Introduction to Blockchain and Recordkeeping

Peter Van Garderen
March 9, 2016
Recordkeeping Roundtable
Sydney, Australia

http://www.slideshare.net/peterVG999/introduction-to-blockchain-and-recordkeeping

VANGARDEREN.NET

INFORMATION MANAGEMENT CONSULTING

InterPARES project

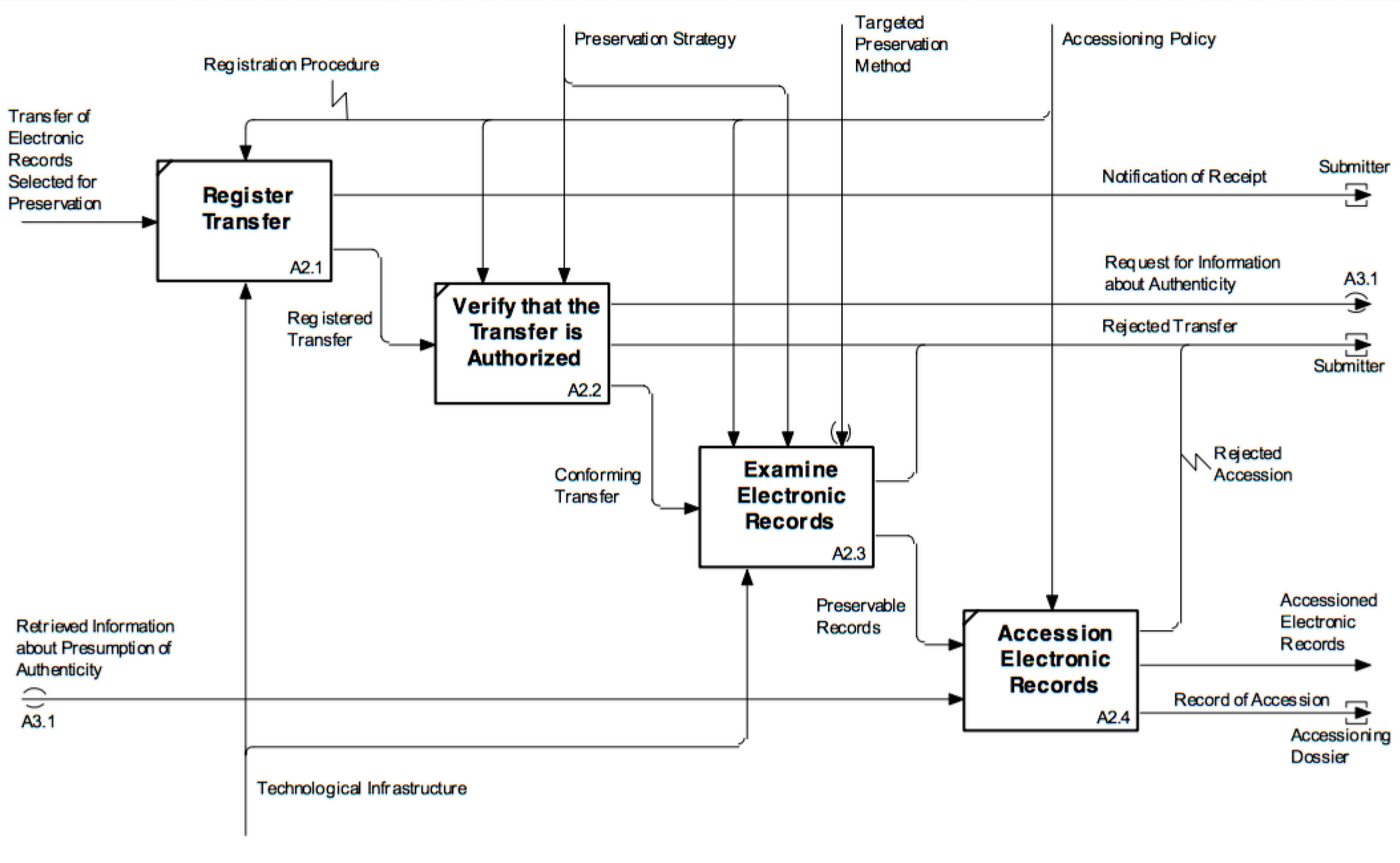
“the authenticity of a record over time rests on the assumption that the physical object that embodies **the record has not changed in any way** that would affect the message it was intended to communicate.”

“The principle of the unbroken **chain of custody** stipulates that, throughout their life cycles, records should be in the custody of known parties who can be trusted to preserve them intact.”

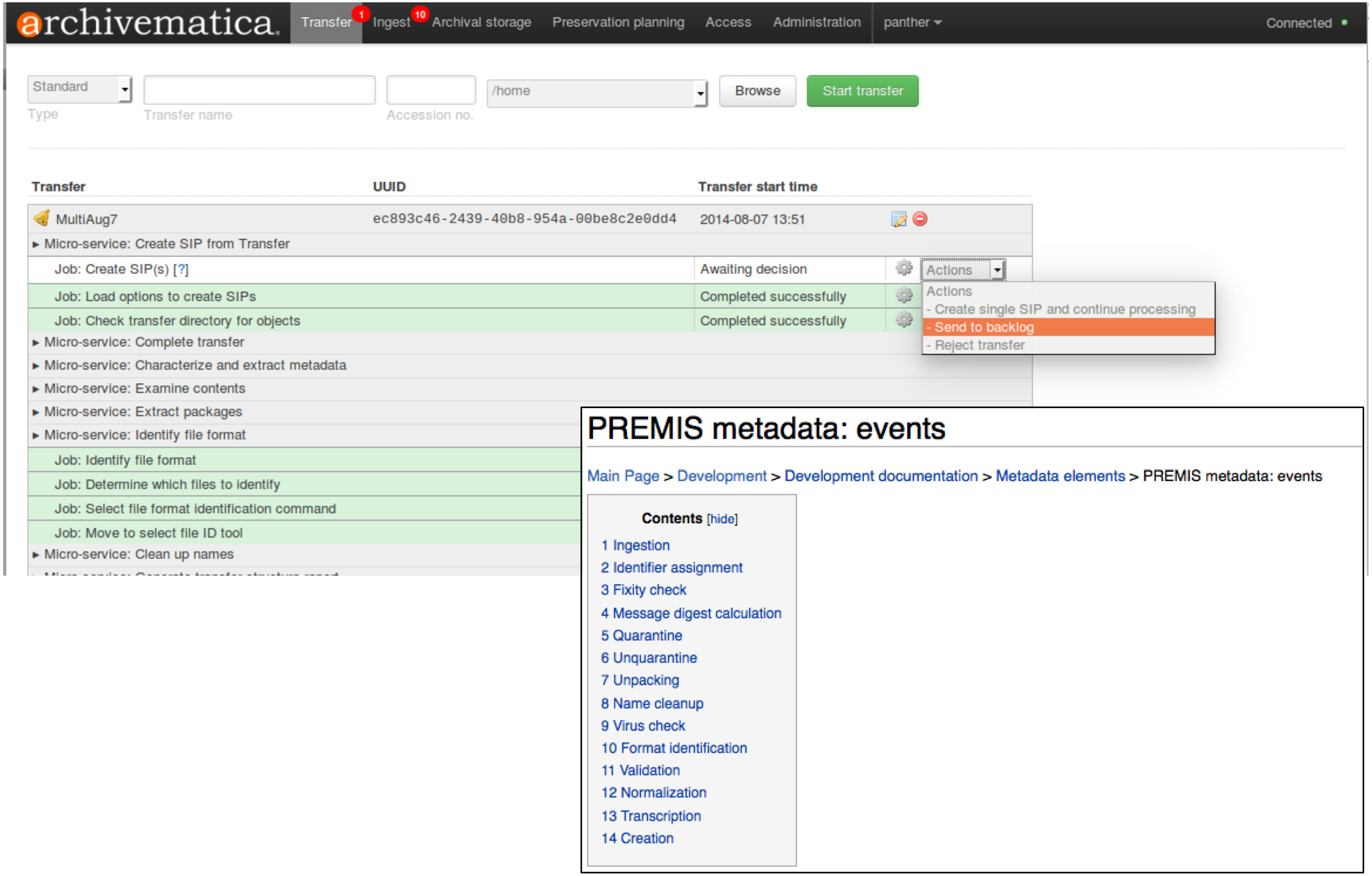
“the **chain of preservation** will include information about the records creator’s practices to support a presumption of authenticity, in accordance with the benchmark requirements for authenticity, information about the processes of bringing the records into the archives and maintaining them over time, and information about the reproduction of records.”

The Long-term Preservation of Authentic Electronic Records: Findings of the InterPARES Project (2001) http://interpares.org/book/

USED AT:	AUTHOR: Preservation Task Force DATE: 24/01/2002 PROJECT: InterPARES REV: 31/05/2002 NOTES: 1 2 3 4 5 6 7 8 9 10	WORKING	READER DATE	CONTEXT:
		DRAFT		
		RECOMMENDED		
		■ PUBLICATION		A0


Registration Procedure
Preservation Strategy
Targeted Preservation Method
Accessioning Policy
Transfer of Electronic Records Selected for Preservation
Register Transfer
A2.1
Notification of Receipt
Submitter
Registered Transfer
Verify that the Transfer is Authorized
A2.2
Request for Information about Authenticity
A3.1
Rejected Transfer
Submitter
Conforming Transfer
Examine Electronic Records
A2.3
Rejected Accession
Preservable Records
Accession Electronic Records
A2.4
Accessioned Electronic Records
Record of Accession
Accessioning Dossier
Retrieved Information about Presumption of Authenticity
A3.1
Technological Infrastructure

NODE: A2	TITLE: Bring In Electronic Records	NUMBER: v 6.0



Transfer	UUID	Transfer start time	
MultiAug7	ec893c46-2439-40b8-954a-00be8c2e0dd4	2014-08-07 13:51	
▸ Micro-service: Create SIP from Transfer			
Job: Create SIP(s) [?]		Awaiting decision	Actions
Job: Load options to create SIPs		Completed successfully	
Job: Check transfer directory for objects		Completed successfully	
▸ Micro-service: Complete transfer			
▸ Micro-service: Characterize and extract metadata			
▸ Micro-service: Examine contents			
▸ Micro-service: Extract packages			
▸ Micro-service: Identify file format			
Job: Identify file format			
Job: Determine which files to identify			
Job: Select file format identification command			
Job: Move to select file ID tool			
▸ Micro-service: Clean up names			
▸ Micro-service: Generate transfer structure report			

PREMIS metadata: events

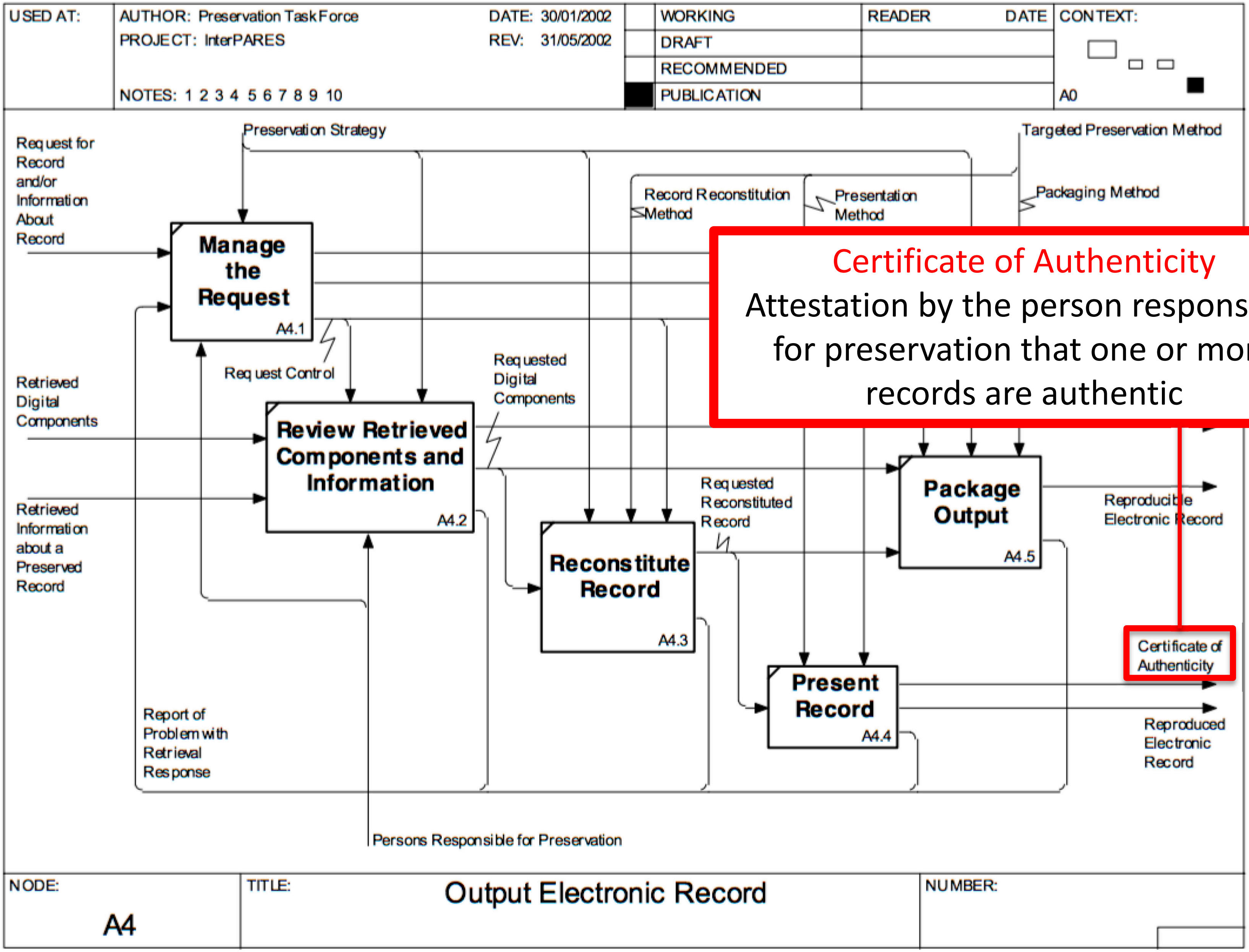
Main Page > Development > Development documentation > Metadata elements > PREMIS metadata: events

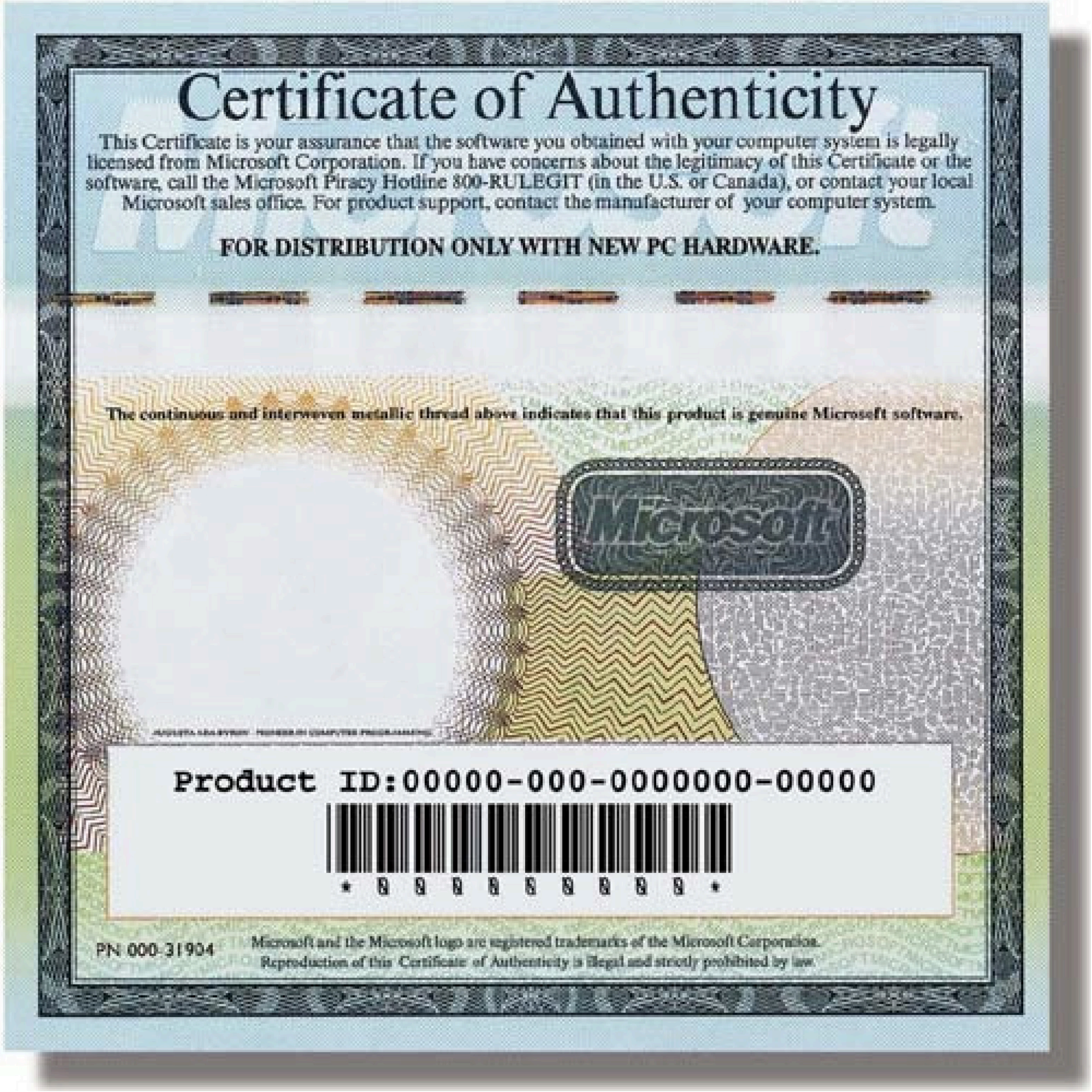
Contents [hide]

1 Ingestion
2 Identifier assignment
3 Fixity check
4 Message digest calculation
5 Quarantine
6 Unquarantine
7 Unpacking
8 Name cleanup
9 Virus check
10 Format identification
11 Validation
12 Normalization
13 Transcription
14 Creation

Certificate of Authenticity

Attestation by the person responsible for preservation that one or more records are authentic


USED AT:
AUTHOR: Preservation Task Force
PROJECT: InterPARES
DATE: 30/01/2002
REV: 31/05/2002
NOTES: 1 2 3 4 5 6 7 8 9 10
WORKING
DRAFT
RECOMMENDED
PUBLICATION
READER
DATE
CONTEXT:
A0
Preservation Strategy
Targeted Preservation Method
Request for Record and/or Information About Record
Record Reconstitution Method
Presentation Method
Packaging Method
Manage the Request
A4.1
Request Control
Requested Digital Components
Retrieved Digital Components
Review Retrieved Components and Information
A4.2
Retrieved Information about a Preserved Record
Requested Reconstituted Record
Package Output
A4.5
Reproducible Electronic Record
Reconstitute Record
A4.3
Present Record
A4.4
Certificate of Authenticity
Reproduced Electronic Record
Report of Problem with Retrieval Response
Persons Responsible for Preservation
NODE:
A4
TITLE:
Output Electronic Record
NUMBER:



Certificate of Authenticity

This Certificate is your assurance that the software you obtained with your computer system is legally licensed from Microsoft Corporation. If you have concerns about the legitimacy of this Certificate or the software, call the Microsoft Piracy Hotline 800-RULEGIT (in the U.S. or Canada), or contact your local Microsoft sales office. For product support, contact the manufacturer of your computer system.

FOR DISTRIBUTION ONLY WITH NEW PC HARDWARE.

The continuous and interwoven metallic thread above indicates that this product is genuine Microsoft software.

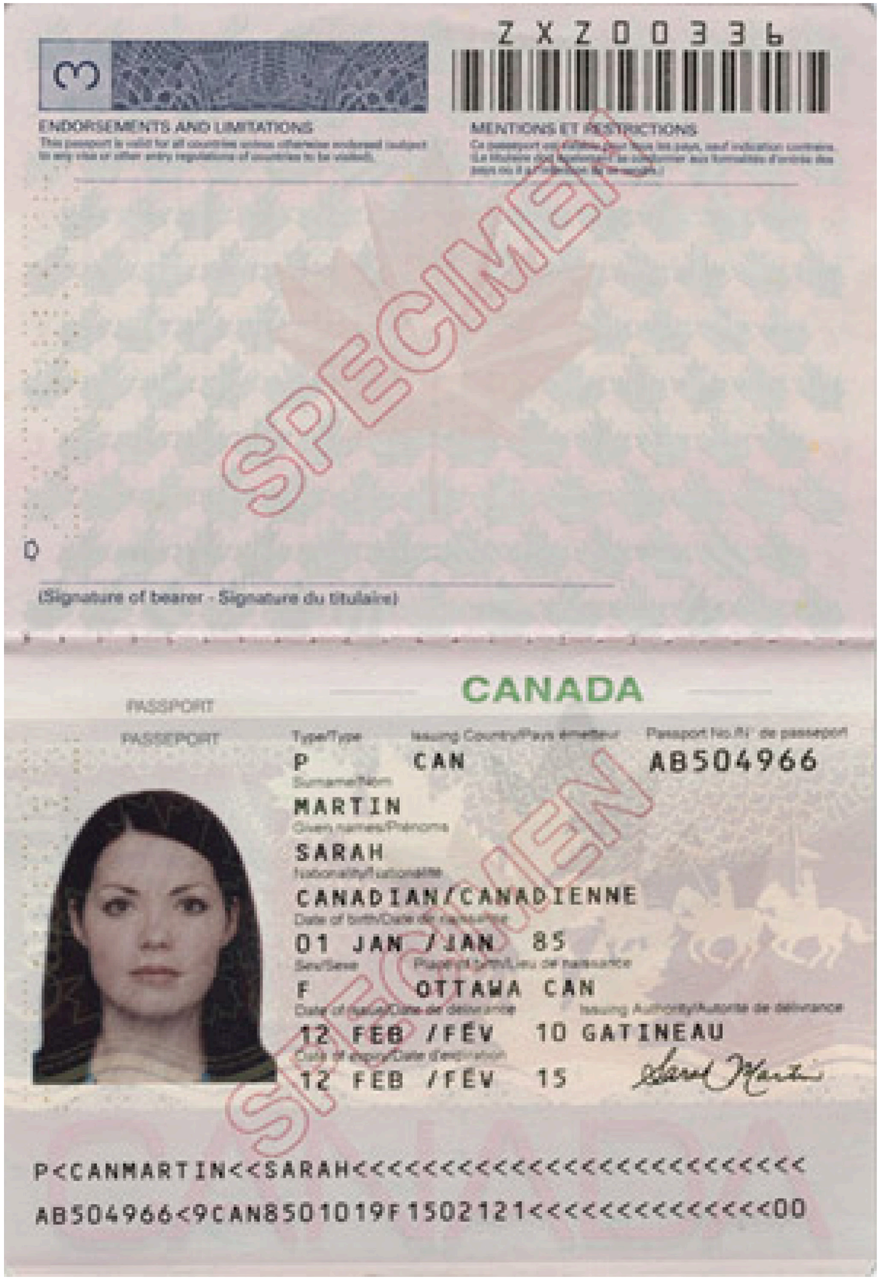
AUGUSTA ADA BYRON · PIONEER IN COMPUTER PROGRAMMING

Product ID:00000-000-0000000-00000

* 0 0 0 0 0 0 0 0 0 0 *

PN 000-31904

Microsoft and the Microsoft logo are registered trademarks of the Microsoft Corporation.
Reproduction of this Certificate of Authenticity is illegal and strictly prohibited by law.



ZXZ00336

ENDORSEMENTS AND LIMITATIONS

This passport is valid for all countries unless otherwise endorsed (subject to any visa or other entry regulations of countries to be visited).

MENTIONS ET RESTRICTIONS

Ce passeport est valable pour tous les pays, sauf indication contraire. (Le titulaire doit néanmoins se conformer aux formalités d'entrée des pays où il a l'intention de voyager.)

(Signature of bearer - Signature du titulaire)

SPECIMEN

CANADA

PASSPORT

PASSEPORT

Type/Type: P

Issuing Country/Pays émetteur: CAN

Passport No./N° de passeport: AB504966

Surname/Nom: MARTIN

Given names/Prénoms: SARAH

Nationality/Nationalité: CANADIAN/CANADIENNE

Date of birth/Date de naissance: 01 JAN /JAN 85

Sex/Sexe: F

Place of birth/Lieu de naissance: OTTAWA CAN

Date of issue/Date de délivrance: 12 FEB /FÉV 10

Issuing Authority/Autorité de délivrance: GATINEAU

Date of expiry/Date d'expiration: 12 FEB /FÉV 15

Sarah Martin

SPECIMEN

CANADA

```
P<CANMARTIN<<SARAH<<<<<<<<<<<<<<<<<<<<<<<<<<
AB504966<9CAN8501019F1502121<<<<<<<<<<<<<<00
```

Certificate of A
of Notary P

County

N, Clerk of Superior Court in and for said
whose address is [illegible]
was duly appointed and sworn in as a Notary
17, Art. 1 as Amended, that their term of office
expires on the **14th day of May, 2012.**

WITNESS my hand and seal of said Co
15th day of May, 2008

(Deputy Clerk's
Deputy Clerk of Su
PUTNAM Co

SSL Certificate

SATISFACTION 100% GUARANTEED

RapidSSL

VeriSign®

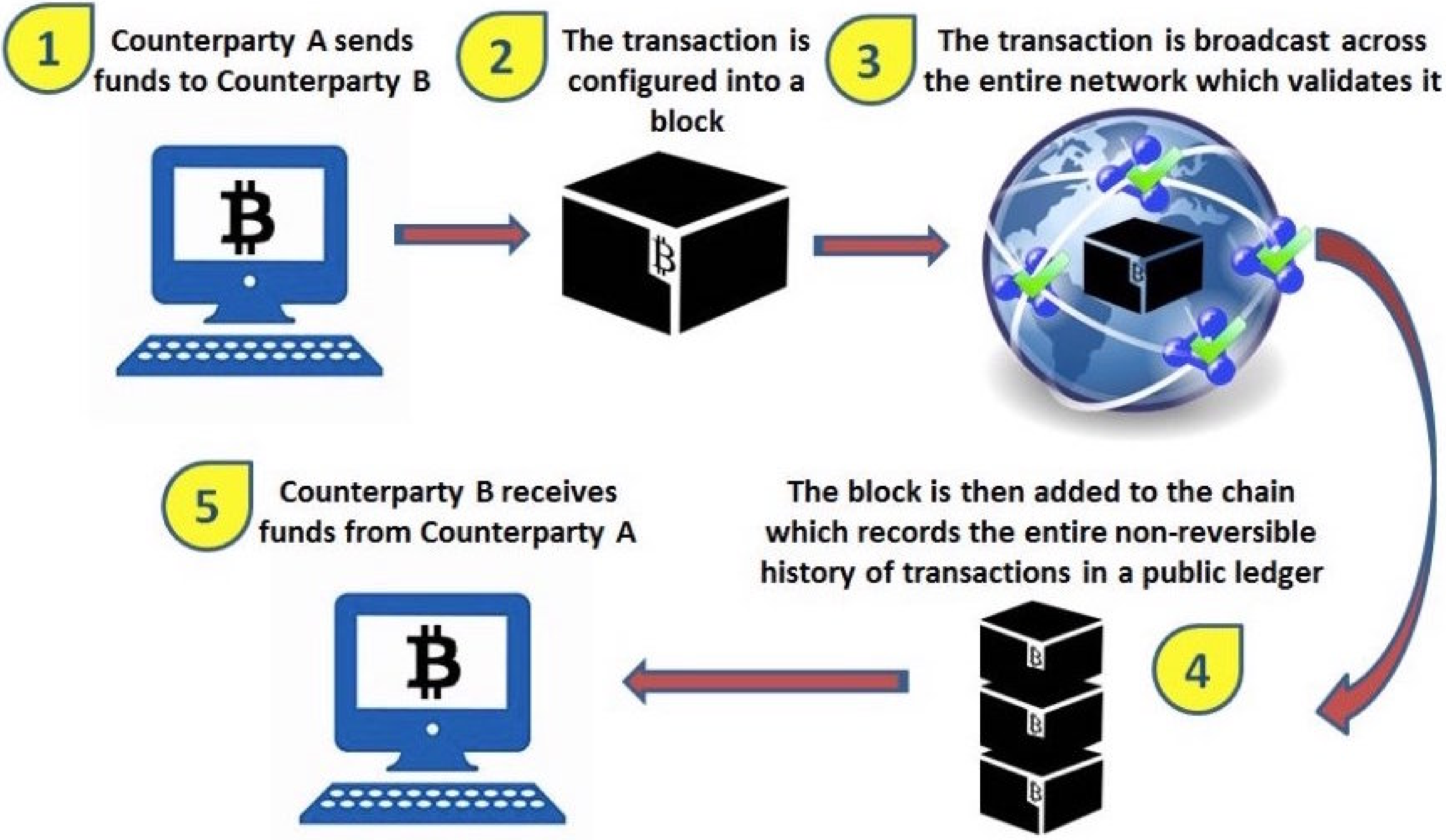
thawte™

GeoTrust®

traditional record authenticity	blockchain record authenticity
• high cost	• low cost
• long delays	• quick turnaround
• permission granted	• permissionless
• trusted third-party	• trustless

What is a blockchain?

a distributed public database that leverages cryptography and peer-to-peer technology to group data into blocks and store them in an immutable chain of transactions



1 Counterparty A sends funds to Counterparty B

2 The transaction is configured into a block

3 The transaction is broadcast across the entire network which validates it

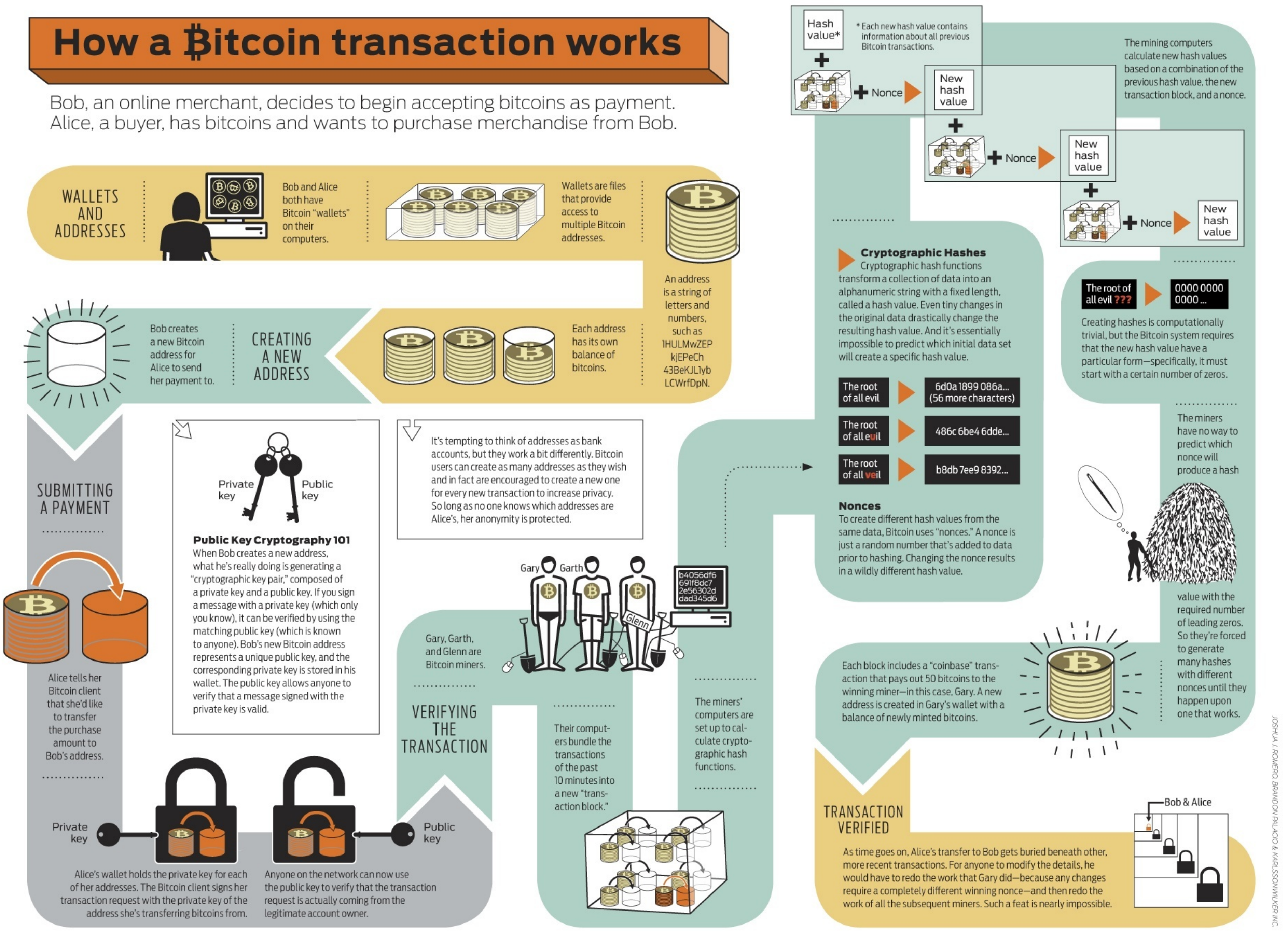
4 The block is then added to the chain which records the entire non-reversible history of transactions in a public ledger

5 Counterparty B receives funds from Counterparty A

source: Goldman Sachs Investment Research

How a Ƀitcoin transaction works

Bob, an online merchant, decides to begin accepting bitcoins as payment. Alice, a buyer, has bitcoins and wants to purchase merchandise from Bob.



WALLETS AND ADDRESSES

Bob and Alice both have Bitcoin "wallets" on their computers.

Wallets are files that provide access to multiple Bitcoin addresses.

An address is a string of letters and numbers, such as 1HULMwZEP kjEPeCh 43BeKJL1yb LCWrfDpN.

Each address has its own balance of bitcoins.

CREATING A NEW ADDRESS

Bob creates a new Bitcoin address for Alice to send her payment to.

It's tempting to think of addresses as bank accounts, but they work a bit differently. Bitcoin users can create as many addresses as they wish and in fact are encouraged to create a new one for every new transaction to increase privacy. So long as no one knows which addresses are Alice's, her anonymity is protected.

Public Key Cryptography 101
When Bob creates a new address, what he's really doing is generating a "cryptographic key pair," composed of a private key and a public key. If you sign a message with a private key (which only you know), it can be verified by using the matching public key (which is known to anyone). Bob's new Bitcoin address represents a unique public key, and the corresponding private key is stored in his wallet. The public key allows anyone to verify that a message signed with the private key is valid.

SUBMITTING A PAYMENT

Alice tells her Bitcoin client that she'd like to transfer the purchase amount to Bob's address.

Alice's wallet holds the private key for each of her addresses. The Bitcoin client signs her transaction request with the private key of the address she's transferring bitcoins from.

Anyone on the network can now use the public key to verify that the transaction request is actually coming from the legitimate account owner.

VERIFYING THE TRANSACTION

Gary, Garth, and Glenn are Bitcoin miners.

Their computers bundle the transactions of the past 10 minutes into a new "transaction block."

The miners' computers are set up to calculate cryptographic hash functions.

Cryptographic Hashes
Cryptographic hash functions transform a collection of data into an alphanumeric string with a fixed length, called a hash value. Even tiny changes in the original data drastically change the resulting hash value. And it's essentially impossible to predict which initial data set will create a specific hash value.

The root of all evil	6d0a 1899 086a... (56 more characters)
The root of all euil	486c 6be4 6dde...
The root of all veil	b8db 7ee9 8392...

Nonces
To create different hash values from the same data, Bitcoin uses "nonces." A nonce is just a random number that's added to data prior to hashing. Changing the nonce results in a wildly different hash value.

* Each new hash value contains information about all previous Bitcoin transactions.

The mining computers calculate new hash values based on a combination of the previous hash value, the new transaction block, and a nonce.

The root of all evil ???	0000 0000 0000 ...

Creating hashes is computationally trivial, but the Bitcoin system requires that the new hash value have a particular form—specifically, it must start with a certain number of zeros.

The miners have no way to predict which nonce will produce a hash value with the required number of leading zeros. So they're forced to generate many hashes with different nonces until they happen upon one that works.

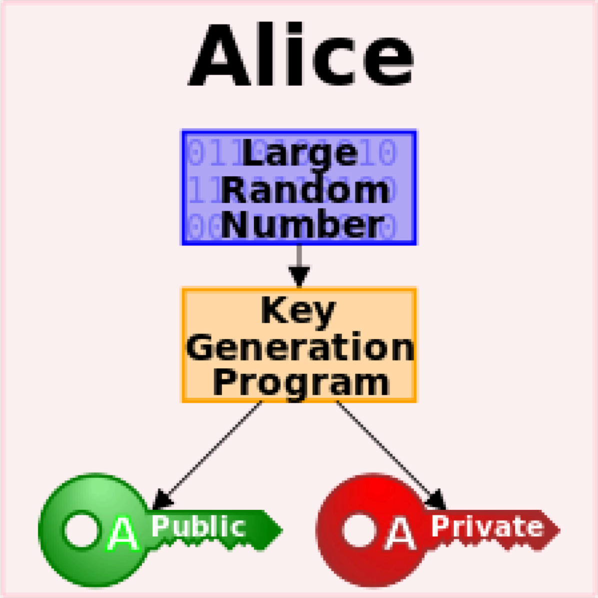
Each block includes a "coinbase" transaction that pays out 50 bitcoins to the winning miner—in this case, Gary. A new address is created in Gary's wallet with a balance of newly minted bitcoins.

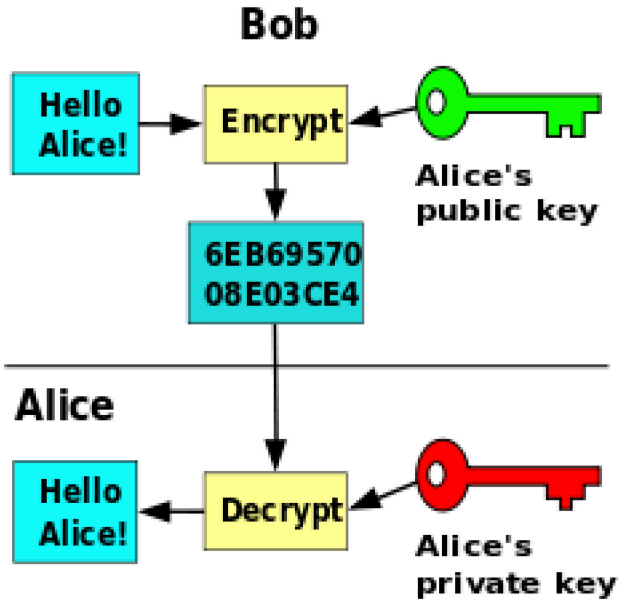
TRANSACTION VERIFIED

As time goes on, Alice's transfer to Bob gets buried beneath other, more recent transactions. For anyone to modify the details, he would have to redo the work that Gary did—because any changes require a completely different winning nonce—and then redo the work of all the subsequent miners. Such a feat is nearly impossible.

JOSHUA J. ROMERO; BRANDON PALACIO & KARLSSONWILKER INC.

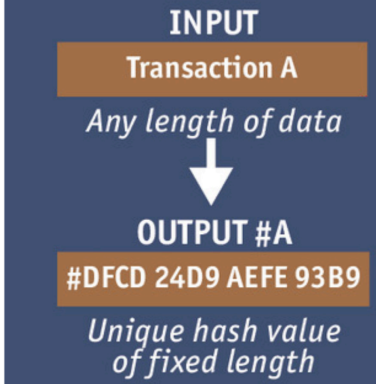
source: https://www.techinasia.com/southeast-asia-blockchain-technology-bitcoin-insights

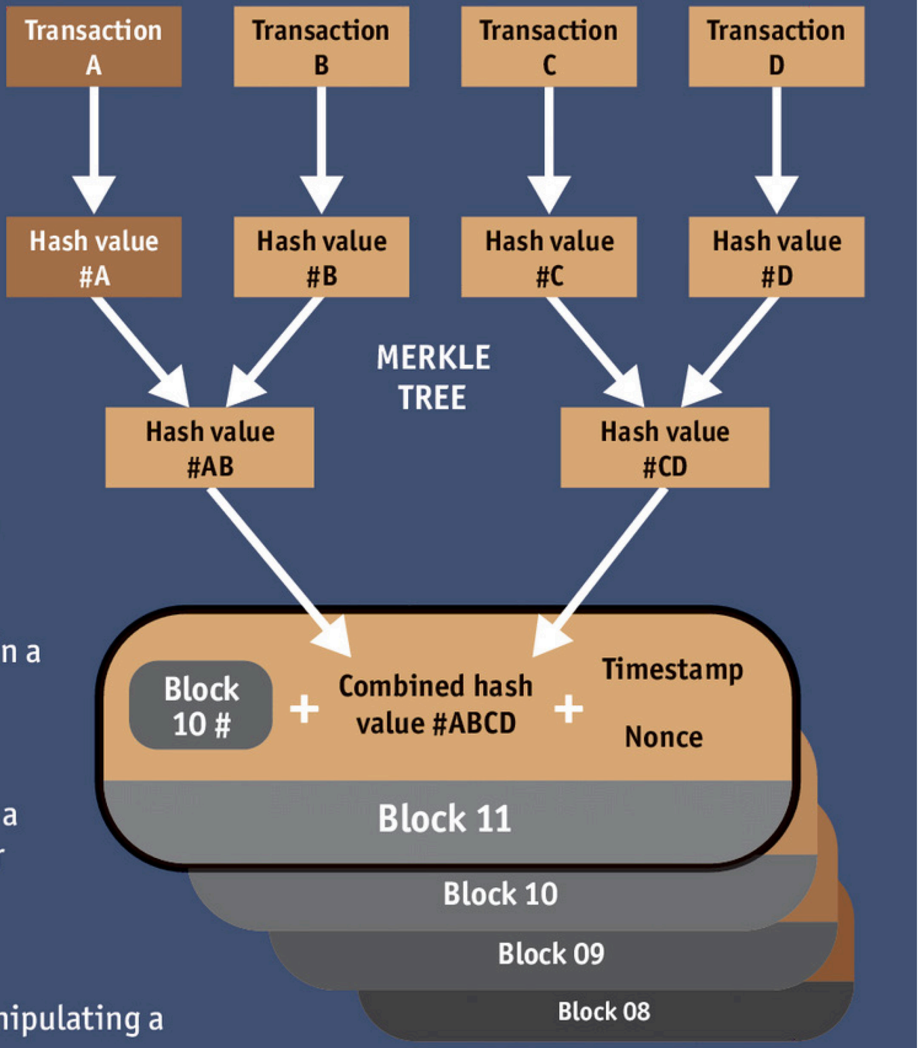




source: https://en.wikipedia.org/wiki/Public-key_cryptography

Making a hash of it





Each transaction in the set that makes up a block is fed through a program that creates an encrypted code known as the hash value.

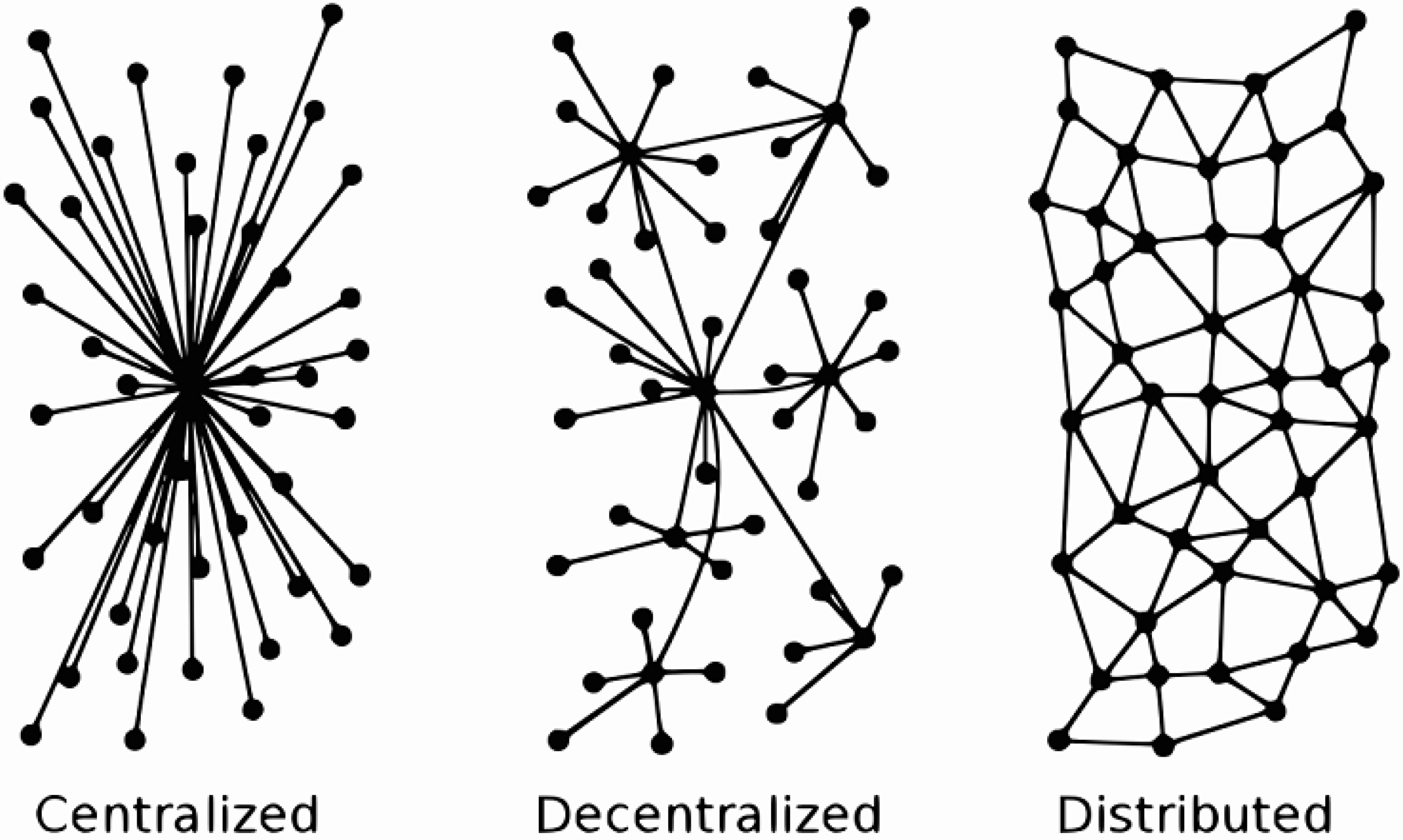
Hash values are further combined in a system known as a Merkle Tree.

The result of all this hashing goes into the block's header, along with a hash of the previous block's header and a timestamp.

The header then becomes part of a cryptographic puzzle solved by manipulating a number called the nonce.

Once a solution is found the new block is added to the blockchain.

Economist.com


Centralized
Decentralized
Distributed

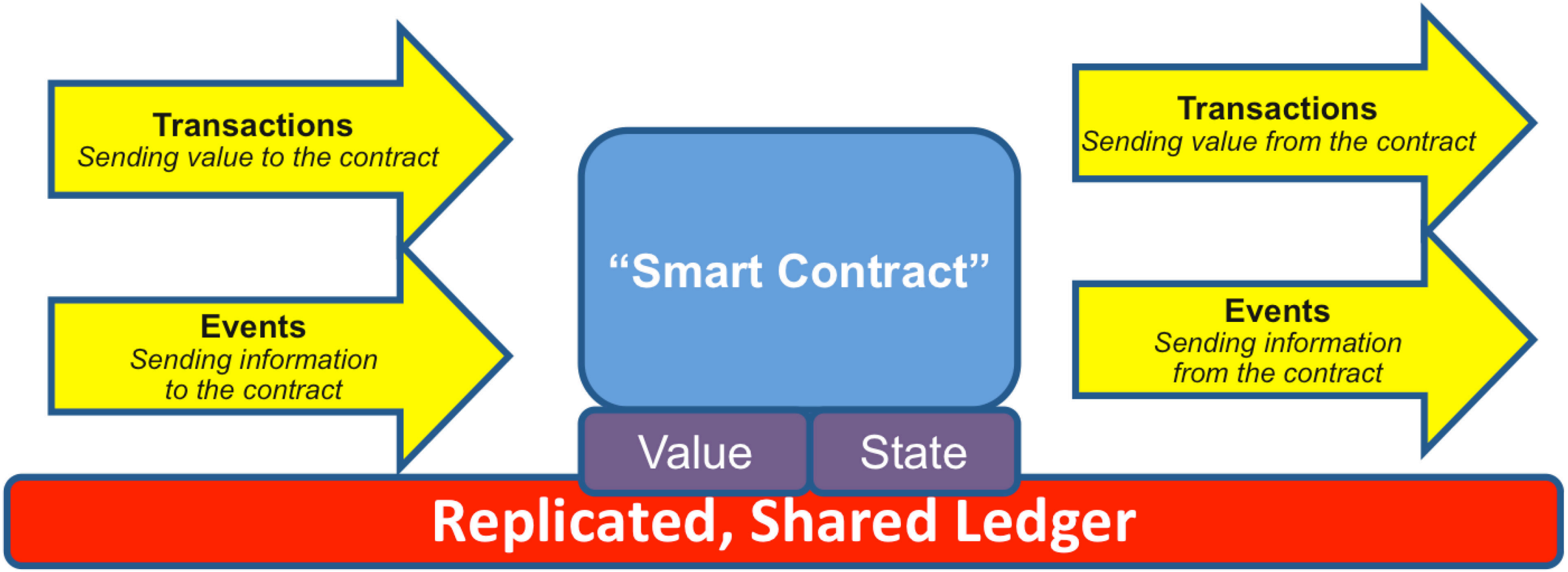
bitcoin

- Excellent protocol for storing and transmitting value
- Not a generic protocol on which other platforms and functionality are easily built
  - Light clients for Bitcoin but not feasible for other apps on its blockchain
  - more like SMTP than TCP
- SHA-256 proof-of-work mining algorithm
  - costly electricity use and e-waste
  - ASICs and mining farms
- Scalability?

ETHEREUM

- Blockchain protocol for building decentralized, trustless applications (DAPPs)
- Goal: commodity hardware friendly (proof-of-stake)
  - Dagger Hashimoto mining algorithm
  - ASIC-resistant (IO bound)
  - light-client verifiable
- “Turing-complete” smart contracts
  - Ethereum virtual machine: internal state & computation
  - transactions costs: “gas” paid in Ether cryptocurrency token

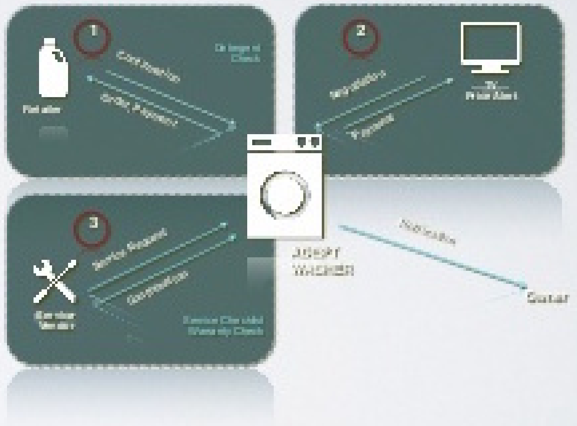
Smart Contract


Transactions
Sending value to the contract
Events
Sending information to the contract
"Smart Contract"
Value
State
Transactions
Sending value from the contract
Events
Sending information from the contract
Replicated, Shared Ledger

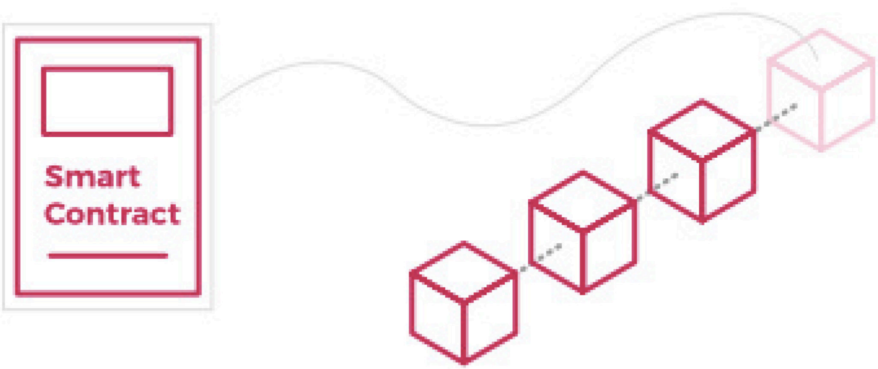
"A smart-contract is an event-driven program, with state, which runs on a replicated, shared ledger and which can take custody over assets on that ledger."

source: Richard Gendal Brown

- washer buying detergent
- washer bartering energy use
- washer ordering service



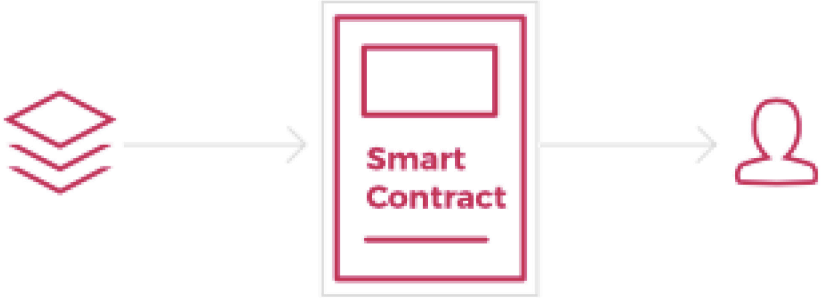
ujo MUSIC



Blockchain

Creators publish ownership information and use policies on the blockchain – a permanent and transparent string of transactions viewable and stored by everybody on the network.

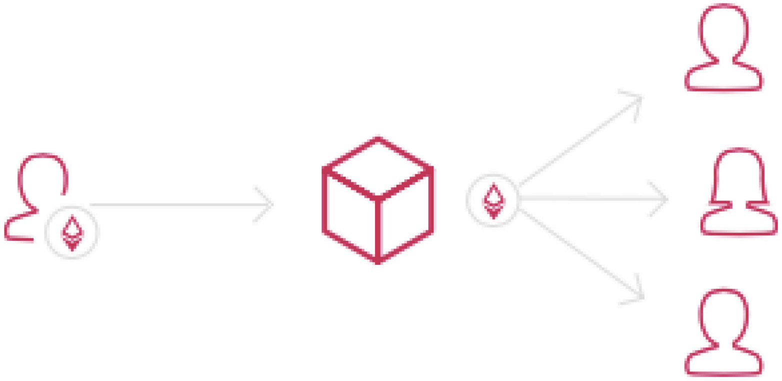
ujo MUSIC



Smart Contracts

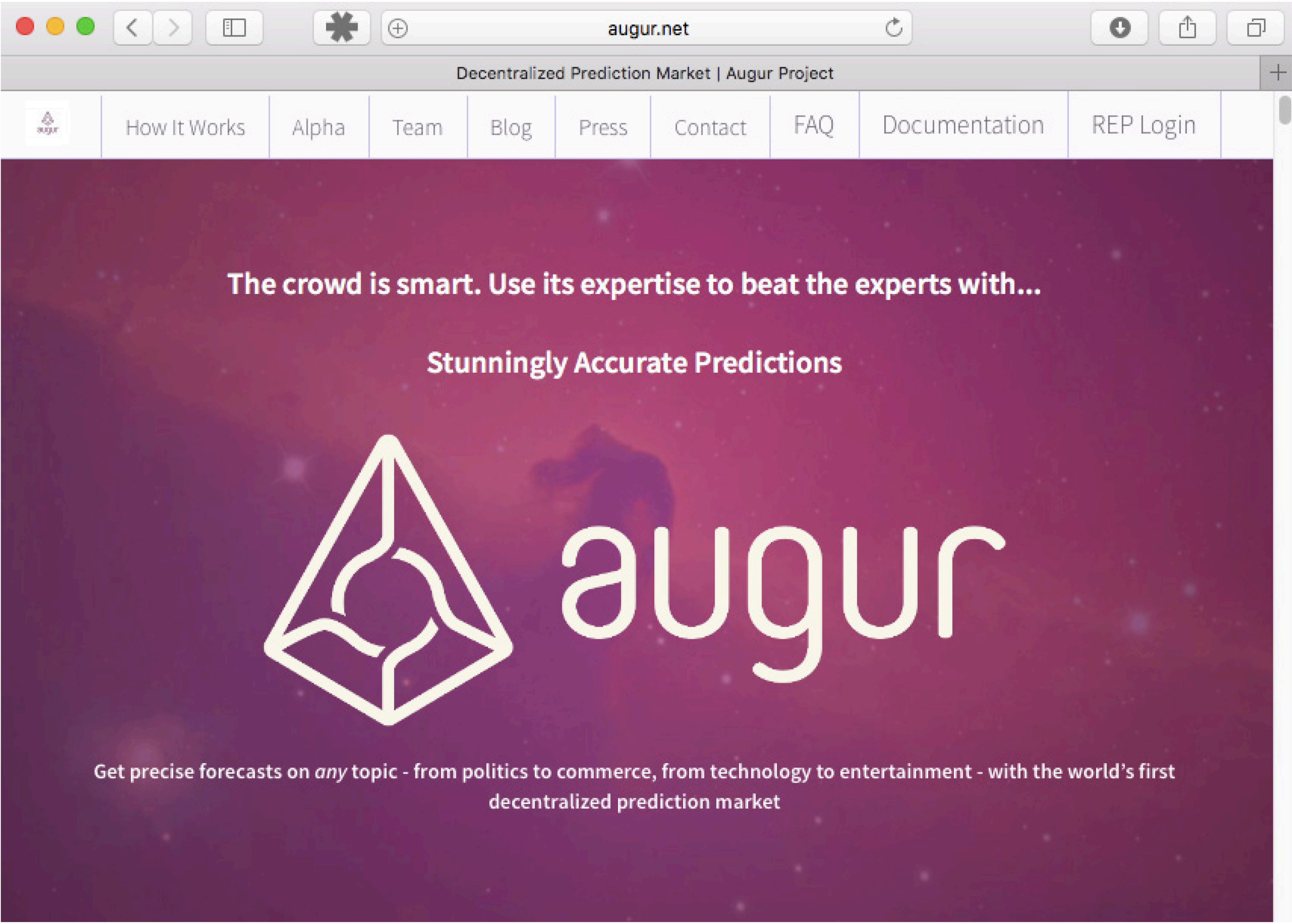
Anybody can use the registered content provided that they meet the terms of the policy. The right to do so is transferred automatically through a smart contract.

ujo MUSIC



Instant Payment

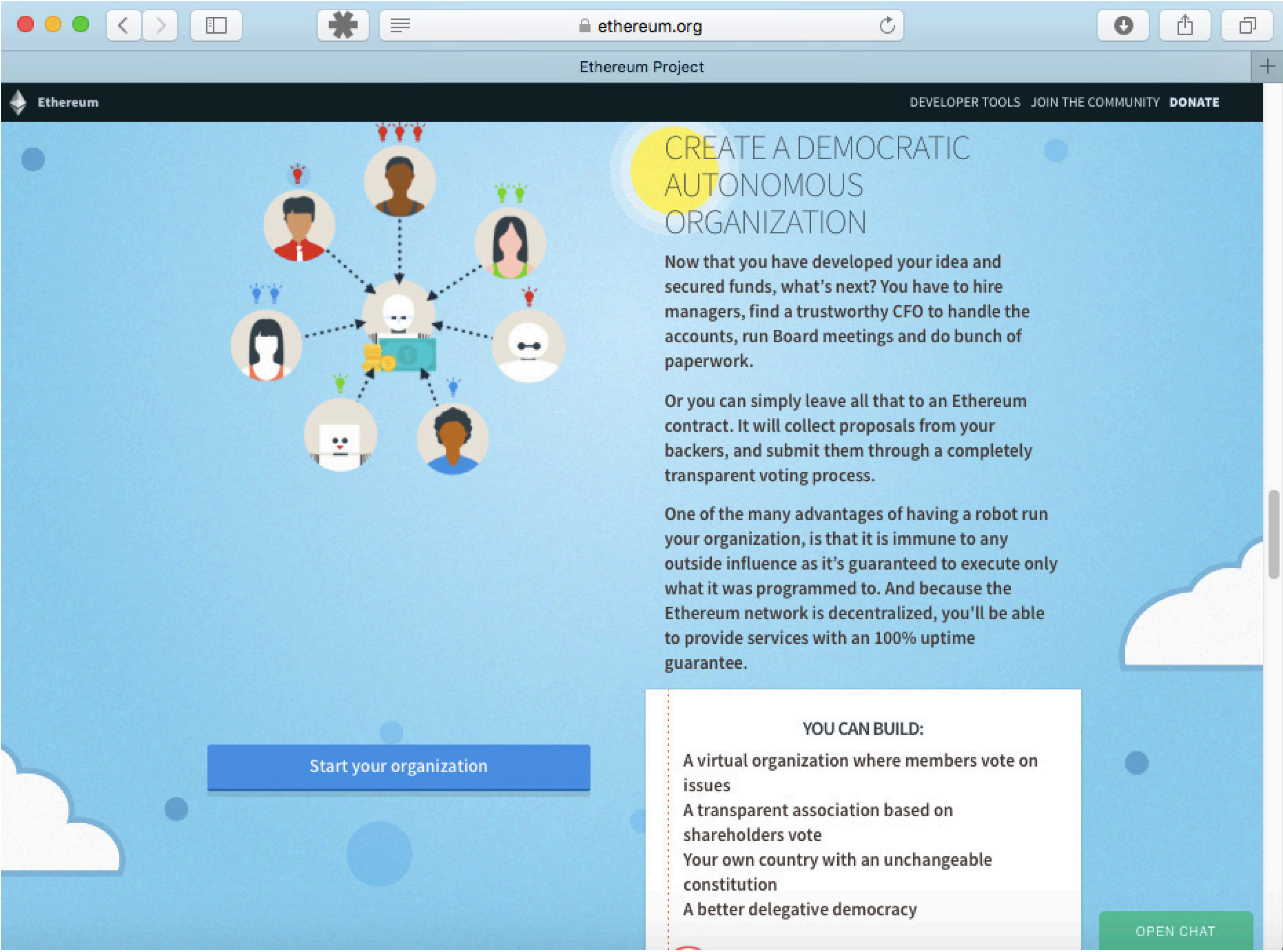
Payments are delivered to individual stakeholders instantly and automatically using digital currency, eliminating the need for intermediaries.



The crowd is smart. Use its expertise to beat the experts with...

Stunningly Accurate Predictions

Get precise forecasts on *any* topic - from politics to commerce, from technology to entertainment - with the world's first decentralized prediction market



CREATE A DEMOCRATIC AUTONOMOUS ORGANIZATION

Now that you have developed your idea and secured funds, what's next? You have to hire managers, find a trustworthy CFO to handle the accounts, run Board meetings and do bunch of paperwork.

Or you can simply leave all that to an Ethereum contract. It will collect proposals from your backers, and submit them through a completely transparent voting process.

One of the many advantages of having a robot run your organization, is that it is immune to any outside influence as it's guaranteed to execute only what it was programmed to. And because the Ethereum network is decentralized, you'll be able to provide services with an 100% uptime guarantee.

YOU CAN BUILD:

A virtual organization where members vote on issues

A transparent association based on shareholders vote

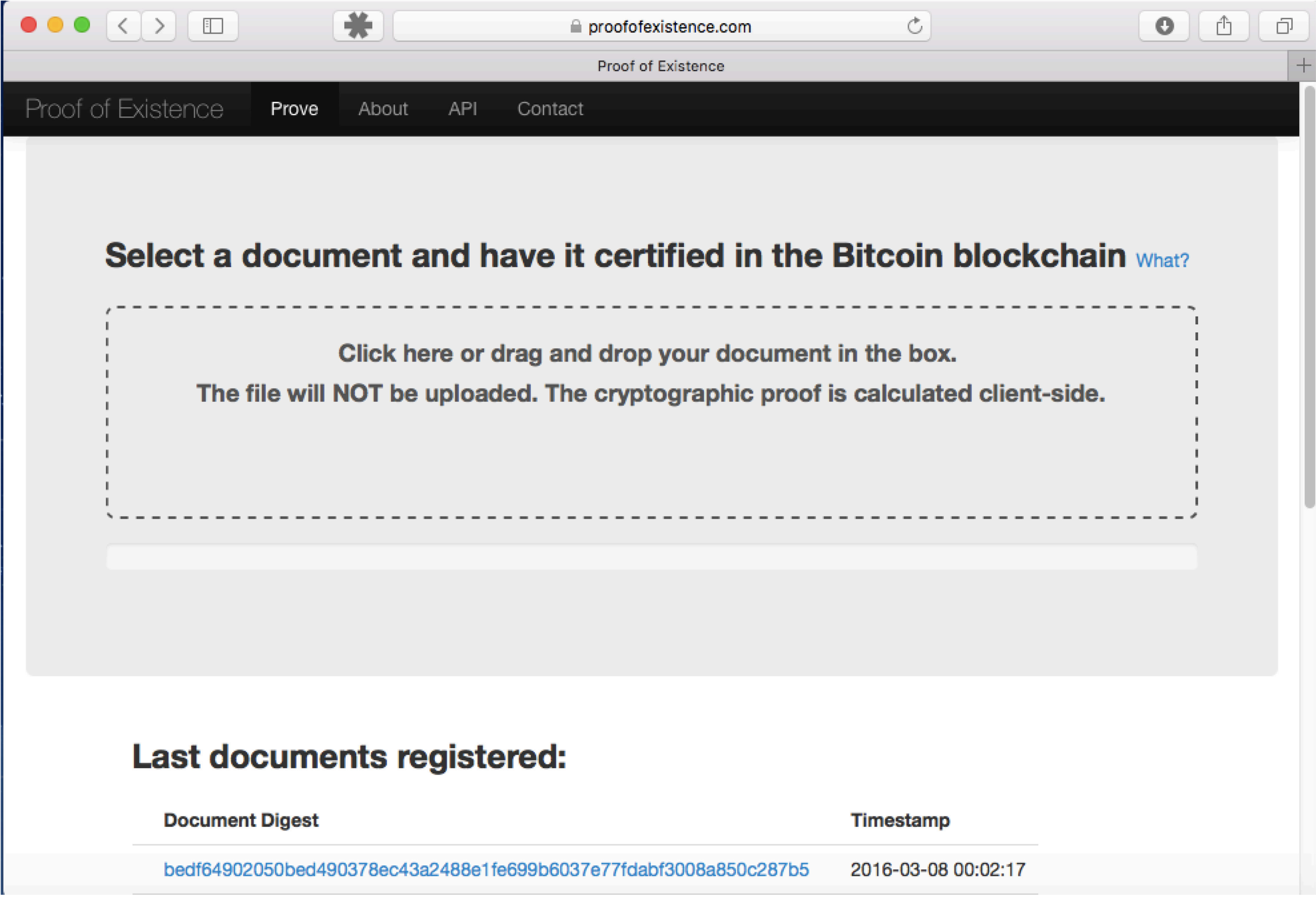
Your own country with an unchangeable constitution

A better delegative democracy

traditional record authenticity	blockchain record authenticity
• high cost	• low cost
• long delays	• quick turnaround
• permission granted	• permissionless
• trusted third-party	• trustless

Permissionless, trustless certification of authenticity

- Proof of existence
- Proof of presence
- Proof of process
- Proof of audit



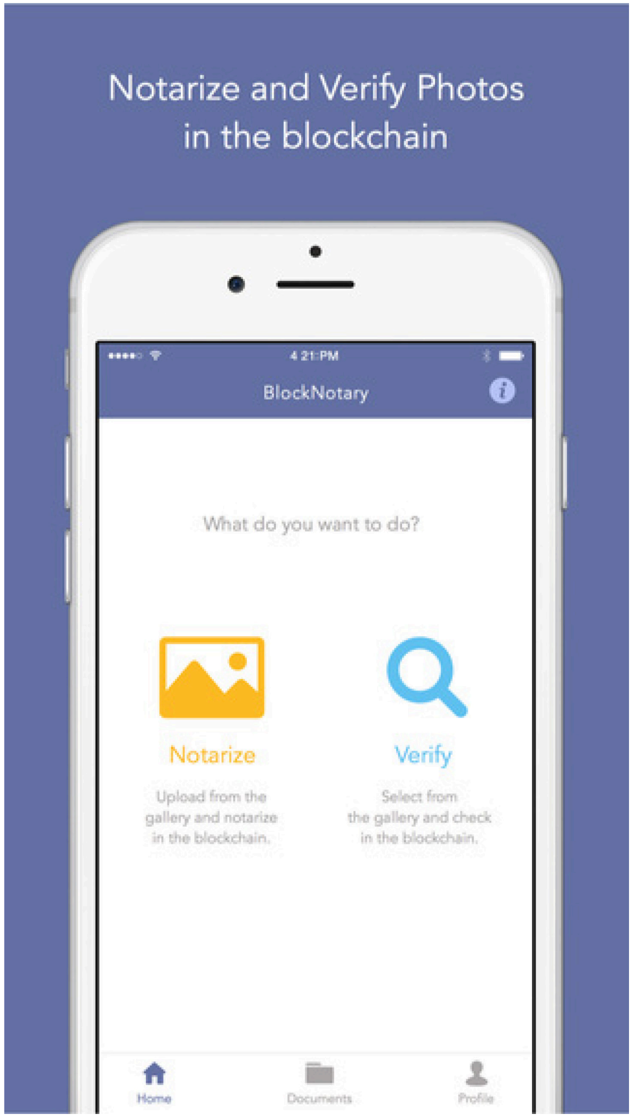
Select a document and have it certified in the Bitcoin blockchain What?

Click here or drag and drop your document in the box.
The file will NOT be uploaded. The cryptographic proof is calculated client-side.

Last documents registered:

Document Digest	Timestamp
bedf64902050bed490378ec43a2488e1fe699b6037e77fdabf3008a850c287b5	2016-03-08 00:02:17

blocknotary.com



Notarize and Verify Photos in the blockchain

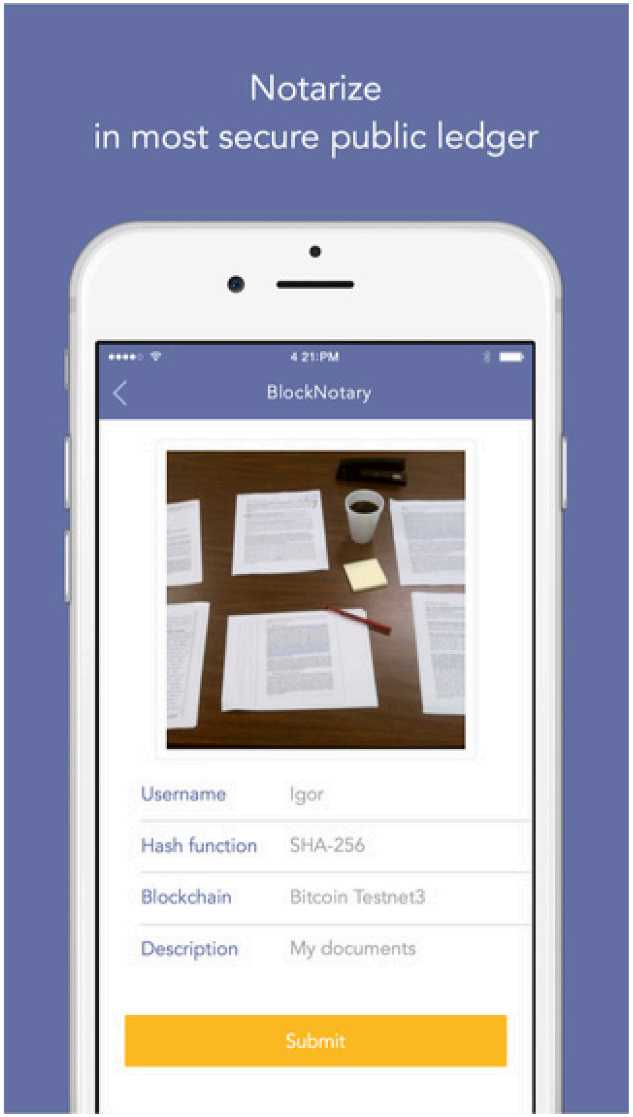
What do you want to do?

Notarize

Upload from the gallery and notarize in the blockchain.

Verify

Select from the gallery and check in the blockchain.



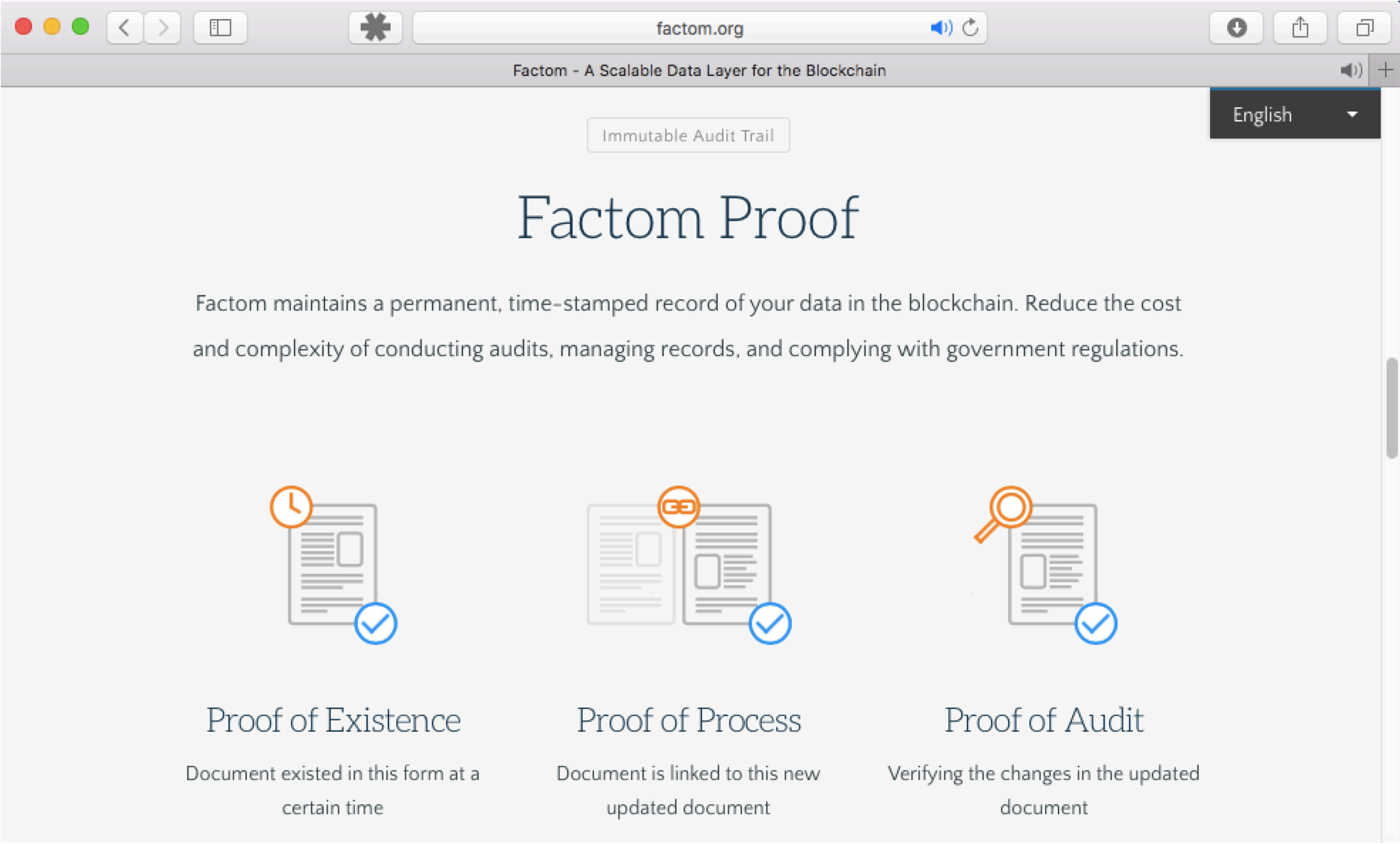
Notarize in most secure public ledger

Username Igor

Hash function SHA-256

Blockchain Bitcoin Testnet3

Description My documents



Immutable Audit Trail

Factom Proof

Factom maintains a permanent, time-stamped record of your data in the blockchain. Reduce the cost and complexity of conducting audits, managing records, and complying with government regulations.

Proof of Existence

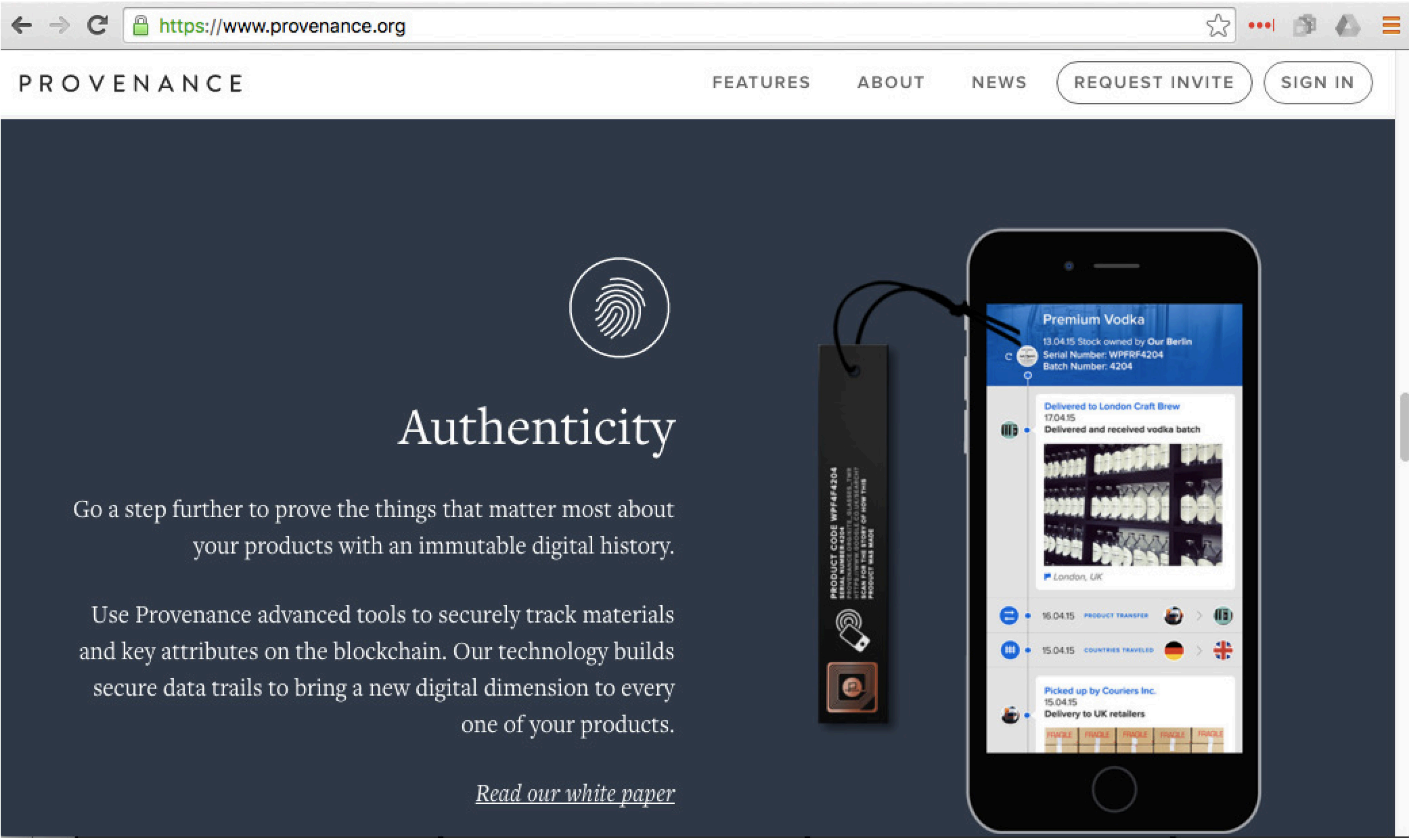
Document existed in this form at a certain time

Proof of Process

Document is linked to this new updated document

Proof of Audit

Verifying the changes in the updated document



Authenticity

Go a step further to prove the things that matter most about your products with an immutable digital history.

Use Provenance advanced tools to securely track materials and key attributes on the blockchain. Our technology builds secure data trails to bring a new digital dimension to every one of your products.

Read our white paper

PRODUCT CODE WPF4F4204
SERIAL NUMBER 4204
SCAN FOR THE STORY OF HOW THIS PRODUCT WAS MADE

Premium Vodka
13.04.15 Stock owned by **Our Berlin**
Serial Number: WPFRF4204
Batch Number: 4204

Delivered to London Craft Brew
17.04.15
Delivered and received vodka batch
London, UK

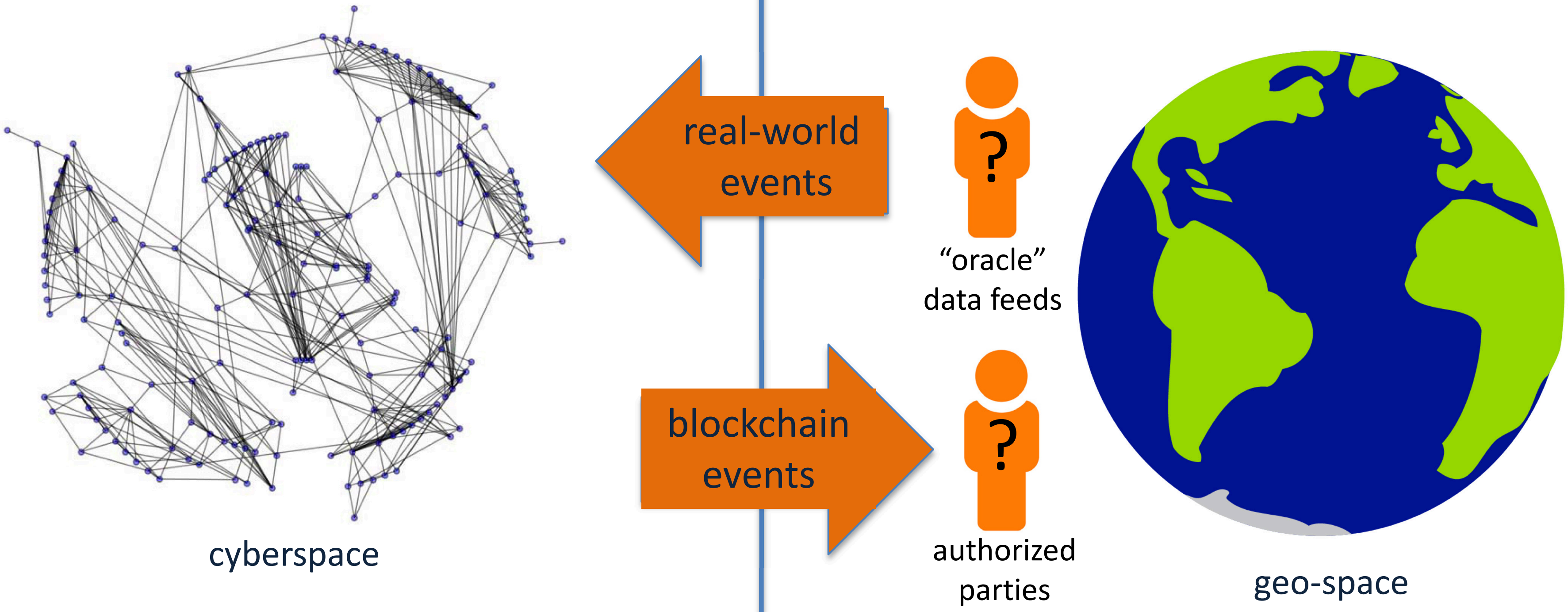
16.04.15 PRODUCT TRANSFER

15.04.15 COUNTRIES TRAVELED

Picked up by Couriers Inc.
15.04.15
Delivery to UK retailers

blockchain world

real world



real-world events

blockchain events

“oracle” data feeds

authorized parties

cyberspace

geo-space

including:

- chained blocks of data
- executable smart contracts
- mining and wallet clients
- blockchain explorers
- internet backbone
- off-blockchain data storage

including:

- 3D locations and objects
- people

time

source: Peter Van Garderen (2016) CC-BY