f638...
1121531102320	2	0x48d816e...
...	...	...
1121531102320	10234	0x**000**2ba2...

Mining: Expensive to calculate, easy to verify

BLOCKCHAIN PLUS SMART CONTRACTS

Bitcoin-style blockchain

Ethereum-style blockchain
with smart contracts

SMART CONTRACT

=

Program on a blockchain that can control financial assets.

Let's add a contract to our blockchain

Block number – 1		
From	**To**	**Value**
0xf91a47...	0x826507...	15
0x1d0954...	0xf91a47...	10
826507...	0x1d0954...	20

Block number – 2 / previous block hash – 3eb571a...		
From	**To**	**Value**
0x1d0954...	0x826507...	200
0x826507...	0xf91a47...	10

Block number – 3 / previous block hash – a97b130...		
From	**To**	**Value**
0xf91a47...	0x1d0954...	50
0x826507...	0xf91a47...	20

Let’s add a contract to our blockchain

ValidityLabs

Block number – 1			
From	**To**	**Value**	**Payload**
1	2	15	0xb1a12b4564...
3		10	
2	3	20	

Address 2 is a contract

Contract deployment

Block number – 2 / previous block hash – 3eb571a...			
From	**To**	**Value**	
3	2	200	'Hello World!"
2		10	

Contract receives data

Contract sends money to its creator!

Block number – 3 / previous block hash – a97b130...			
From	**To**	**Value**	
1	3	50	
2	4	20	0x054e120380...

Contract creates another contract!

ValidityLabs

A new dimension for payments

Since ~ 10.000 years

Transaction of financial assets from and to:

- People
- Organizations

ValidityLabs

ethereum

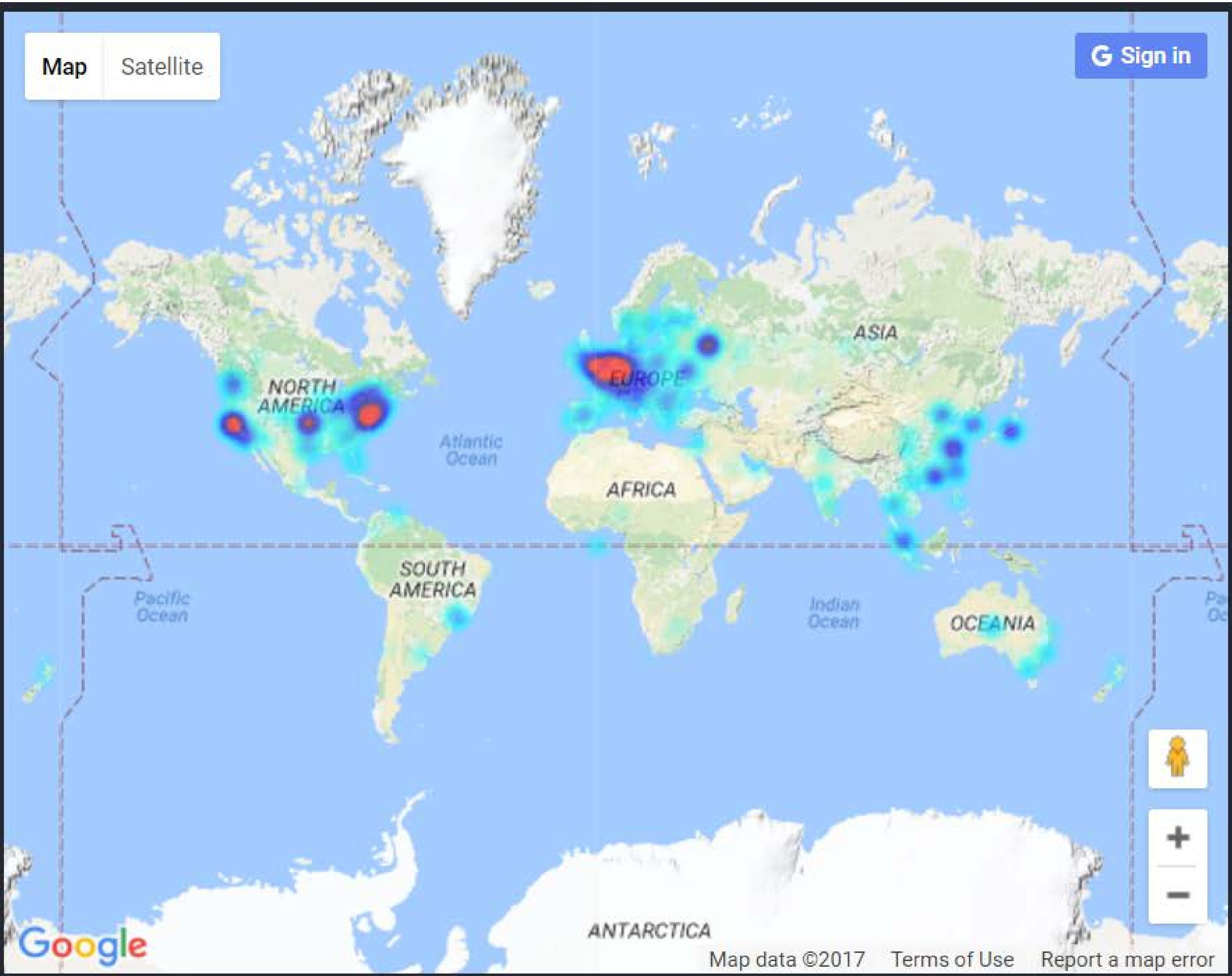
A new dimension for payments

Since 07/30/2015 3:26 UTC
(Ethereum genesis block)

Transaction of financial assets from and to:

- People
- Organizations
- **Programs**

Total	5937 (100%)
United States	1665 (28.04%)
Germany	450 (7.58%)
Russian Federation	342 (5.76%)
China	321 (5.41%)
United Kingdom	314 (5.29%)
Canada	250 (4.21%)
Netherlands	232 (3.91%)
France	228 (3.84%)
Australia	123 (2.07%)
Ukraine	122 (2.05%)



Timelock Smart Contract

```
contract LockTimeContract
{
    struct accountData
    {
        uint balance;
        uint releaseTime;
    }

    mapping (address => accountData) accounts;

    function payIn(uint lockTimeS) returns (bool x)
    {
        uint amount = msg.value;
```

```
accounts[msg.sender].balance = amount;
```

```
            return false;
        }
        accounts[msg.sender].balance = amount;
        accounts[msg.sender].releaseTime = now + lockTimeS;
        return true;
    }

    function payOut() returns (bool x)
    {
        if (accounts[msg.sender].balance != 0 && accounts[msg.sender].releaseTime < now)
        {
            msg.sender.send(accounts[msg.sender].balance);
            return true;
        }
        else
            return true;
    }

    function getMyLockedFunds() constant returns (uint x)
```

[github.com/SCBuergel/timeLock-smartContract]

But this was just for fun...

Right?!

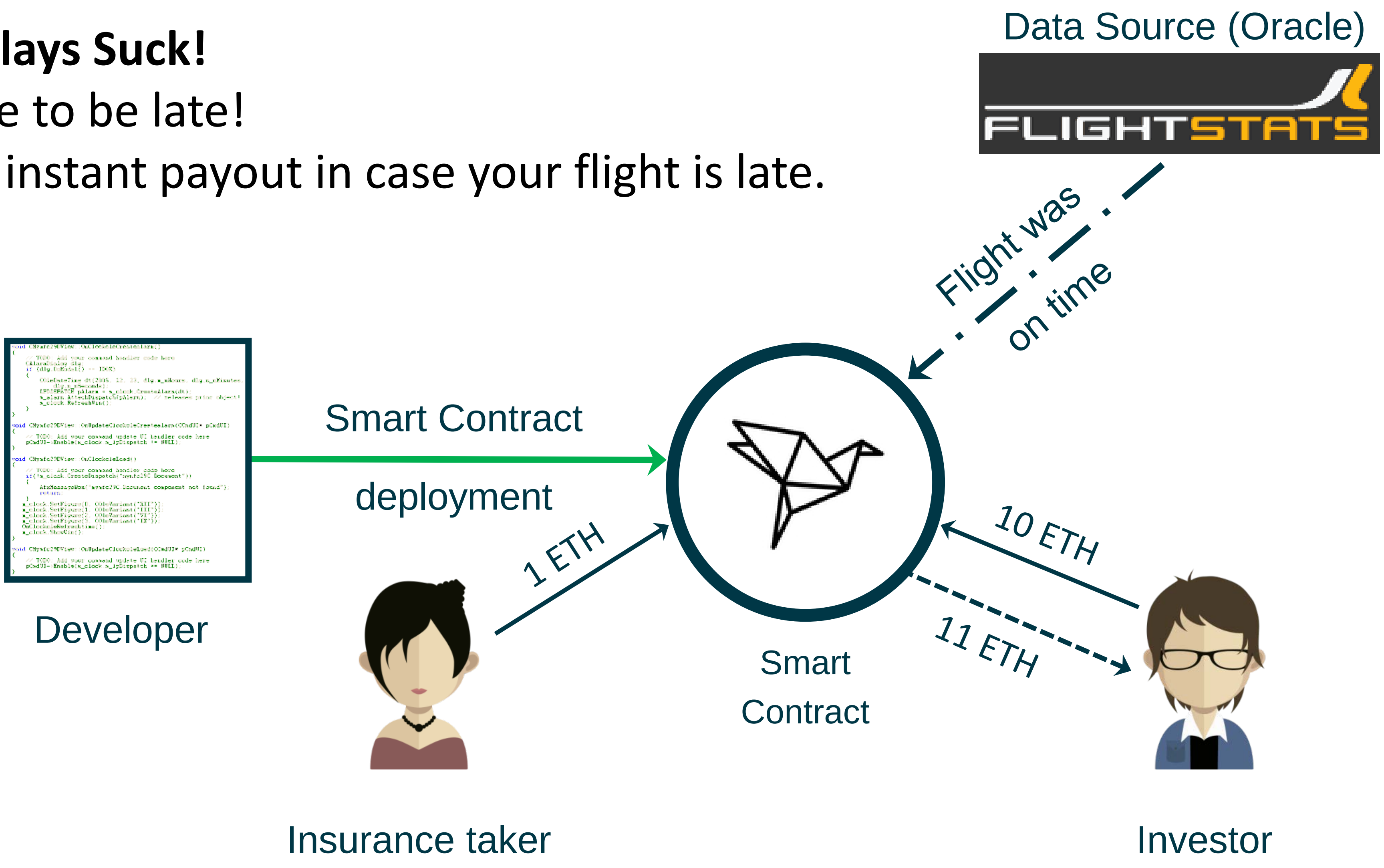
Flight Delay Dapp

ARCHITECTURE

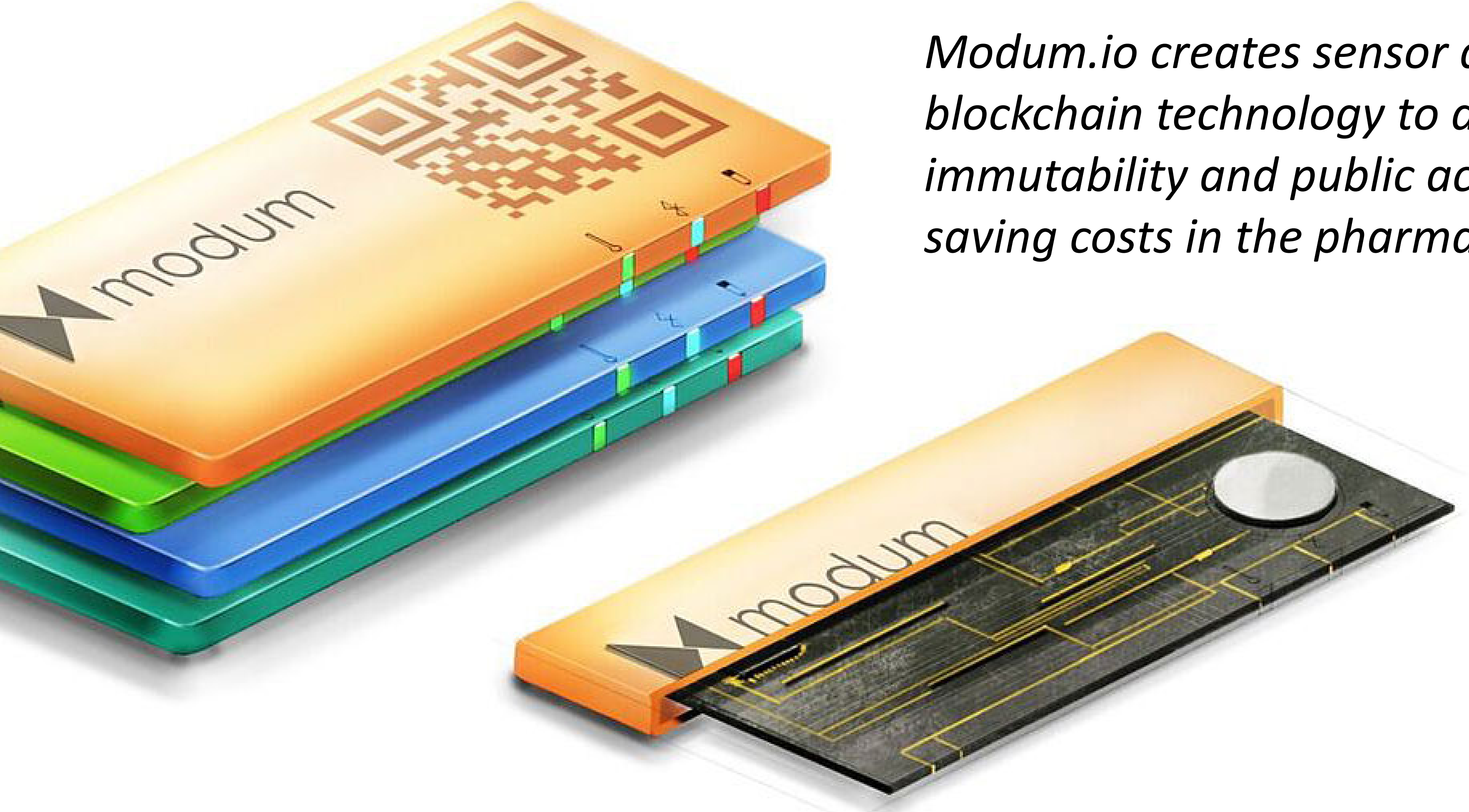
Flight Delays Suck!

You'll love to be late!

Get your instant payout in case your flight is late.



Modum.io creates sensor devices leveraging blockchain technology to assert data immutability and public accessibility while saving costs in the pharma supply chain.



MELONPORT

Reto Trinkler
Chairman/CTO

Mona El Isa
CEO

George Hallam
Head of Business Development

Ahmad S. Afandi
Head of Design

Ethereum: Melonport fills its CHF2.5m token issuance in under three minutes

The Ethereum hedge fund platform Melonport is breaking records in the world of initial coin offerings.

THANK YOU!

http://validitylabs.org

hello@validitylabs.org

@validitylabs

ValidityLabs