Bitcoin & Blockchain 101

Les bases d'une révolution décentralisée

Jonathan Hamel

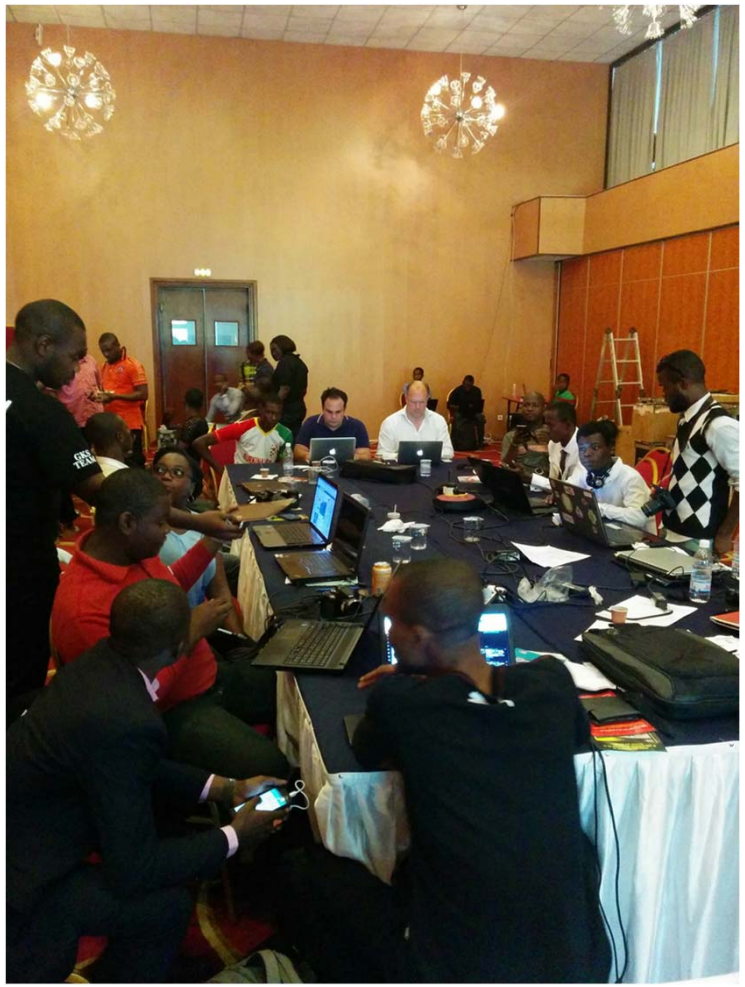
ISACA®
Fiabilisez, optimisez et rentabilisez les systèmes d'information
Section de Québec

Jonathan Hamel

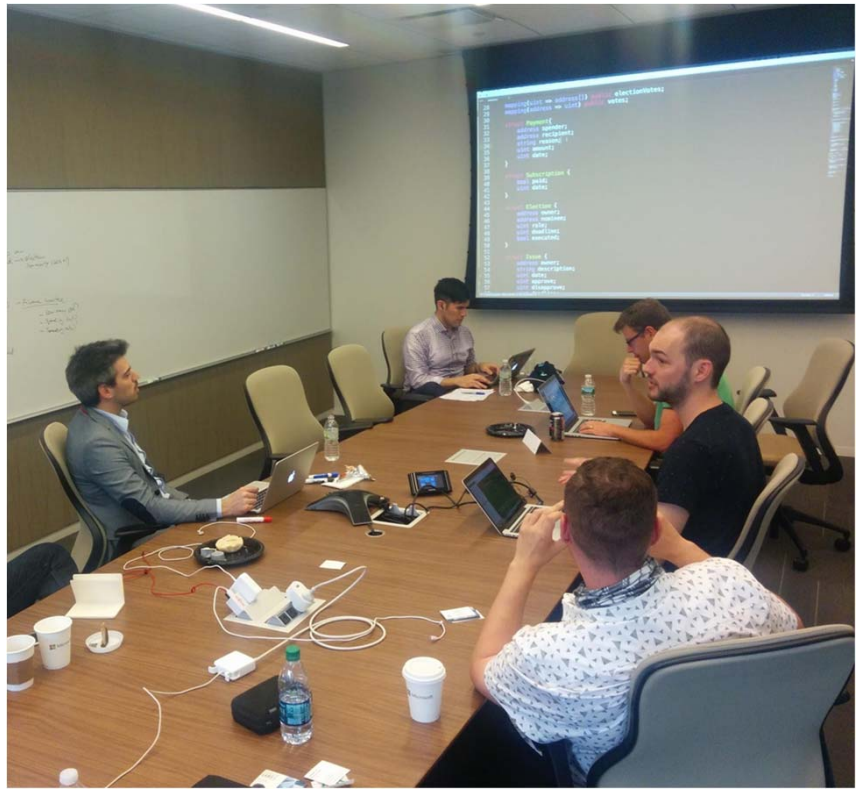
- Entrepreneur (Mobile, Payments) 1999 - 2015
- Formation IT, sécurité et réseautique (MCSE)
- Président et co-fondateur de Catallaxy
- Participe aux communautés Bitcoin (2013) et Ethereum (2014)
- Membre du comité consultatif Fintech de l'Autorité des Marchés Financiers
- Consultant spécialisé Bitcoin / Blockchain
- Forbes.com, HuffPost, P.Arthur Herald, Journal de Montréal, Radio X, Les Affaires, La Presse, The Gazette, Bloomberg, etc.


MAKE BITCOIN
GREAT AGAIN

Africa Web Festival (Abidjan, Côte-d'Ivoire)

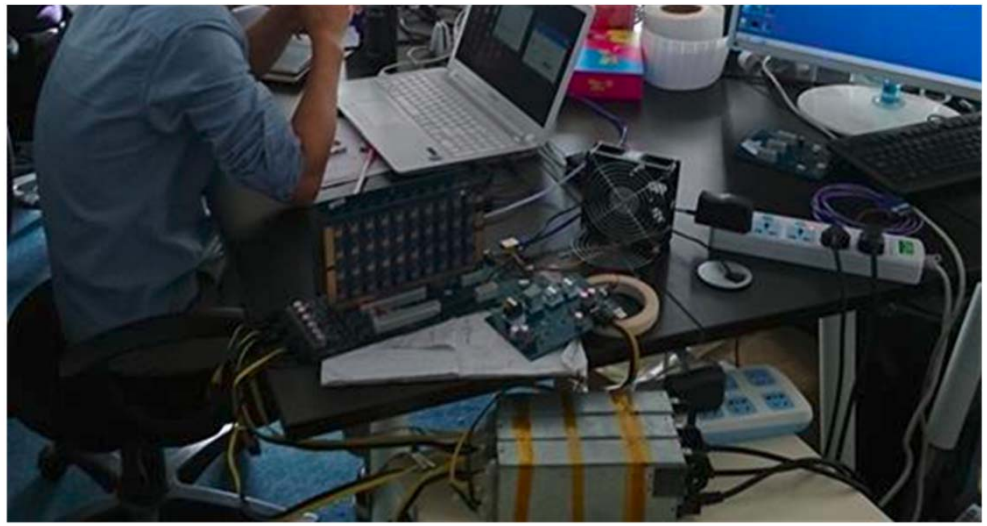


Consensus (New York, USA)



W.I.S.E. Summit (Doha, Qatar)

Shenzhen & Shanghai (Chine)



Au programme

- Qu’est-ce que Bitcoin?
- Histoire accélérée de Bitcoin
- Concepts clés
  - Cryptographie
  - Décentralisation
  - Blockchain
  - Mining
  - Économie et théorie des jeux
- Proposition de valeur de la Blockchain
- Cas d’utilisation concret
- Menaces et limitations actuelles
- Questions & Réponses

Qu’est-ce que Bitcoin?

“I do think Bitcoin is the first [encrypted money] that has the potential to do something like change the world."
- Peter Thiel

- Une vente pyramidale (“Ponzi Scheme”)
- Une entreprise commerciale
- Centralisée (aucune autorité derrière Bitcoin)
- Une technologie propriétaire (fermée)
- Monnaie
- Une conspiration globaliste

- ✓ Une technologie ouverte (open source)
- ✓ Un protocole informatique
- ✓ Un projet maintenu bénévolement
- ✓ Entièrement décentralisée
- ✓ Sécuritaire (cryptographie)
- ✓ La “Fintech” ultime

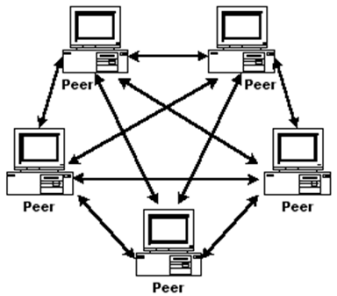
Projets similaires

- Linux
- TOR
- GIT
- Apache
- PGP
- BitTorrent

bitcoin

Principes fondamentaux

Open Source



Peer-to-Peer
(décentralisation)

Cryptographie

Libre marché

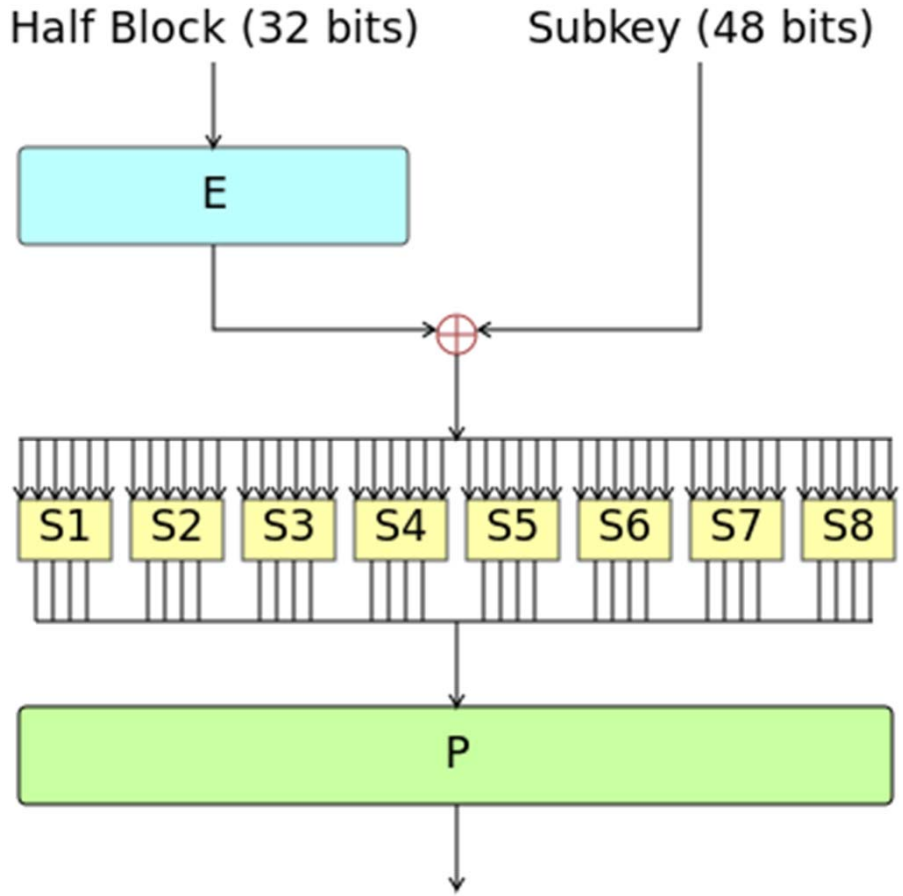
History of Bitcoin

“I see Bitcoin as ultimately becoming a reserve currency for banks, playing much the same role as gold did in the early days of banking. Banks could issue digital cash with greater anonymity and lighter weight, more efficient transactions.” - Hal Finney
- Peter Thiel

1975 DES

Data Encryption Standard

- Lancé par IBM
- Algorithme d'encryption clé symétrique
- Clé de 56 bits
- Non-sécuritaire aujourd'hui
- Début de l'ère cryptographie moderne

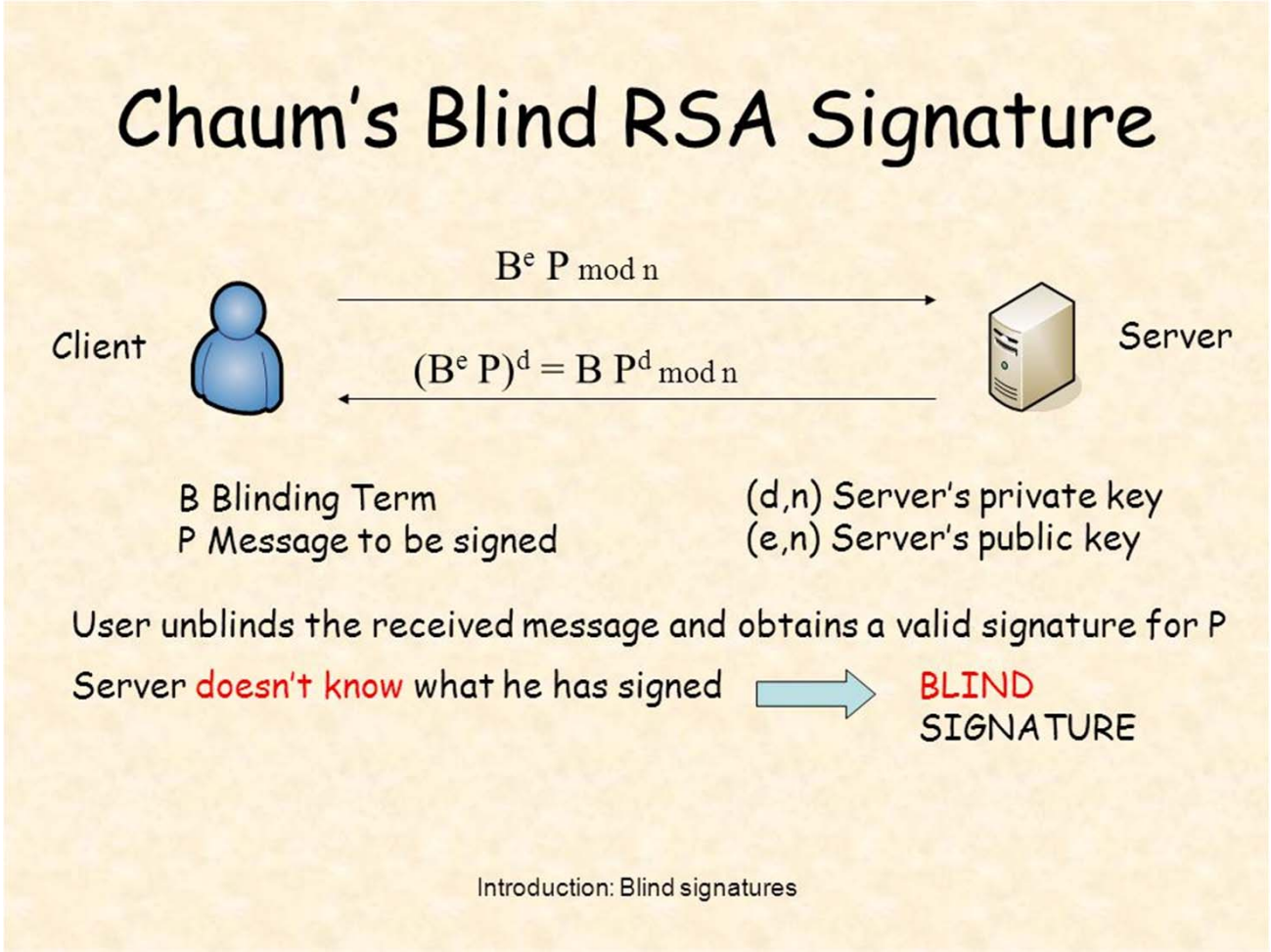


"in January 1999, distributed.net and the Electronic Frontier Foundation collaborated to ***publicly break a DES key in 22 hours and 15 minutes****"*

1983 Ecash

Par David Chaum

- Première monnaie numérique
- Blind Signature + clé publique RSA
- DigiCash Corporation : 1989 - 2002
- Utilisation commerciale limitée



80’s - 90’s

Cypherpunk Era

```
#!/bin/perl -sp0777i<X+d*lMLa^*lN%0]dsXx++lMlN/dsM0<j]dsj
$/=unpack('H*',$_);$_=`echo 16dio\U$k"SK$/SM$n\EsN0p[lN*1
lK[d2%Sa2/d0$^Ixp"|dc`;s/\W//g;$_=pack('H*',/((..)*)$/)
```

- Communauté informelle
  - Mathématiciens
  - Chercheurs
  - Ou simples enthousiastes
- Concepts clés
  - Cryptographie
  - Anonymité
  - Sécurisation des données (Data Privacy)
  - Désobéissance civile (U.S. crypto law 1996)
- Liste d’envoi (Mailing list)

“Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world.”

1997 HashCash

Par Adam Back

- Première implémentation du “Proof-of-Work”
- Pour contrer le SPAM et les DoS attacks
- Influence directe à Bitcoin (mining algorithm)
- SHA1 (vs. 2xSHA256 + Ripemd-160 Bitcoin)

```
X-Hashcash: 1:20:1303030600:adam@cypherspace.org::McMybZIhxKXu57jd:ckvi
```

The header contains:

- *ver*: Hashcash format version, 1 (which supersedes version 0).
- *bits*: Number of "partial pre-image" (zero) bits in the hashed code.
- *date*: The time that the message was sent, in the format `YYMMDD[hhmm[ss]]`.
- *resource*: Resource data string being transmitted, e.g., an IP address or email address.
- *ext*: Extension (optional; ignored in version 1).
- *rand*: String of random characters, encoded in base-64 format.
- *counter*: Binary counter (up to 2^{20}), encoded in base-64 format.

Blockstream

1997

b-money

Par Wei Dai

- Introduction du concept de “rareté”
- Introduction du concept de création de monnaie
- Influence directe à Bitcoin
- Wei Dai = Candidat possible Satoshi Nakamoto

1. The creation of money. ***Anyone can create money by broadcasting the solution to a previously unsolved computational problem.*** *The only conditions are that it must be easy to determine how much computing effort it took to solve the problem and the solution must otherwise have no value, either practical or intellectual.*

- Wei Dai, b-money Whitepaper

1998

bit-gold

Par Nick Szabo

- Précurseur directe de l’architecture Bitcoin
- Jamais implémenté (théorie seulement)
- Problème de centralisation non réglée
- Szabo : Candidature potentielle de Satoshi N.
- Est aussi derrière le concept du “Smart Contract”

2004

RPOW

Par Hal Finney

- RPOW : Reusable Proof-of-Work
- La pièce manquante au puzzle
- Premier receveur de Bitcoin (envoyé par SN)
- Premier opérateur d’une node Bitcoin (après SN)

2008

bitcoin: A Peer-to-Peer Electronic Cash System

Par Satoshi Nakamoto

- RPOW : Reusable Proof-of-Work
- Double-Hash (SHA-256 + Ripemd-160)
- Première implémentation du Blockchain
- Principe de difficulté de “mining” plus avancé
- 2008-2010 : Complètement dans l’ombre
- 2011 : Wikileaks accepte Bitcoin
- 2013 : sommet historique (1000 USD$+)***
- 2014 : MtGox : Crash
- 2017 : Sommet historique (1300 USD$ & 20G$)

From: Satoshi Nakamoto <satoshi <at> vistomail.com>
Subject: **Bitcoin P2P e-cash paper**
Newsgroups: **gmane.comp.encryption.general**
Date: 2008-10-31 18:10:00 GMT (4 years, 52 weeks, 1 day, 3 hours and 23 minu

```
I've been working on a new electronic cash system that's fully
peer-to-peer, with no trusted third party.

The paper is available at:
http://www.bitcoin.org/bitcoin.pdf

The main properties:
 Double-spending is prevented with a peer-to-peer network.
 No mint or other trusted parties.
 Participants can be anonymous.
 New coins are made from Hashcash style proof-of-work.
 The proof-of-work for new coin generation also powers the
    network to prevent double-spending.

Bitcoin: A Peer-to-Peer Electronic Cash System

Abstract.  A purely peer-to-peer version of electronic cash would
allow online payments to be sent directly from one party to another
without the burdens of going through a financial institution.
Digital signatures provide part of the solution, but the main
benefits are lost if a trusted 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 honest nodes control
the most CPU power on the network, they can generate the longest
chain and outpace any attackers.  The network itself requires
```

Fonctionnement de Bitcoin

“Bitcoin is a technological Tour de Force."

- Bill Gates

Concepts clés

- Cryptographie (clé publique et clé privée)
- Chiffrage (Hash)
- Décentralisation
- Mining
- Économie

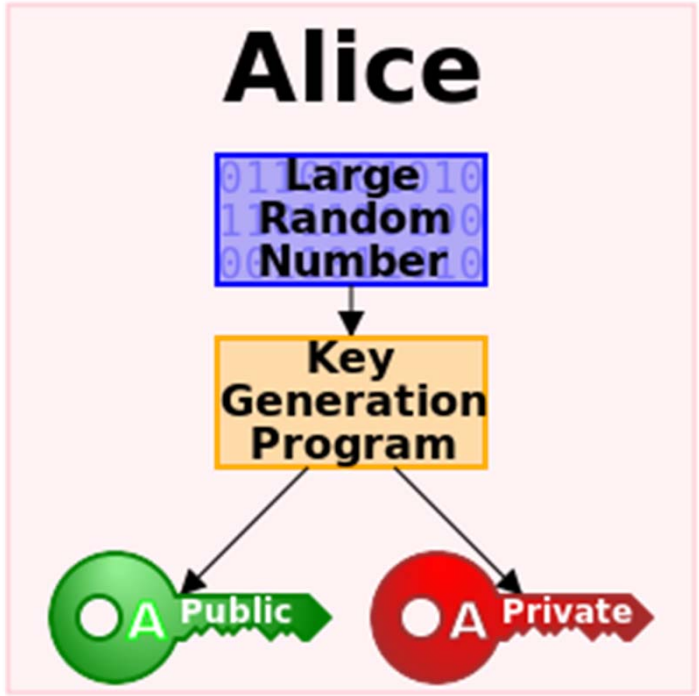
Cryptographie

Cryptographie

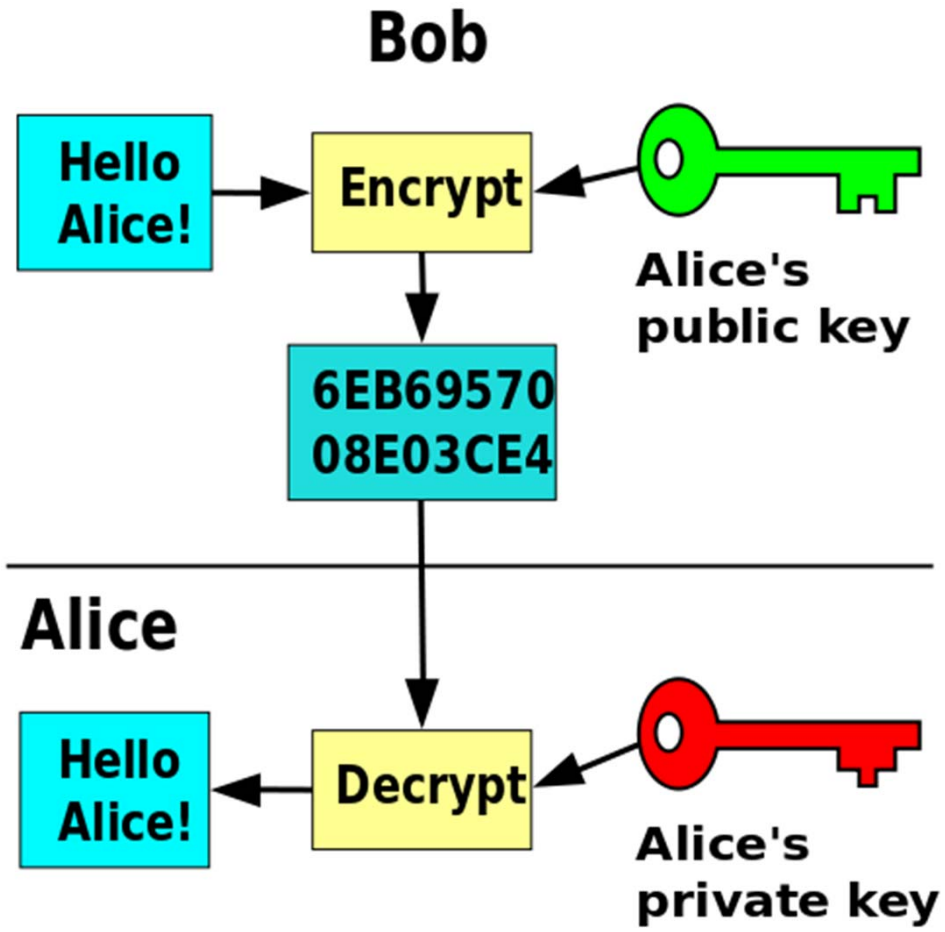
La cryptographie de Bitcoin **est révisée par des pairs (peer-reviewed) et considérée comme inviolable par la communauté scientifique**.

- **Bitcoin n'a jamais été piraté (...)**
- Même technologies d'encryption utilisées sur l'Internet commercial
  - ECDSA (Elliptic Curve Digital Signature Algorithm)
  - SHA256
  - RIPEMD-160

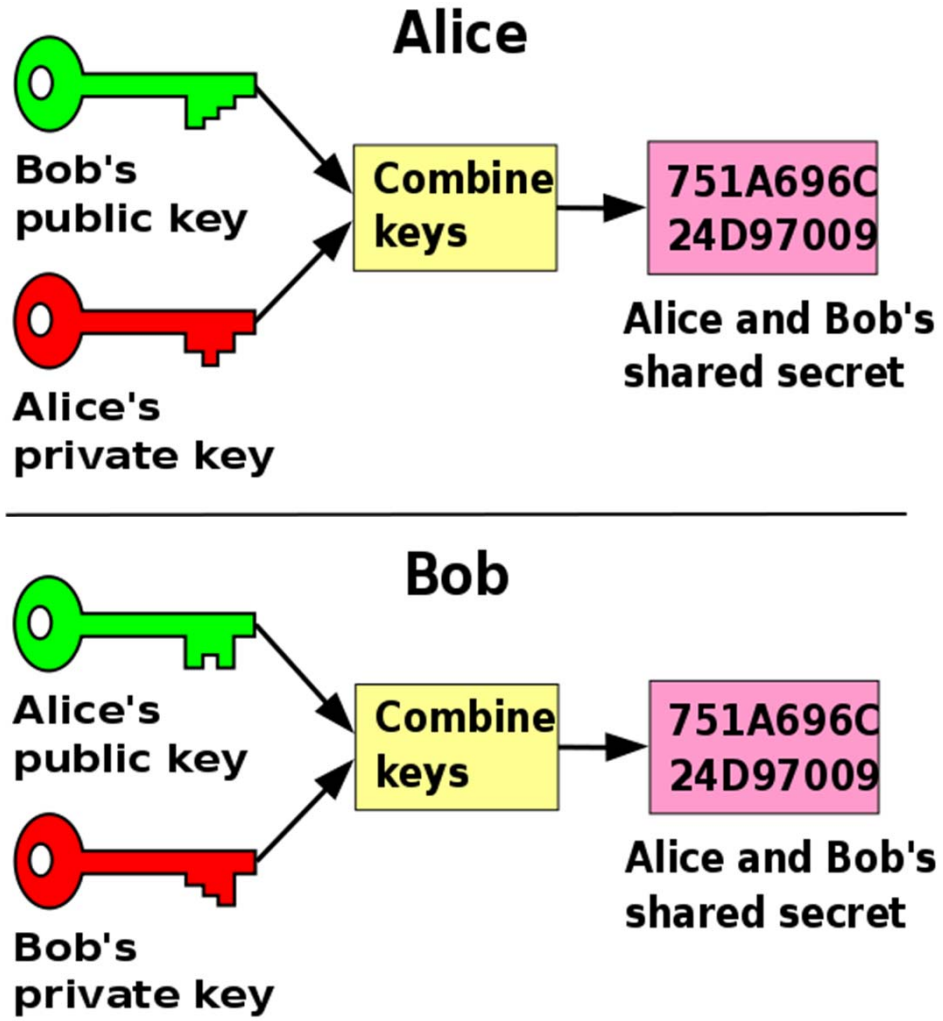
Architecture de clé publique et clé privée



Architecture de clé publique et clé privée

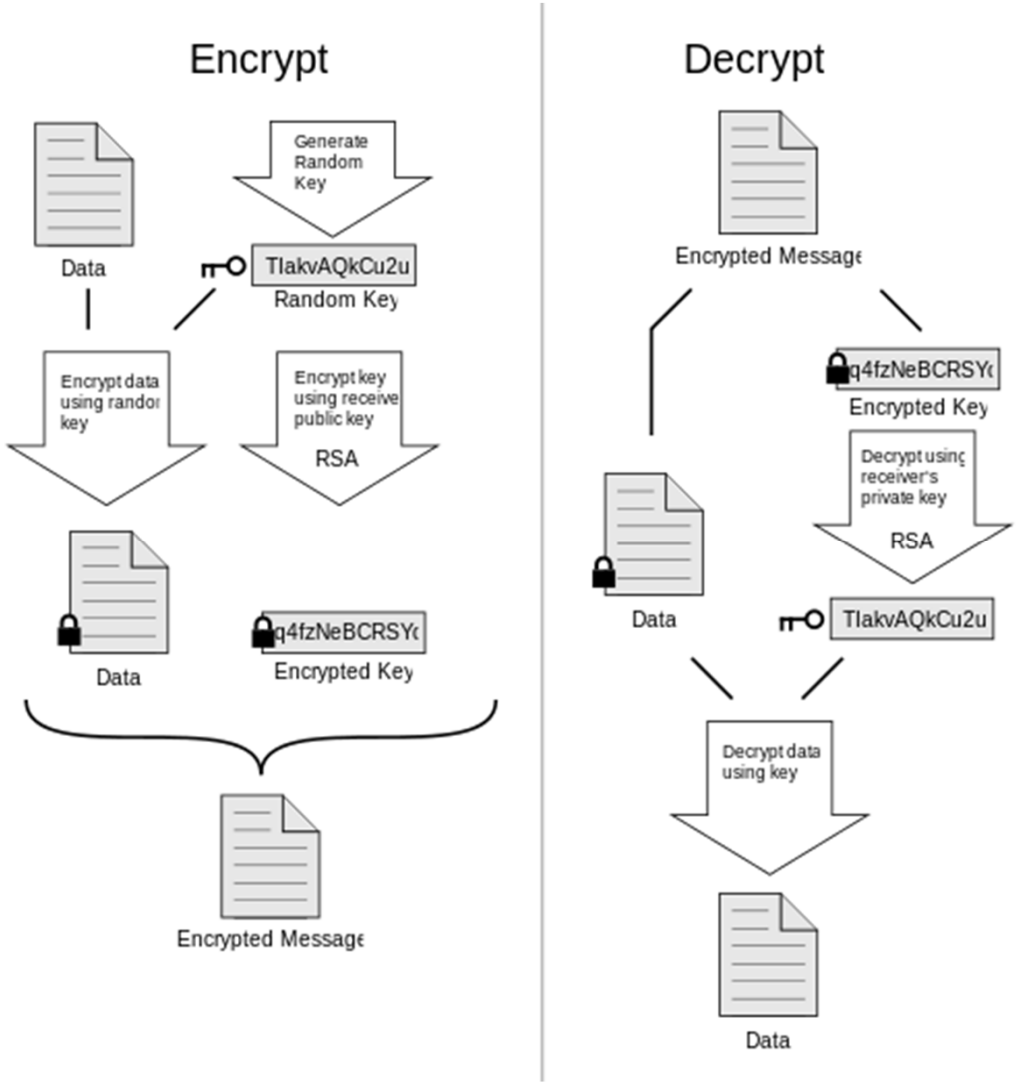


Architecture de clé publique et clé privée



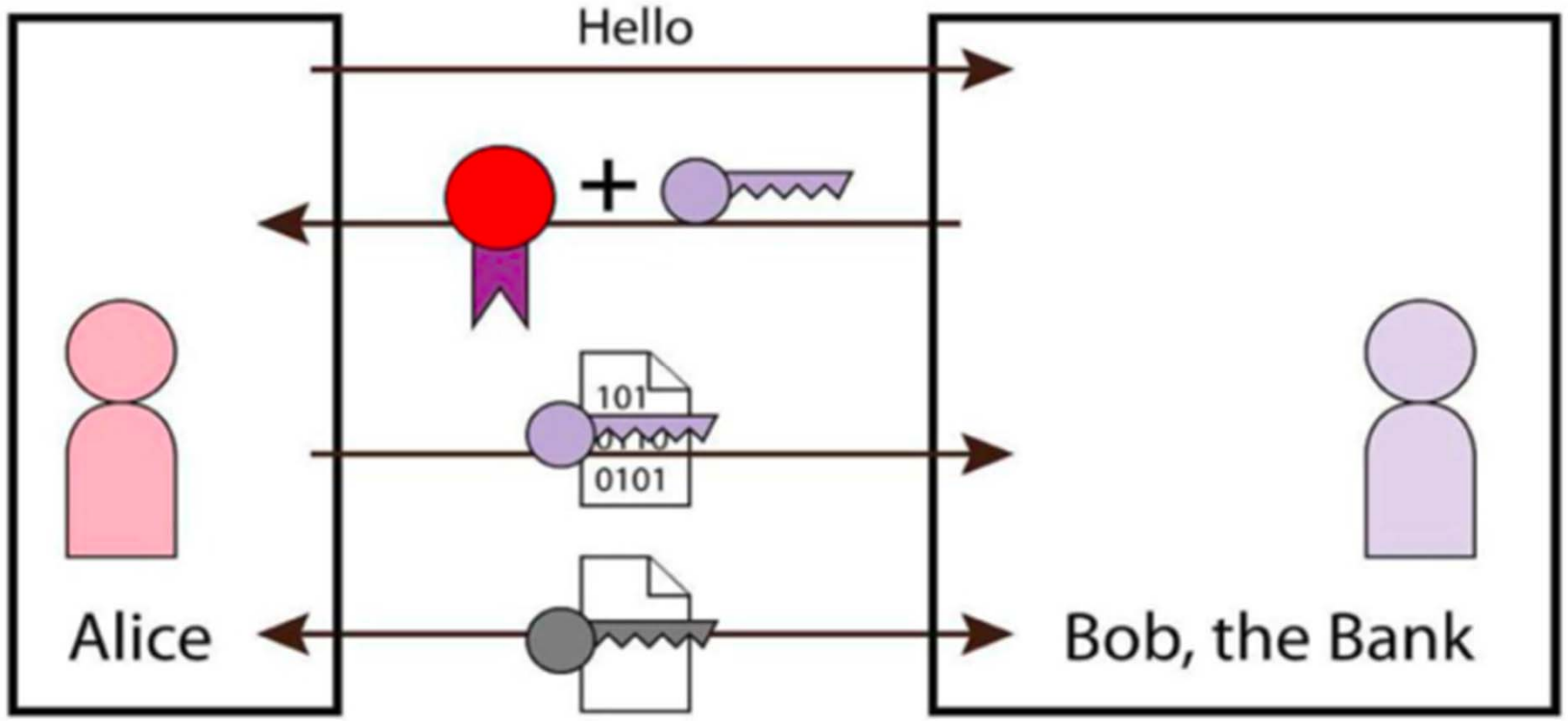
Architecture de clé publique et clé privée

PGP



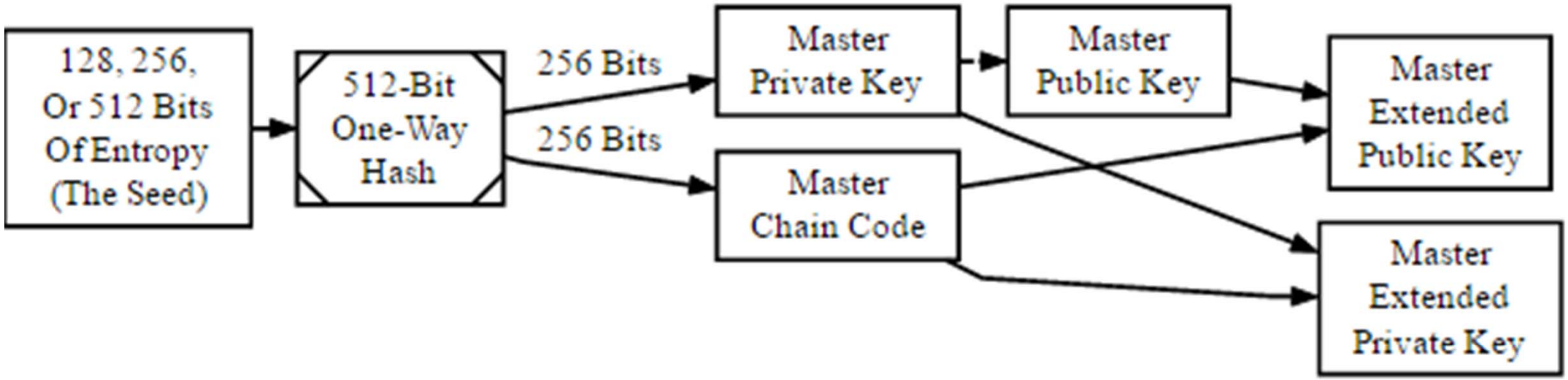
Architecture de clé publique et clé privée

SSL



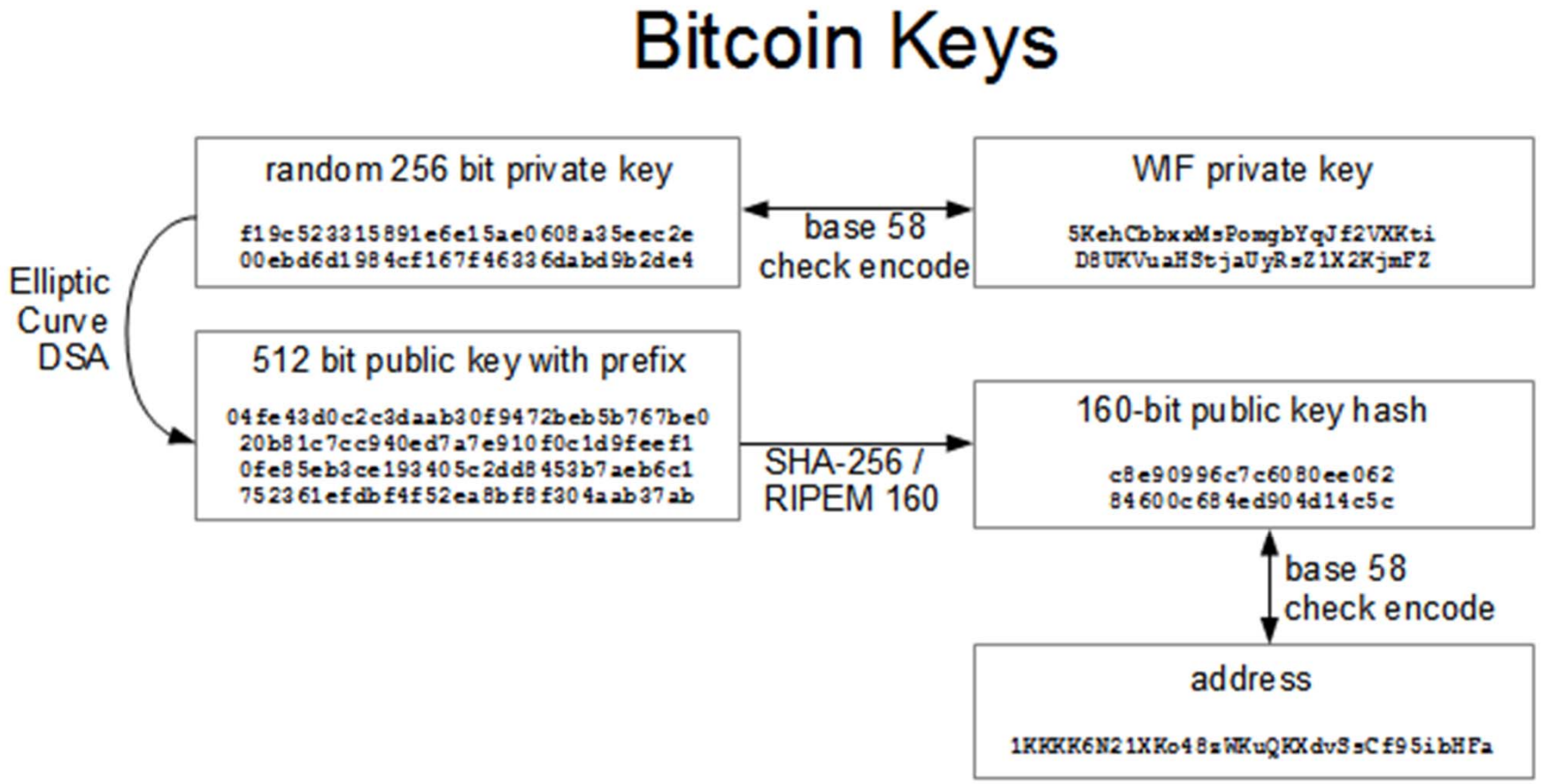
▲ Secure communication with SSL. Alice's browser verifies that Bob's certificate issigned by a trusted CA, then generates and encrypts a one-time public key.

Génération de la paire de clés Bitcoin



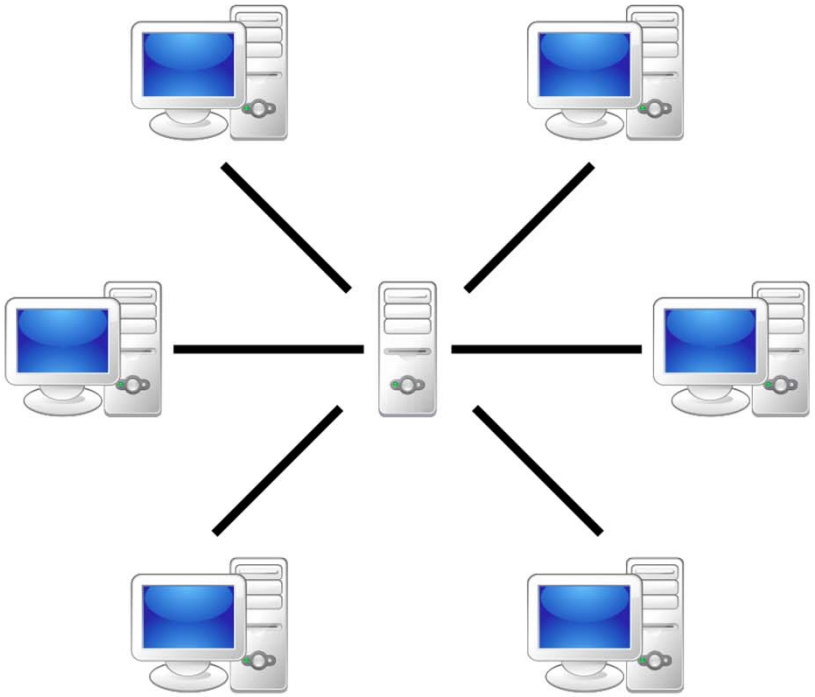
Creation Of The Master Keys

Génération de la paire de clés Bitcoin

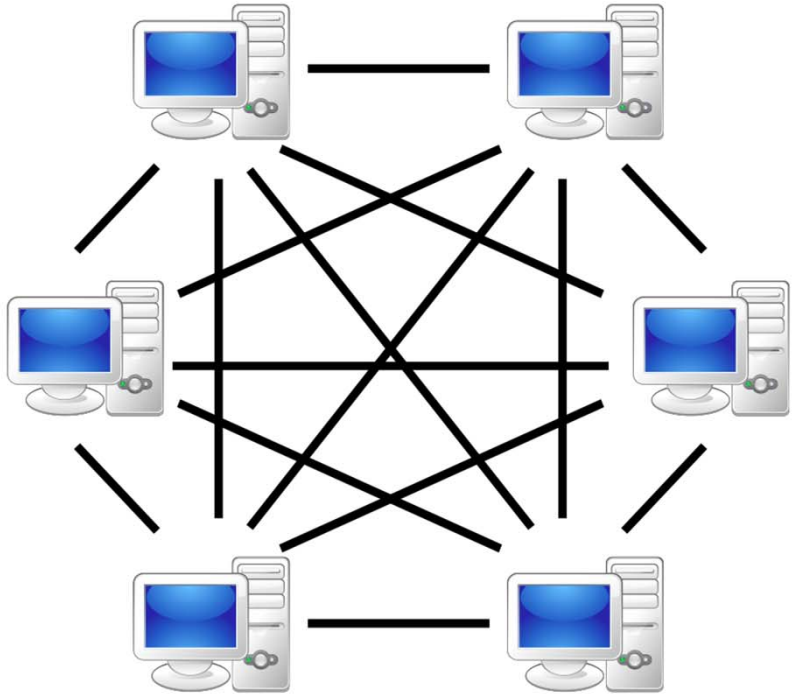


Réseau Bitcoin

Décentralisation

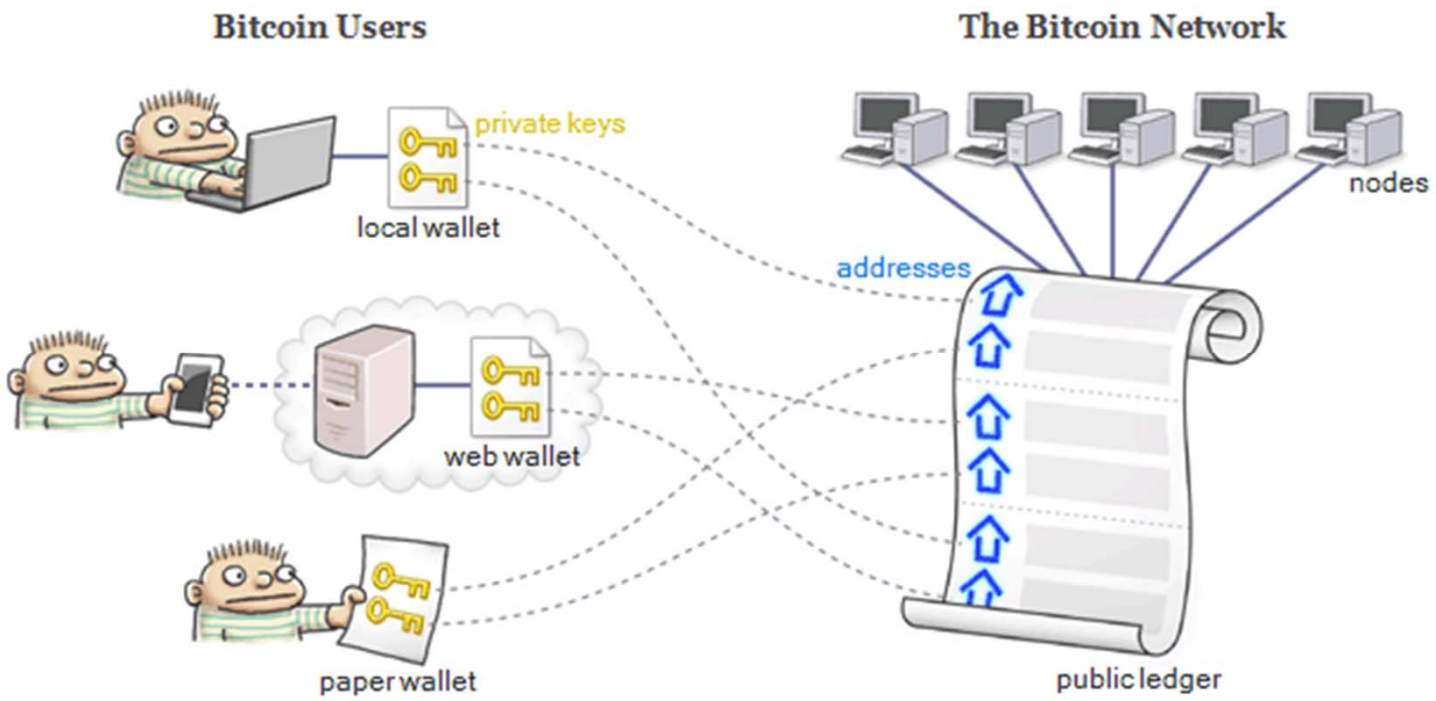


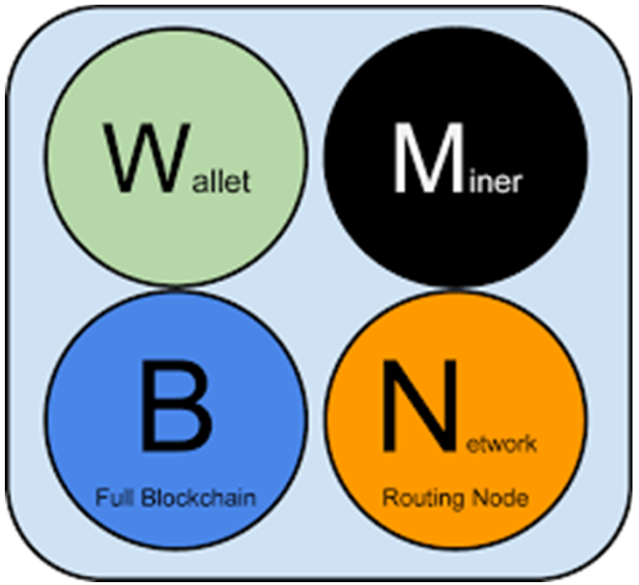
Server-based



P2P-network

Décentralisation





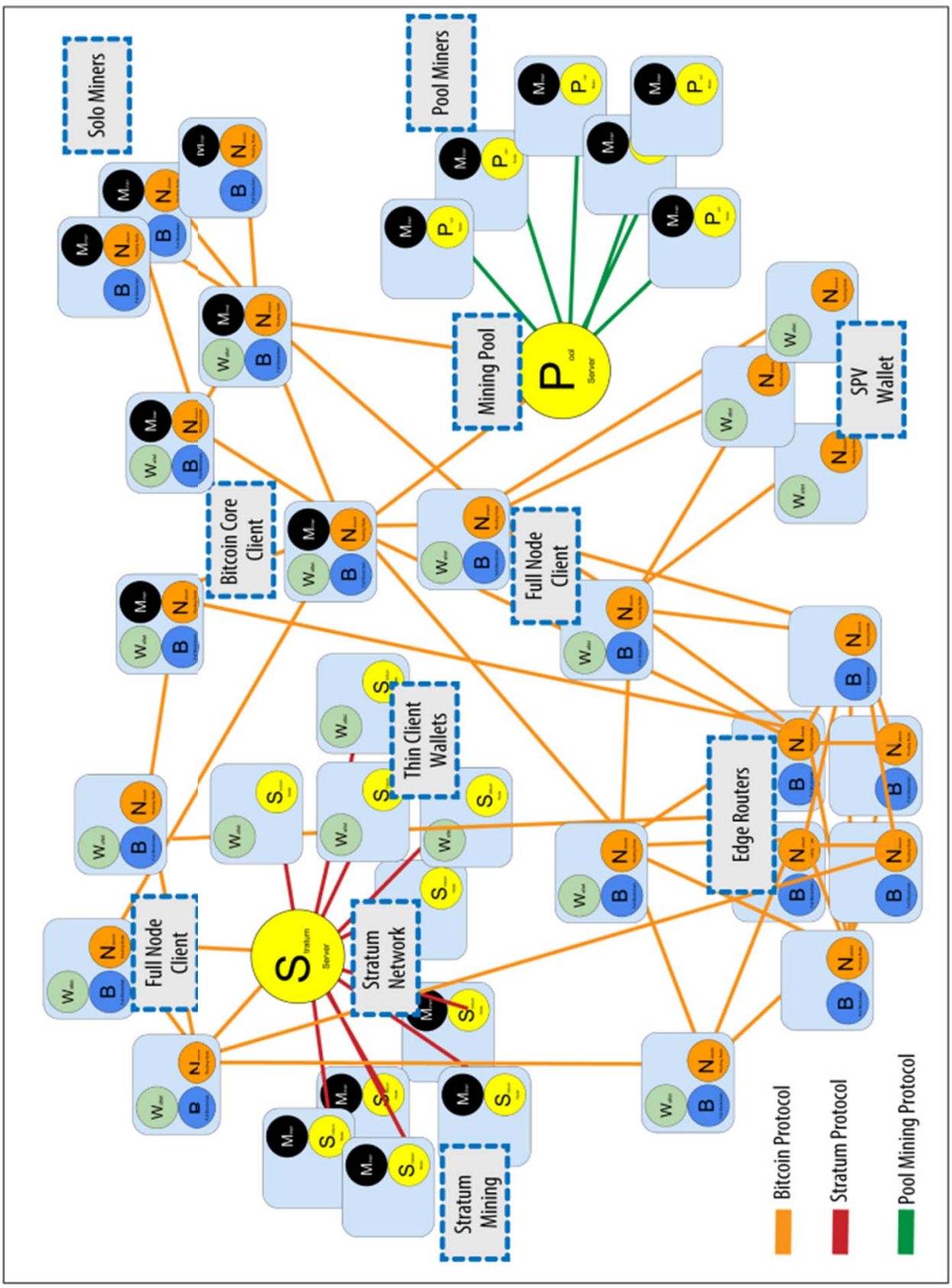


Figure 6-3. The extended bitcoin network showing various node types, gateways, and protocols

Note sur la décentralisation…

La plus grandes avancées de la race humaine sont décentralisées

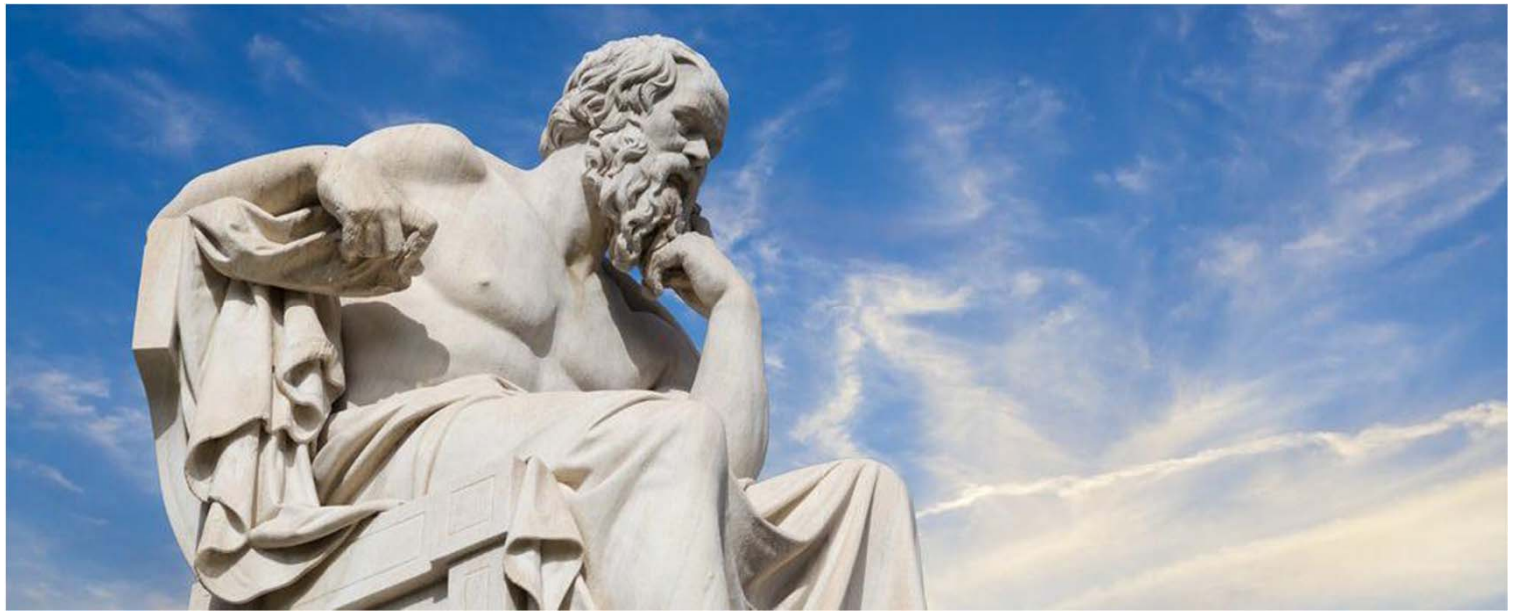
$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Mathématiques

La plus grandes avancées de la race humaine sont décentralisées

Langage

La plus grandes avancées de la race humaine sont décentralisées



Philosophie

Transaction Bitcoin

Comptes (Addresses) avec un solde

LEDGER

Account owner	Value
Mary	4
John	56
Sandra	83
Lisa	16
David	187
Brian	23
…	…

Transaction Bitcoin = Mise à jour du “Ledger”

BITCOIN TRANSACTION REQUEST MESSAGE

“David sends 5 BTC to Sandra”

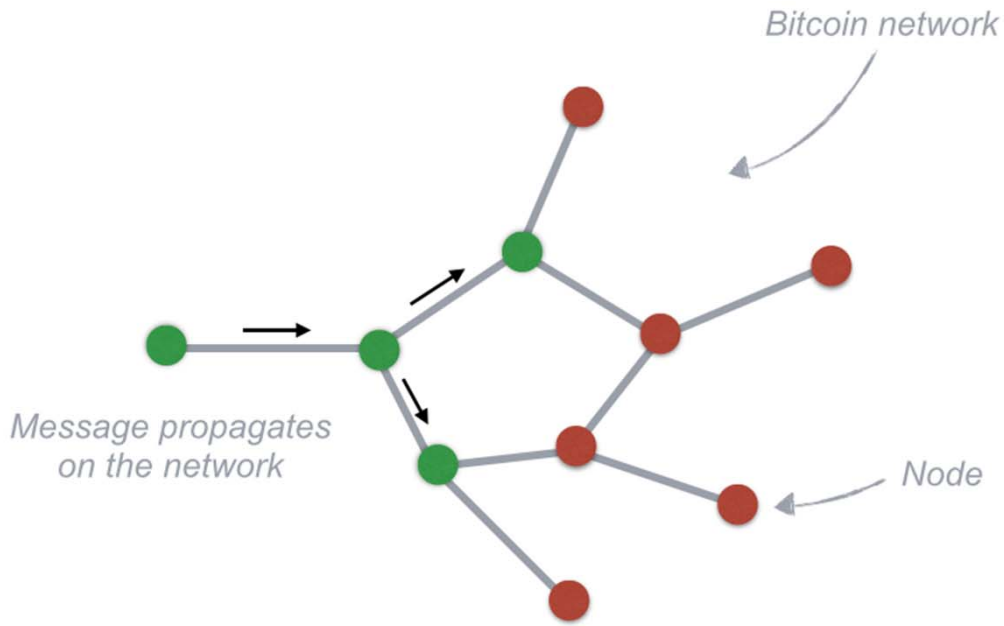
David → Sandra 5 BTC

LEDGER

Account owner	Value
Mary	4
John	56
Sandra	83
Lisa	16
David	187
Brian	23

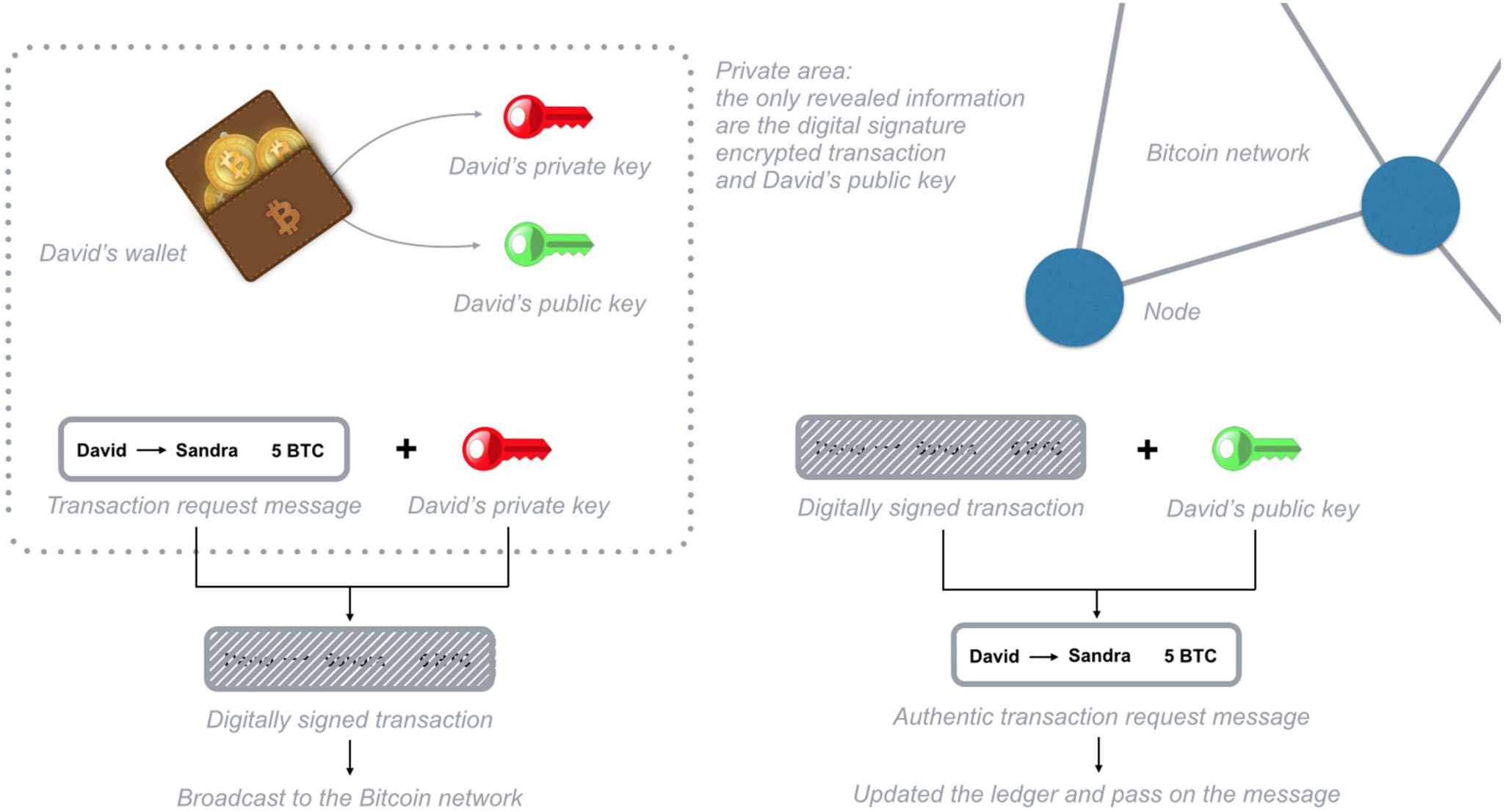
LEDGER

Account owner	Value
Mary	4
John	56
Sandra	88
Lisa	16
David	183
Brian	23



Each *node* receives the transaction request message,
updates its own copy of the *ledger*
and passes on the message to the nearby *nodes.*

Clé publique / Clé privée



UTXO : Unspent Transaction Outputs

Simplified transaction request

Inputs

Previous output	Amount	From address	Signature
n278cojci…1	3.451	Sandra's address	fuw93v2…c3
m8nd53hd…1	6.334	Brian's address	a56fbsuc…s8
cn3792m…1	0.14	Lisa's address	lfue82mc…id
u4her83n…1	2.193	David's address	jwc7fks8…2a

Outputs

Redeemed input	Amount	To address	Signature
j3s8b30f…if	2.118	Mary's address	k732cne…21
ks2f9ms7…j3	10	John's address	87fckwlo…k4

Real transaction request structure

UTXO : Unspent Transaction Outputs

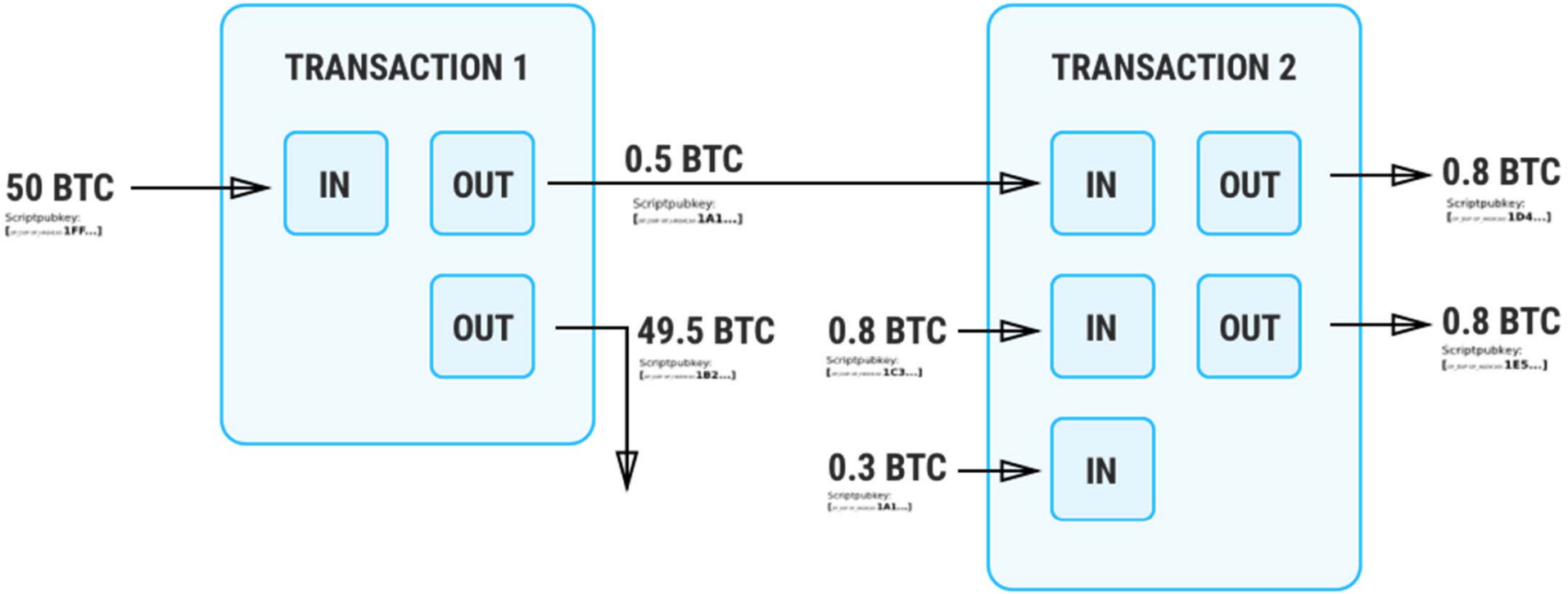


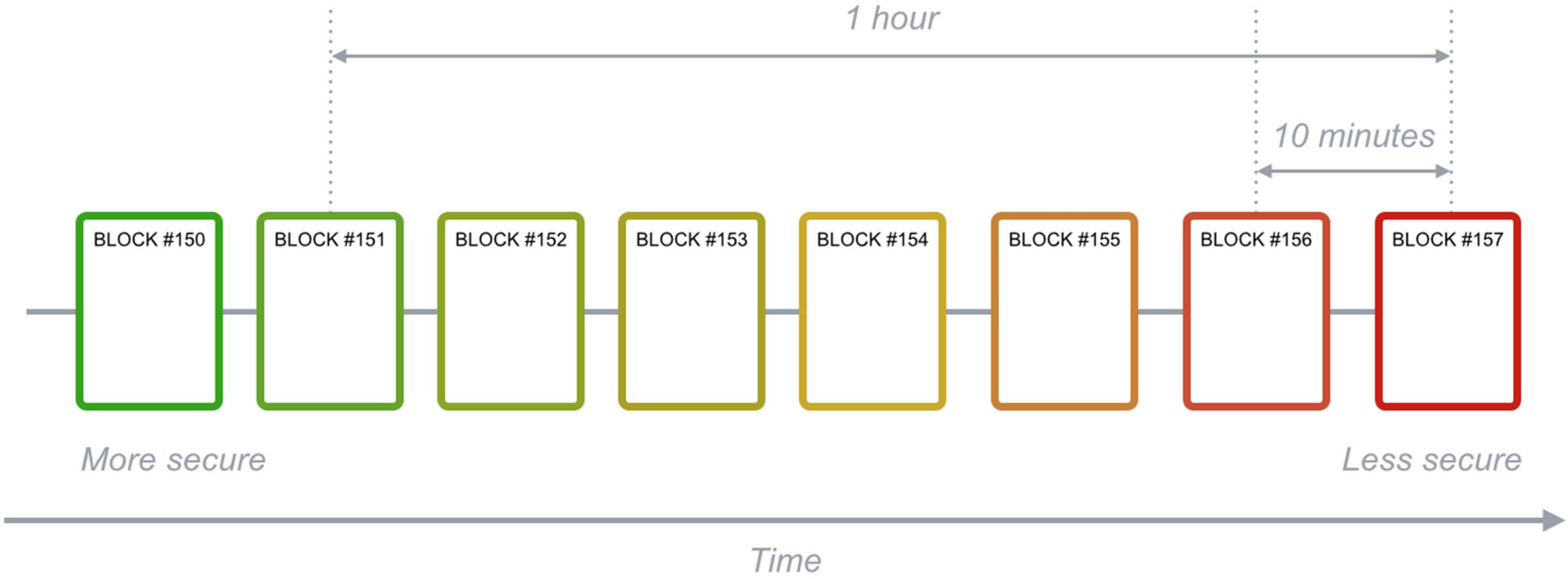
Figure 4 - The UTXO or Unspent Transaction Outputs Model

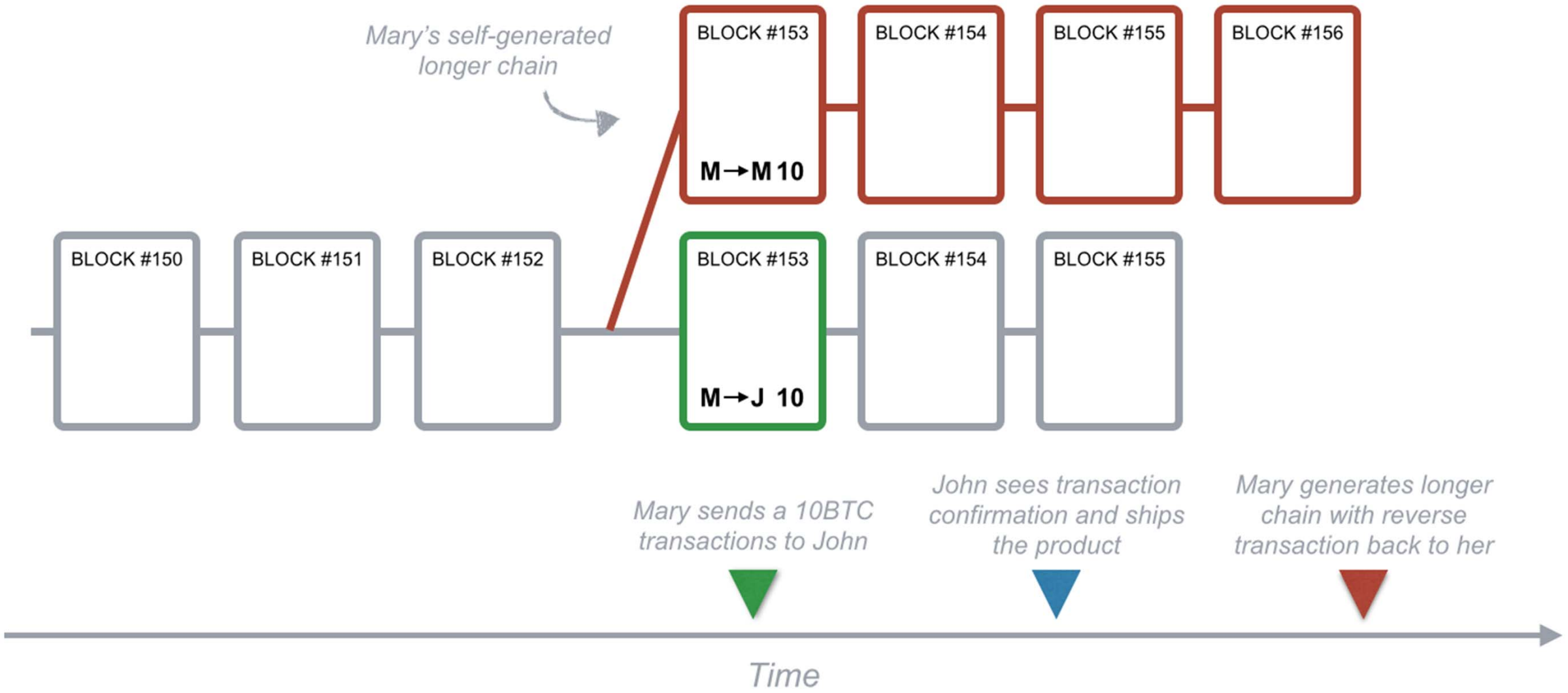
Blockchain

La Blockchain

- Est le produit (la conséquence) du consensus Bitcoin
- **N’est pas une technologie en soi**
- Nécessite plusieurs éléments clés pour fonctionner
  - Consensus (Décentralisation + incitatif)

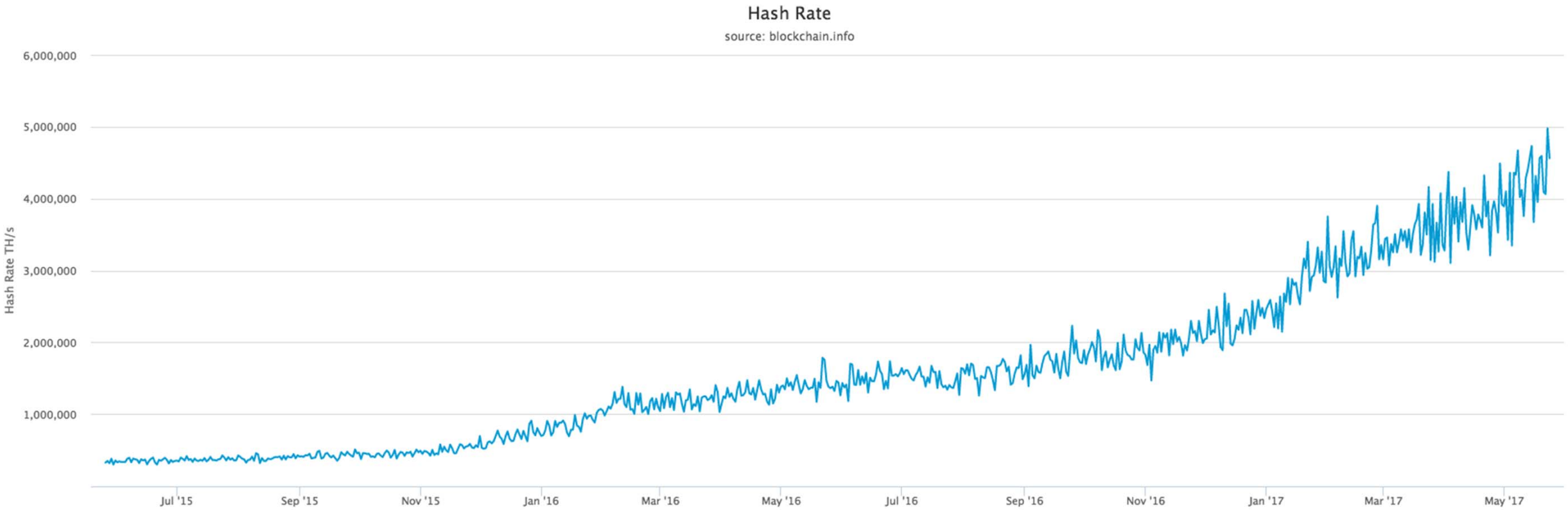
- Grand livre (“ledger”) distribué et décentralisé
- **<u>Chaine de transactions ancrées dans le temps</u>**
- Cryptographie ET réseau P2P (décentralisation)


1 hour
10 minutes
BLOCK #150
BLOCK #151
BLOCK #152
BLOCK #153
BLOCK #154
BLOCK #155
BLOCK #156
BLOCK #157
More secure
Less secure
Time

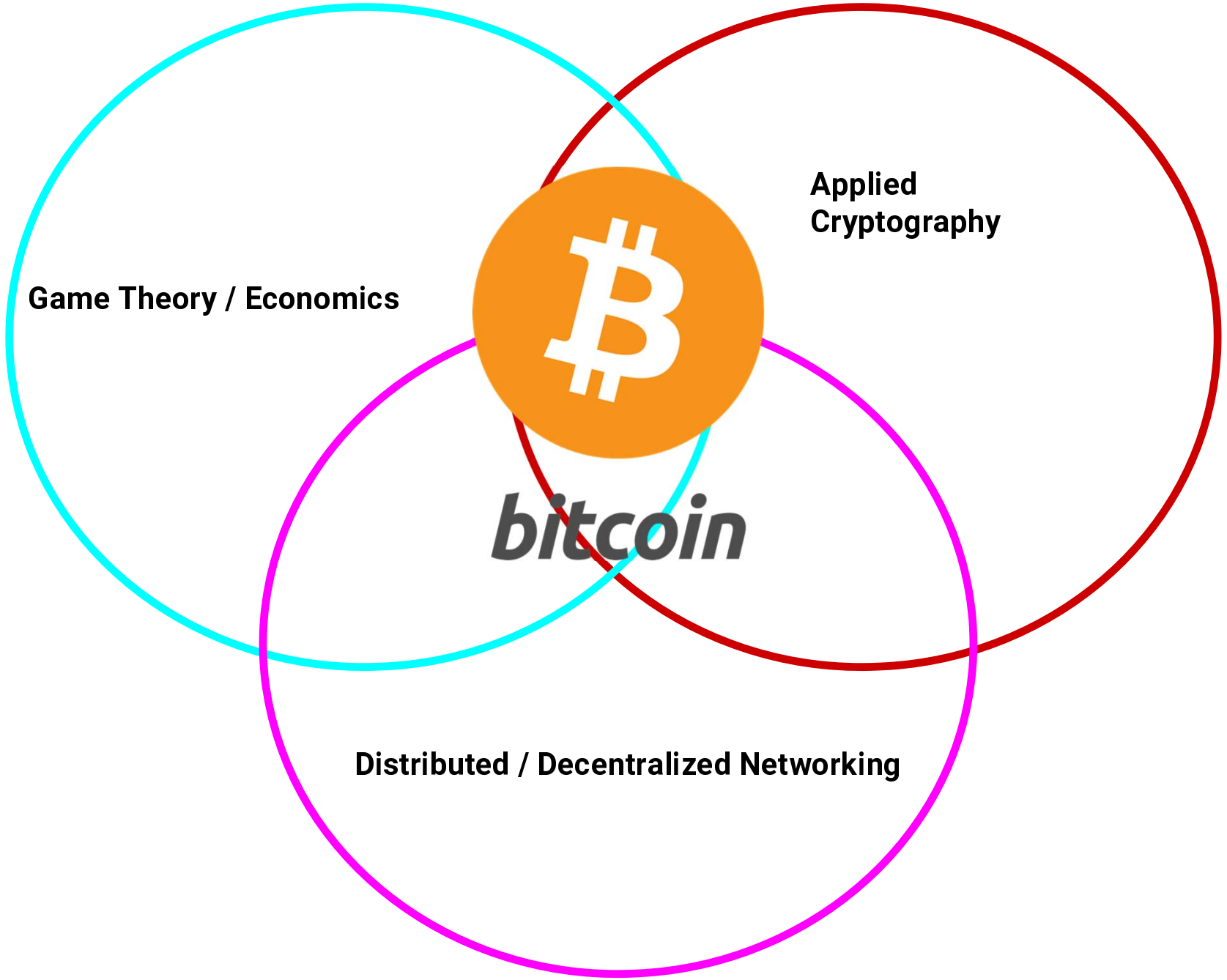

Mary's self-generated longer chain
BLOCK #153
M→M 10
BLOCK #154
BLOCK #155
BLOCK #156
BLOCK #150
BLOCK #151
BLOCK #152
BLOCK #153
M→J 10
BLOCK #154
BLOCK #155
Mary sends a 10BTC transactions to John
John sees transaction confirmation and ships the product
Mary generates longer chain with reverse transaction back to her
Time

Mining

CPU MINING < GPU Mining < ASIC Mining


Hash Rate
source: blockchain.info
Hash Rate TH/s
6,000,000
5,000,000
4,000,000
3,000,000
2,000,000
1,000,000
Jul '15
Sep '15
Nov '15
Jan '16
Mar '16
May '16
Jul '16
Sep '16
Nov '16
Jan '17
Mar '17
May '17

Pourquoi ça fonctionne?


Game Theory / Economics
Applied
Cryptography
bitcoin
Distributed / Decentralized Networking

Fondements économiques

“The one thing that’s missing, but that will soon be developed, is a reliable e-cash, a method whereby on the Internet you can transfer funds from A to B, without A knowing B or B knowing A.”

- Milton Friedman (1999)

Qu’est-ce qui fait une monnaie efficace?

- Rareté
- Non-consommable / Non-Périssable
- Portable
- Fungible et divisible
- Reproduction difficile

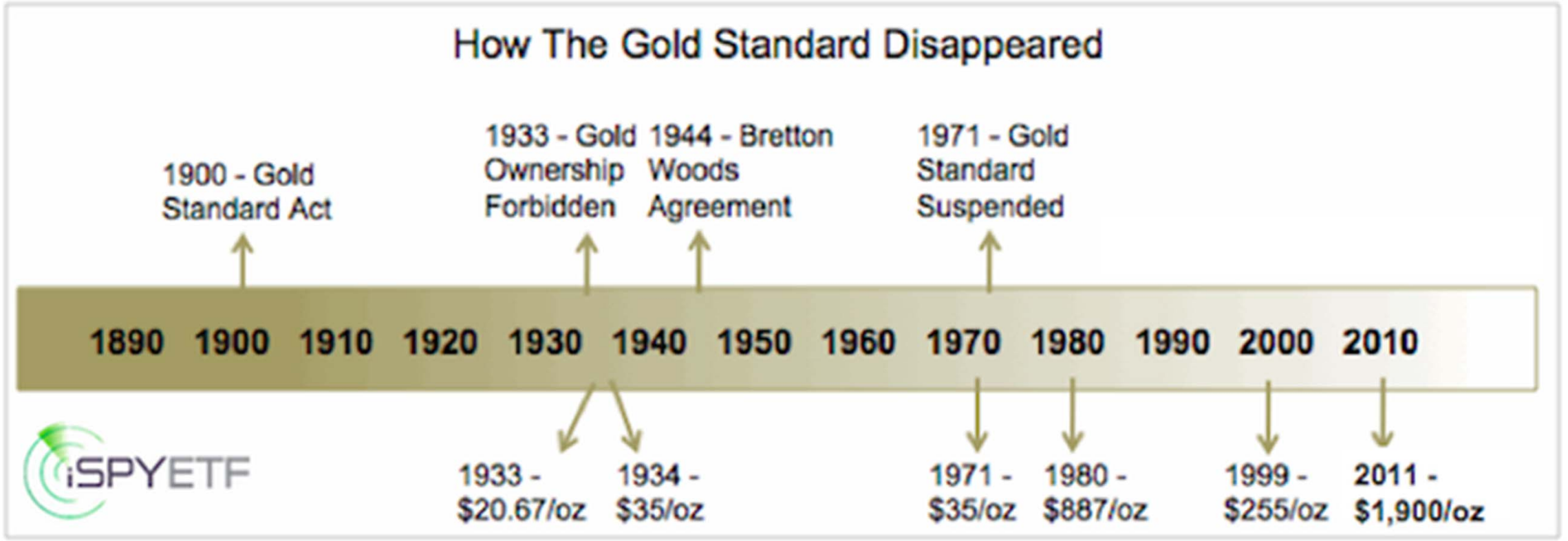
Feathers, shells, beads

Gems, precious metals, coins

Money Today

PAST

PRESENT


How The Gold Standard Disappeared
1900 - Gold Standard Act
1933 - Gold Ownership Forbidden
1944 - Bretton Woods Agreement
1971 - Gold Standard Suspended
1890 1900 1910 1920 1930 1940 1950 1960 1970 1980 1990 2000 2010
iSPYETF
1933 - $20.67/oz
1934 - $35/oz
1971 - $35/oz
1980 - $887/oz
1999 - $255/oz
2011 - $1,900/oz

POSTMASTER: PLEASE POST IN A CONSPICUOUS PLACE.—JAMES A. FARLEY, Postmaster General

UNDER EXECUTIVE ORDER OF THE PRESIDENT

Issued April 5, 1933

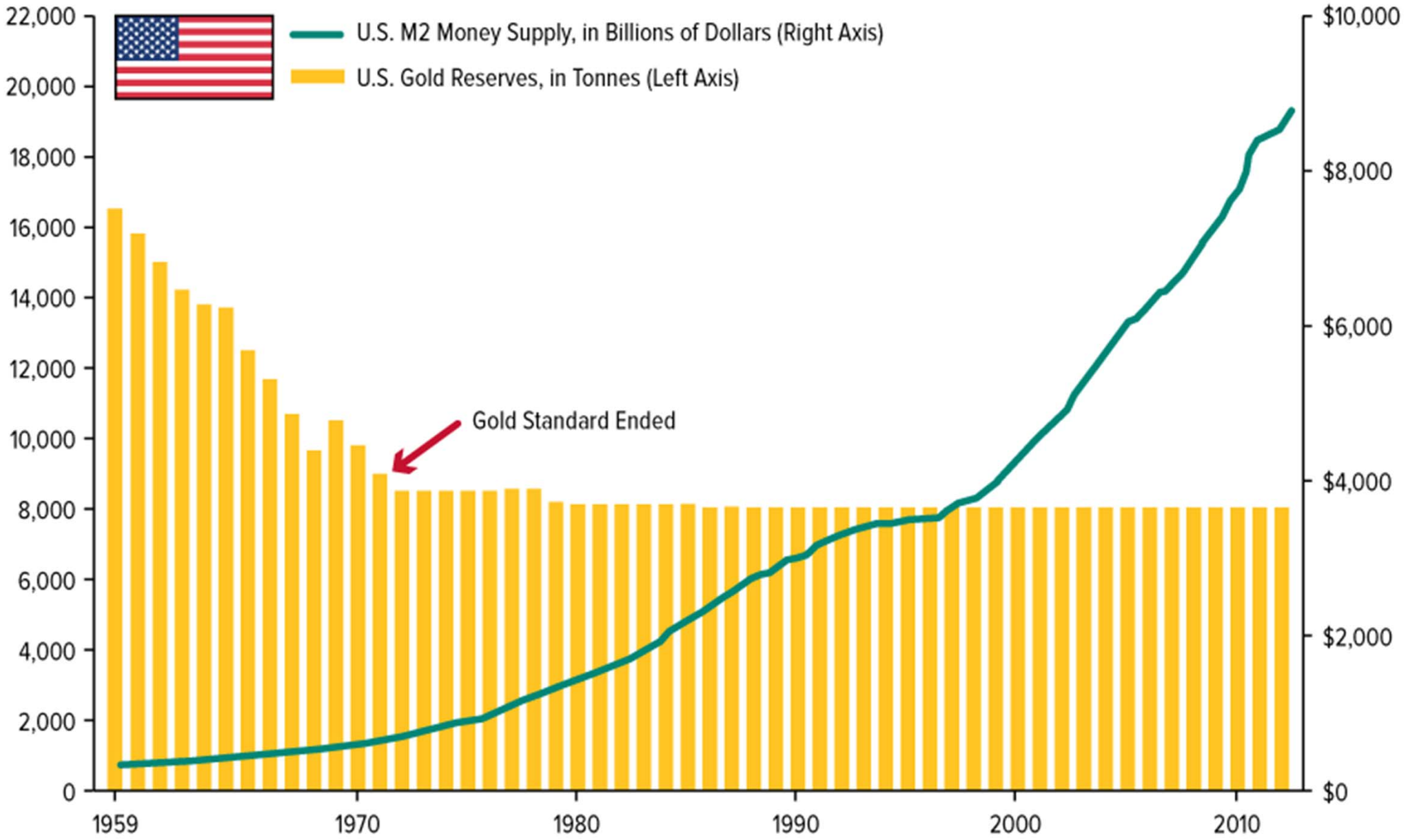
all persons are required to deliver

ON OR BEFORE MAY 1, 1933

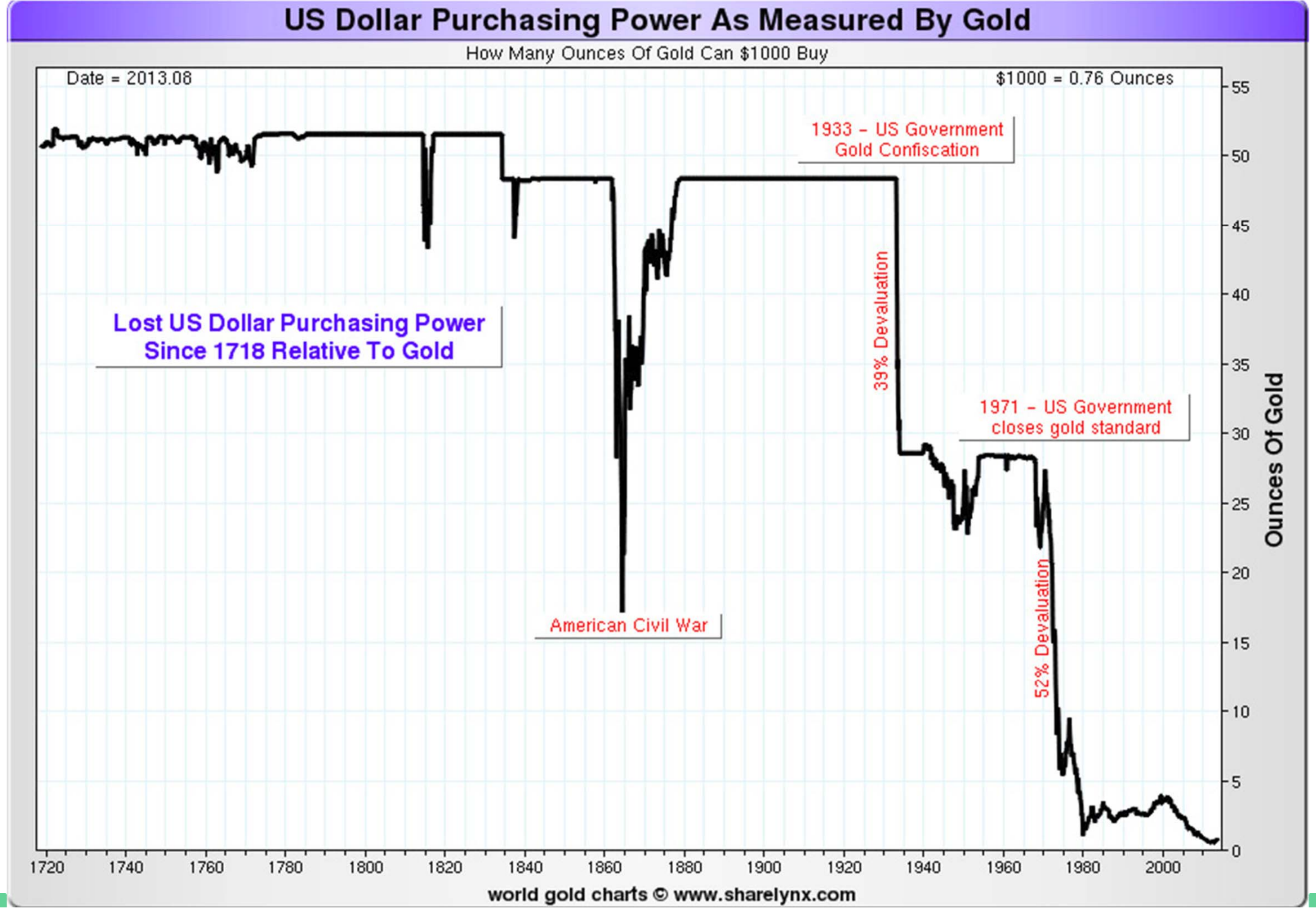
all GOLD COIN, GOLD BULLION, AND GOLD CERTIFICATES now owned by them to a Federal Reserve Bank, branch or agency, or to any member bank of the Federal Reserve System.

Executive Order

M2 Money Supply Rises While Gold Supply Remains the Same, 1959 – 2010

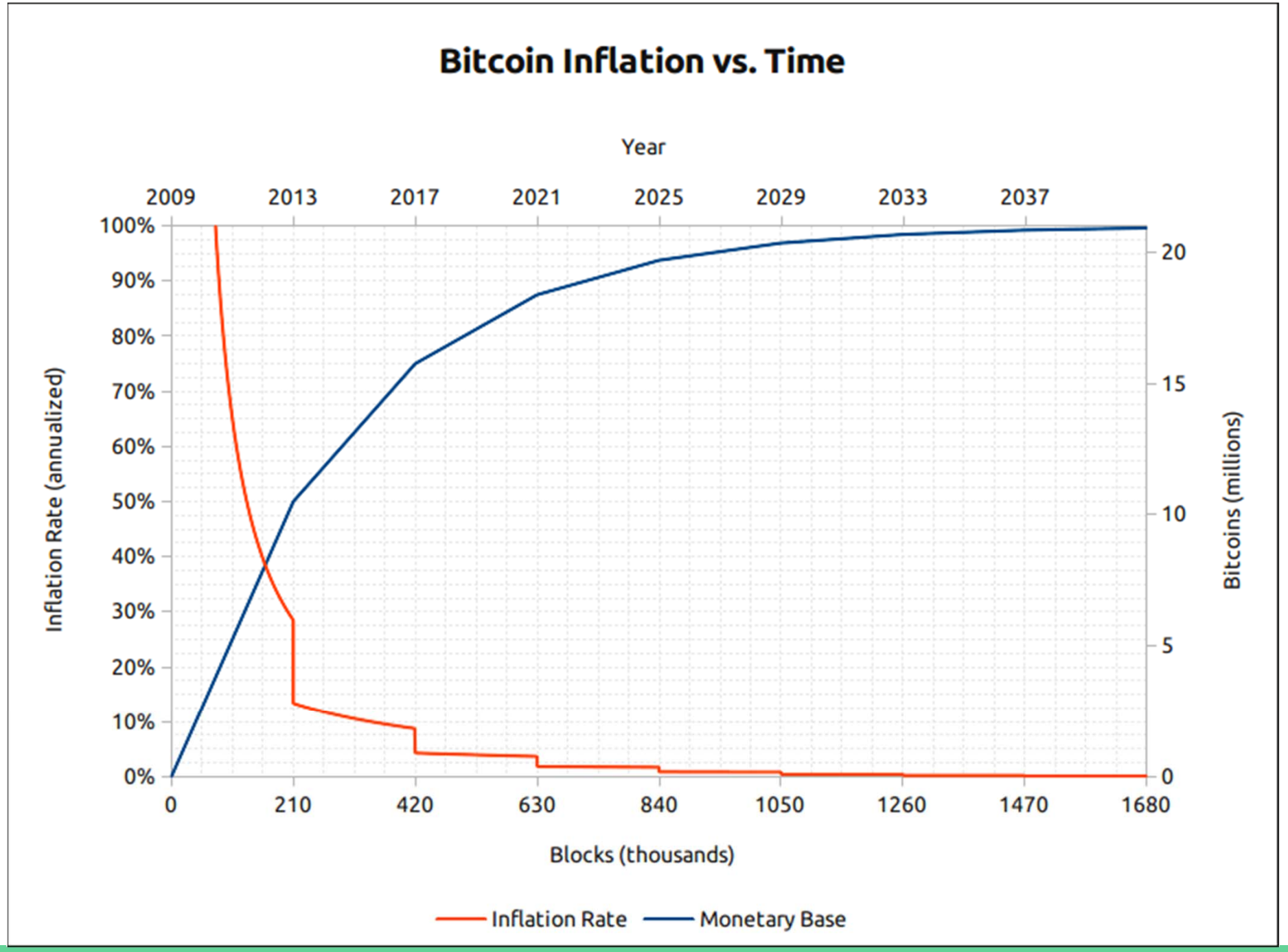


Source: U.S. Federal Reserve, World Gold Council, U.S. Global Investors


US Dollar Purchasing Power As Measured By Gold
How Many Ounces Of Gold Can $1000 Buy
Date = 2013.08
$1000 = 0.76 Ounces
Lost US Dollar Purchasing Power
Since 1718 Relative To Gold
American Civil War
1933 – US Government
Gold Confiscation
39% Devaluation
1971 – US Government
closes gold standard
52% Devaluation
Ounces Of Gold
55
50
45
40
35
30
25
20
15
10
5
0
1720
1740
1760
1780
1800
1820
1840
1860
1880
1900
1920
1940
1960
1980
2000
world gold charts © www.sharelynx.com

Pourquoi 1 Bitcoin vaut 4,500 $ USD

- Rareté : 21 millions de Bitcoin seront “émis” (déflationniste)
- Sécurité : Cryptographie solide, non duplicable
- Fungible : Uniformité de la devise
- Divisible : 1 BTC à 0.00000001 BTC (Satoshi)
- Censure politique difficile
- Immutable
- Solidité du réseau : 100% uptime depuis plus de 8 ans.


Bitcoin Inflation vs. Time
Year
2009
2013
2017
2021
2025
2029
2033
2037
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
Inflation Rate (annualized)
20
15
10
5
0
Bitcoins (millions)
0
210
420
630
840
1050
1260
1470
1680
Blocks (thousands)
Inflation Rate
Monetary Base

Traits of Money	Gold	Fiat (US Dollar)	Crypto (Bitcoin)
Fungible *(Interchangeable)*	High	High	High
Non-Consumable	High	High	High
Portability	Moderate	High	High
Durable	High	Moderate	High
Highly Divisible	Moderate	Moderate	High
Secure *(Cannot be counterfeited)*	Moderate	Moderate	High
Easily Transactable	Low	High	High
Scarce *(Predictable Supply)*	Moderate	Low	High
Sovereign *(Government Issued)*	Low	High	Low
Decentralized	Low	Low	High
Smart *(Programmable)*	Low	Low	High

L’Écosystème Blockchain

Really?

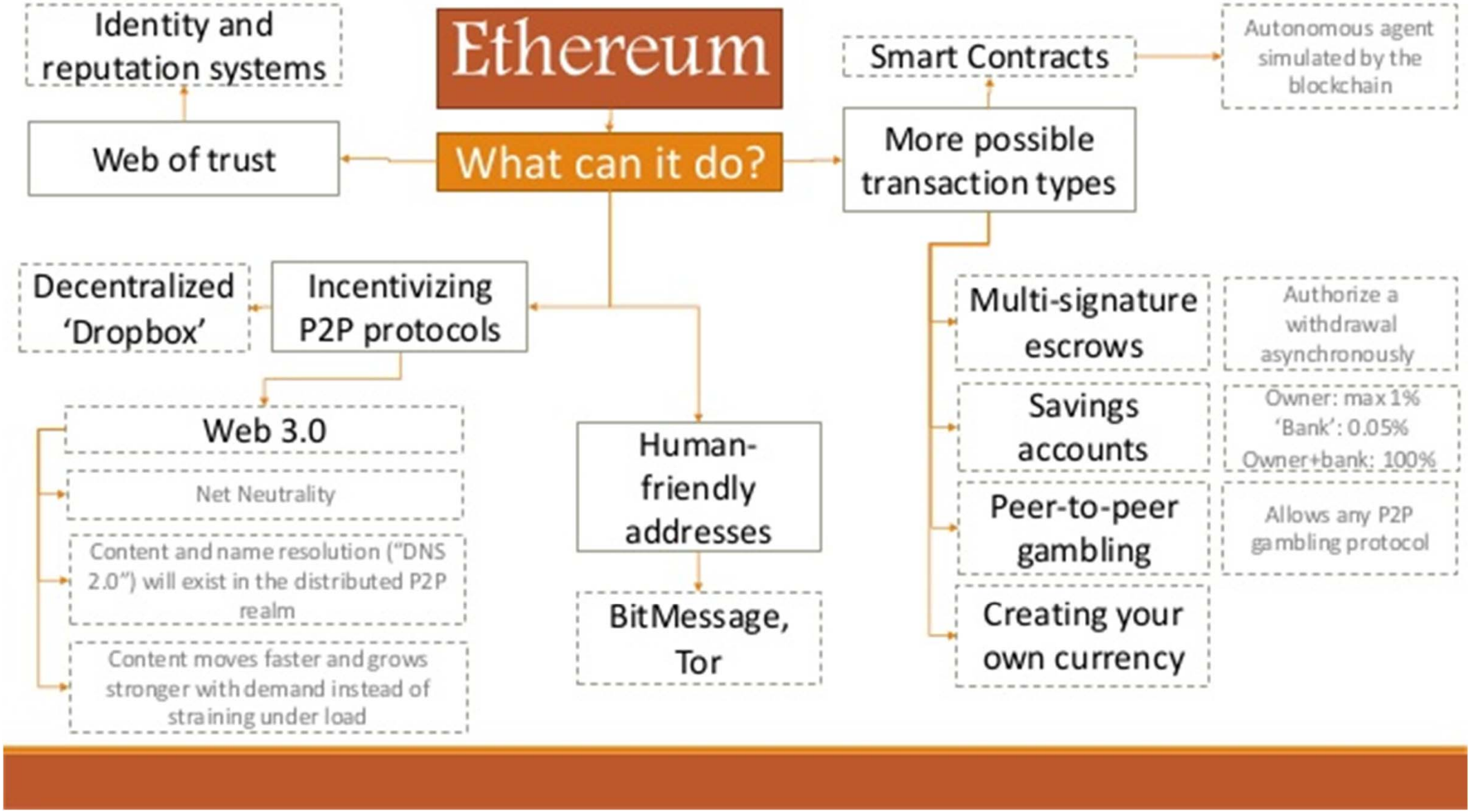
"Blockchain – not bitcoin – will prove revolutionary in banking"

http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine

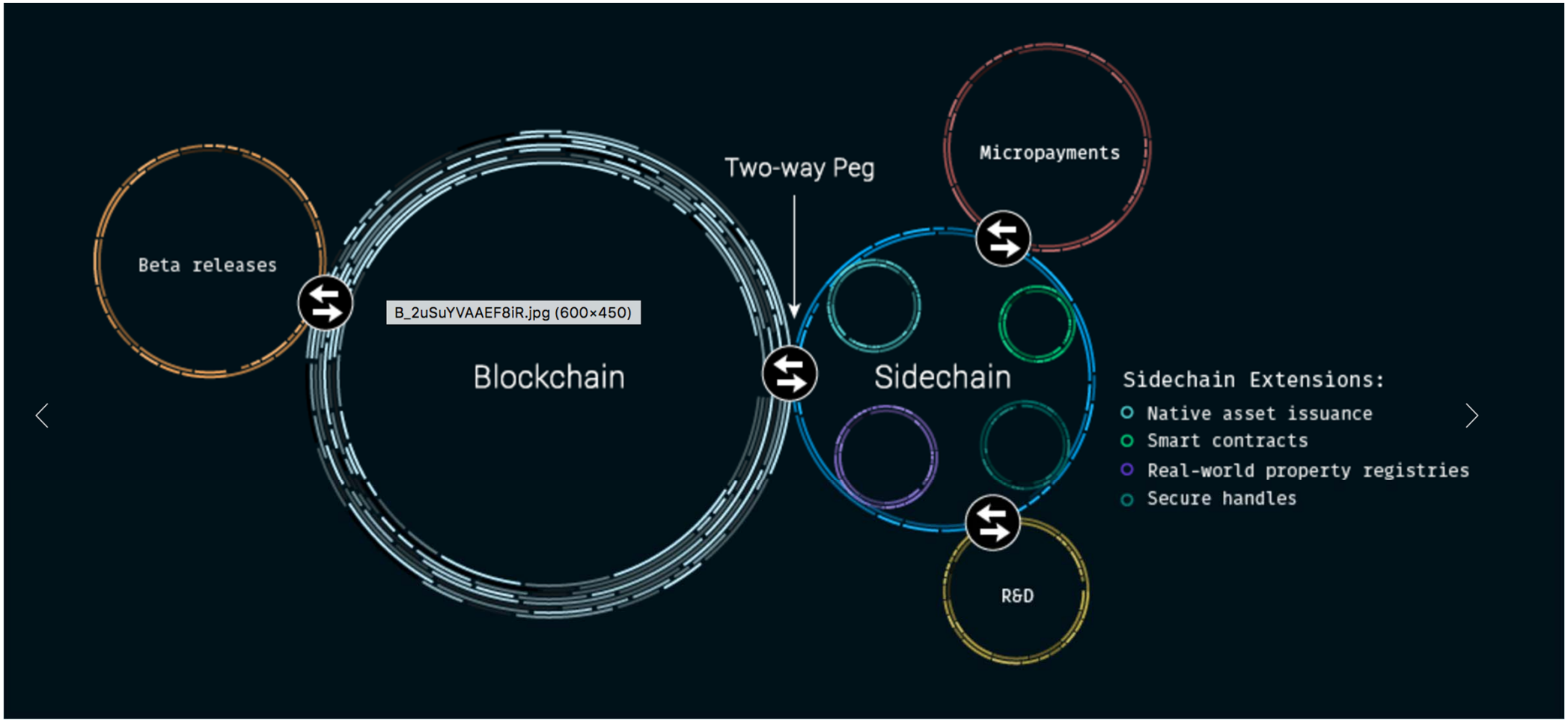
Blockchain public

- Blockchain public (zéro limite d’accès au consensus)
- Devise native (“token) : BTC / ETH
- Preuve de travail (proof-of-work) : Mineurs
- Participants décentralisés / distribués (nodes)
- **Aucune autorité centralisée**

- Plate-forme d’application décentralisée
- Déploiement de Smart Contracts (EVM, Solidity)
- Preuve de travail (proof-of-work) : Mineurs
- Participants décentralisés / distribués (nodes)
- Lancement avec un prévente (premining)


Ethereum
What can it do?
Identity and reputation systems
Web of trust
Decentralized 'Dropbox'
Incentivizing P2P protocols
Web 3.0
Net Neutrality
Content and name resolution ("DNS 2.0") will exist in the distributed P2P realm
Content moves faster and grows stronger with demand instead of straining under load
Human-friendly addresses
BitMessage, Tor
Smart Contracts
Autonomous agent simulated by the blockchain
More possible transaction types
Multi-signature escrows
Authorize a withdrawal asynchronously
Savings accounts
Owner: max 1%
'Bank': 0.05%
Owner+bank: 100%
Peer-to-peer gambling
Allows any P2P gambling protocol
Creating your own currency

Sidechains


Beta releases
Two-way Peg
Micropayments
B_2uSuYVAAEF8iR.jpg (600×450)
Blockchain
Sidechain
Sidechain Extensions:
Native asset issuance
Smart contracts
Real-world property registries
Secure handles
R&D

Sidechains

Production (Bitcoin network)

Experimental

“Blockchain” privé

HYPERLEDGER

r3.

ENTERPRISE
ETHEREUM
ALLIANCE

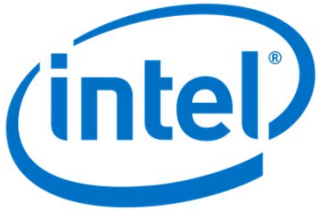
- Réseau privé (barrière à l'entrée)
- Pas de devise native / aucun incitatif à participer
- Consensus : "Proof-of-stake"
- Rôles prédéfinis (voir point suivant)
- Autorité centralisée
- **Réalité : Base de données distribuée avec fonctions cryptographiques**

HYPERLEDGER

Hyperledger is an open source collaborative effort created to advance cross-industry blockchain technologies. It is a global collaboration, hosted by The Linux Foundation

THE LINUX FOUNDATION

HYPERLEDGER



SawTooth

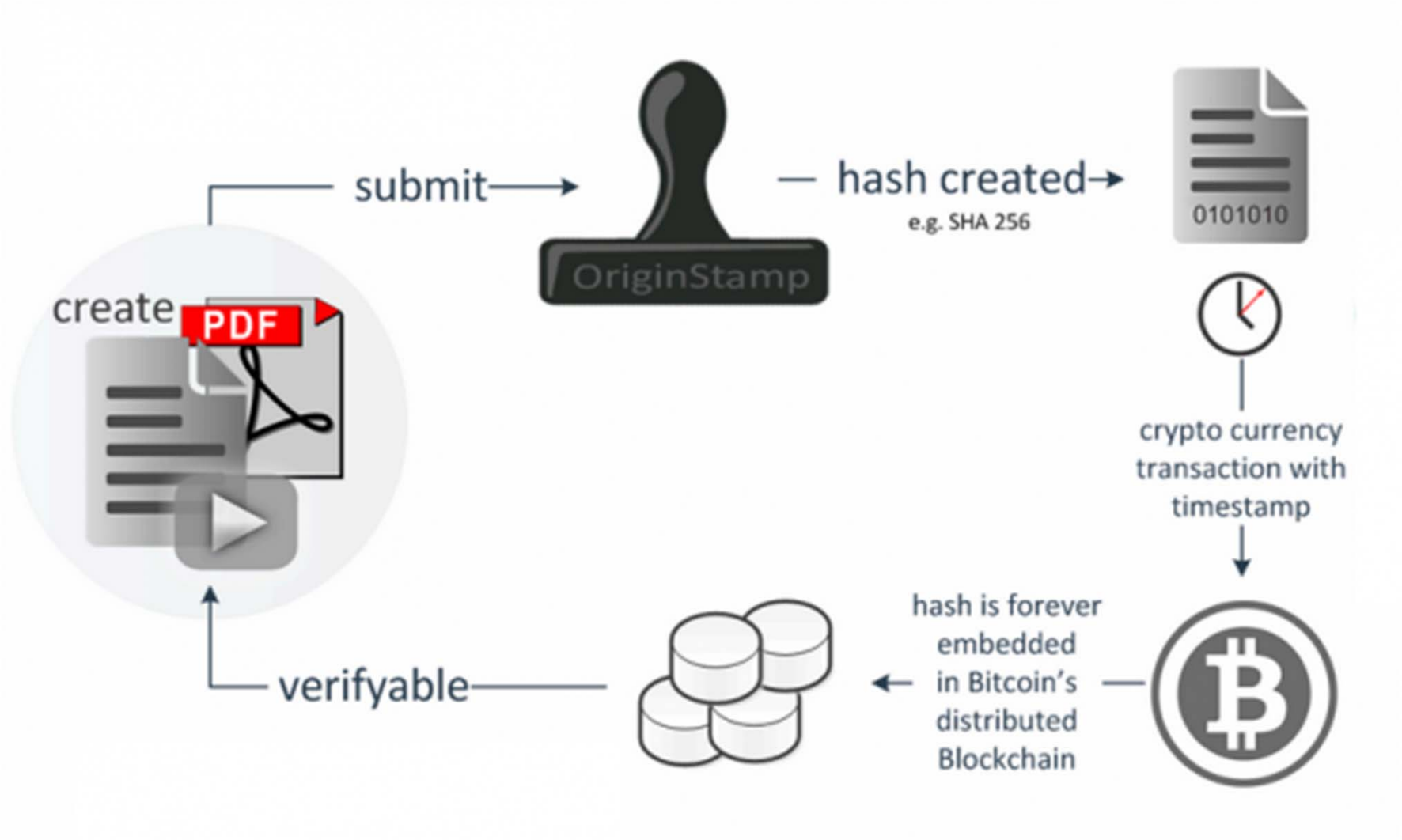
Fabric

Burrow

Quelques exemples

- Marché de prédiction
- Marchés décentralisés
- Entiercement (Escrow)
- Jetonisation d’actifs (ERC20)

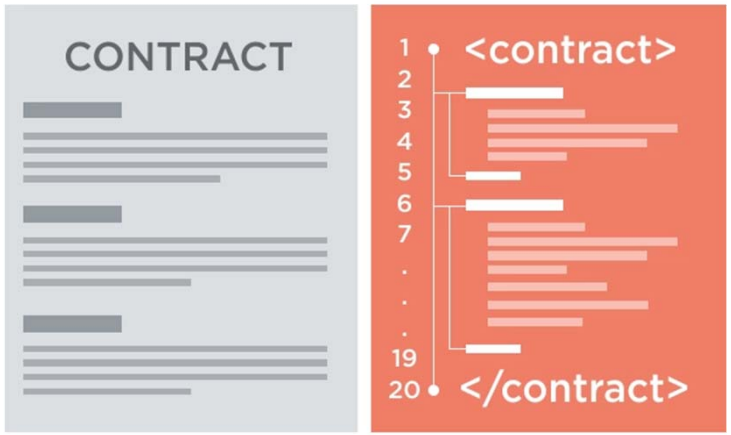
Notarisation / Timestamping


submit
OriginStamp
hash created
e.g. SHA 256
0101010
create
PDF
crypto currency
transaction with
timestamp
hash is forever
embedded
in Bitcoin's
distributed
Blockchain
verifyable

Jetons / Smart Contracts

Propositions de valeur

ethereum

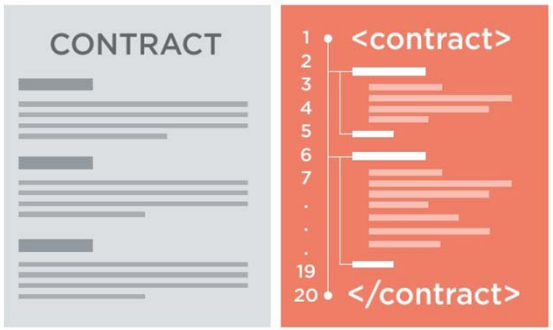


Smart Contracts

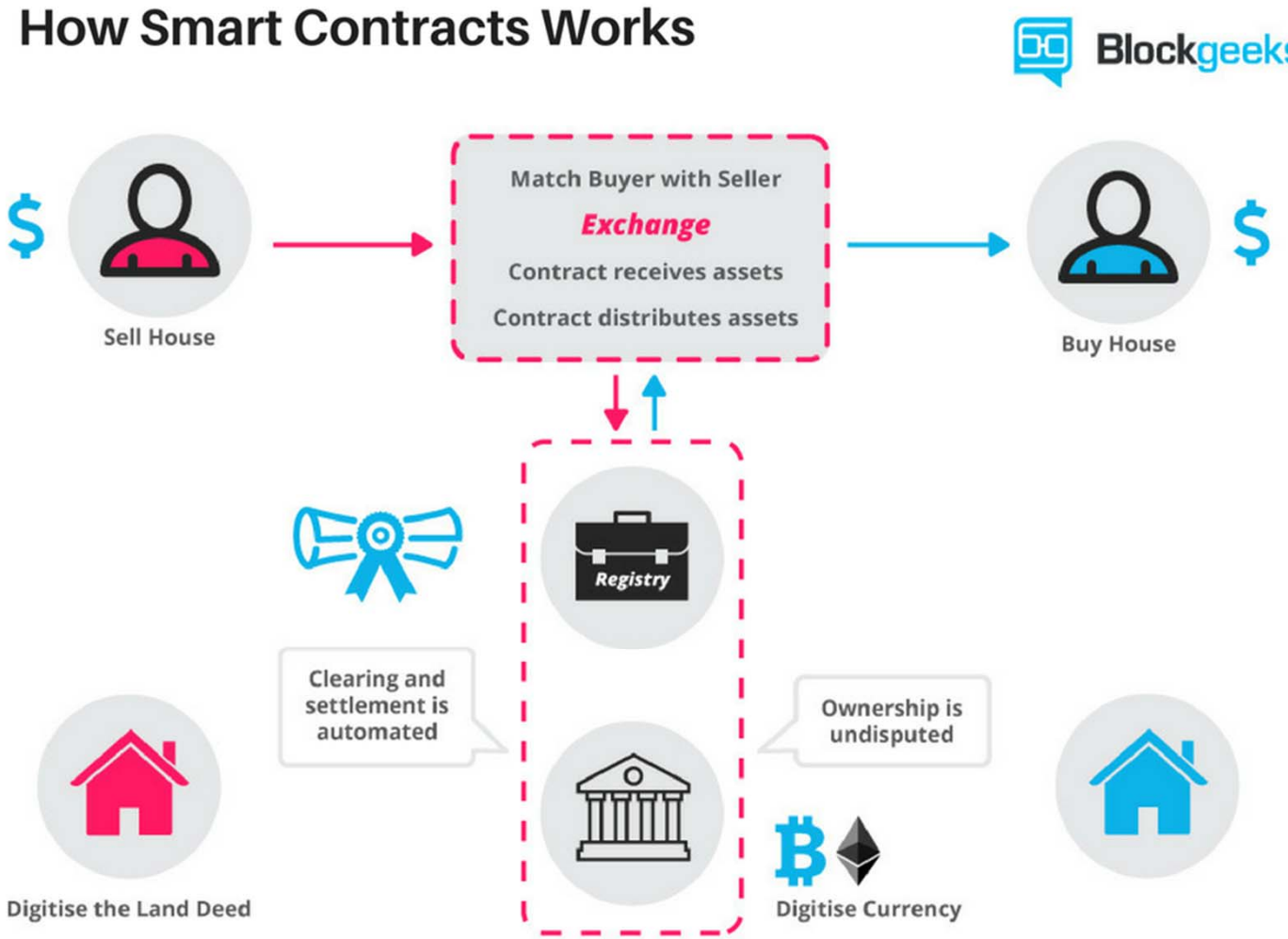
Jetons

Propositions de valeur

ethereum

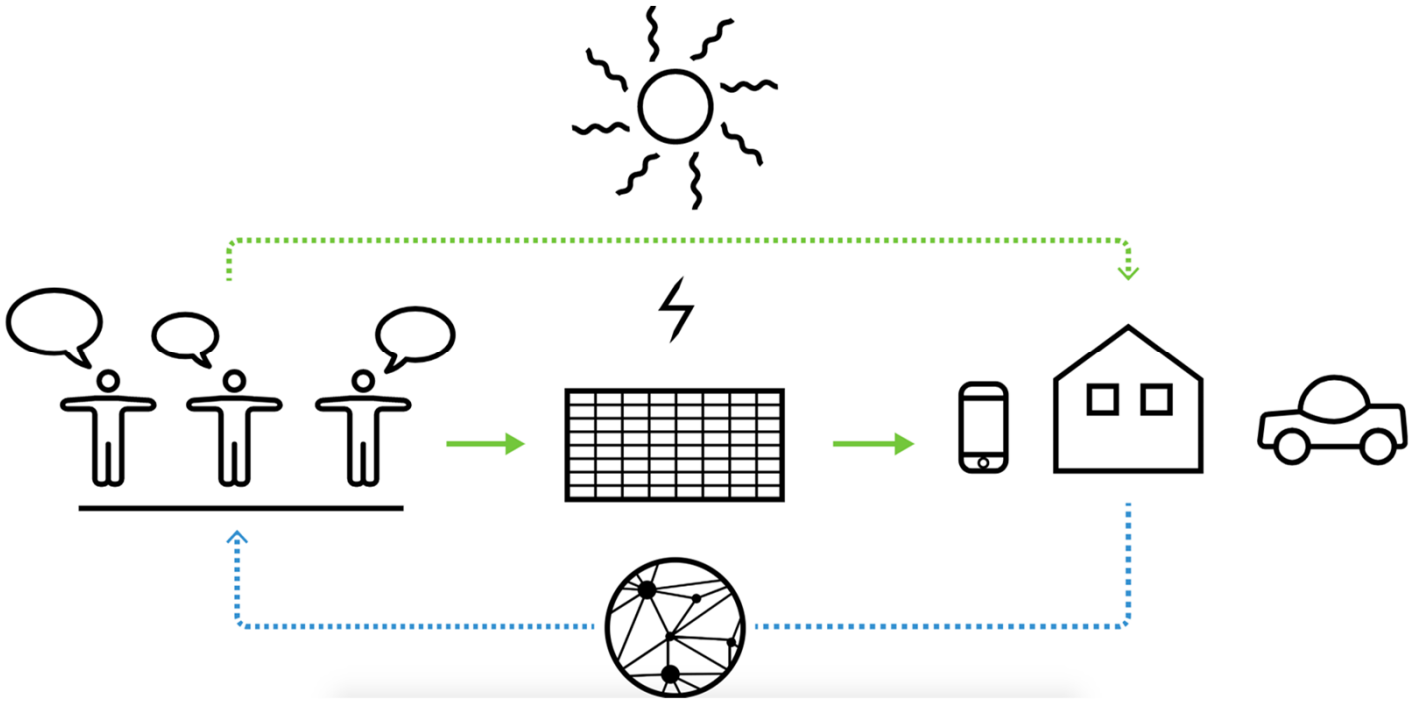


Smart Contracts



Cas d'utilisation

ethereum



Marché énergétique décentralisé

Quels intérêts ?

➔ Emplacement isolé (“grid non disponible)

➔ Liquifier un actif intangible (Énergie > Jetons)

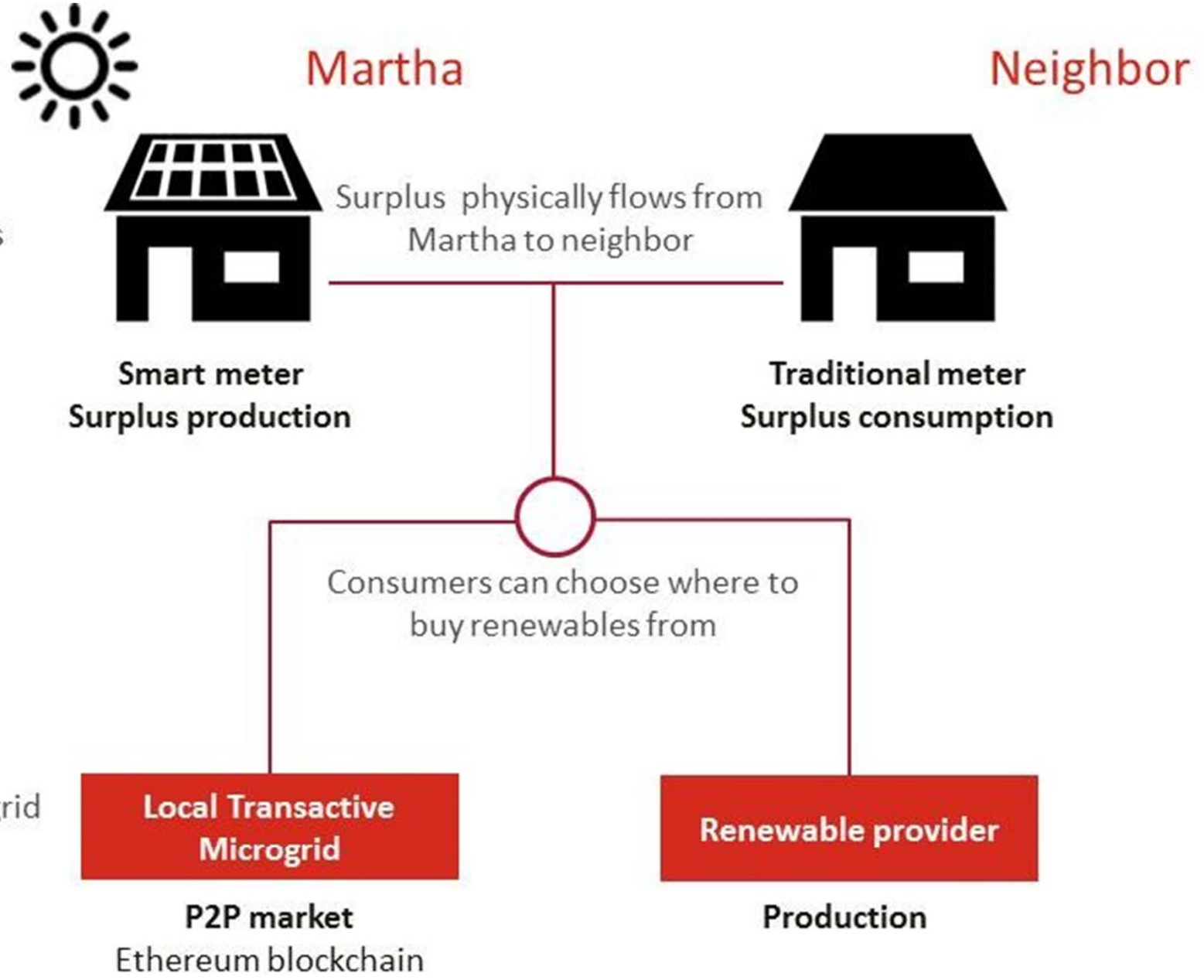
➔ Permettre l’échange entre les participants

Cas d’utilisation

➔ Borne de recharge EV communautaire (Revenus)

➔ Pays en voie de développement (électrification + financiarisation)

➔ Diminuer la dépendance à la “grid” (échange)



Source: Transactive Grid

Menaces et limites

Menaces Non-techniques

- Législatif (interdiction par les gouvernements)
- Finance traditionnelle / Secteur légal (status quo)
- Division dans la communauté sur l'orientation technologique
  - Ex: Bitcoin SegWit 2X
  - Ethereum : Migration vers Proof-of-Stake (Casper / Metropolis)
- Réputationnel : Fraude, Vols, etc reliés aux cryptomonnaies (ex: ICO)

Menaces techniques

- Informatique Quantique (menace à la cryptographie SHA256)
- “Scaling” (performance vs. solidité)
- Failles et piratage d’acteurs (échanges, “Wallet”, etc.)

Q&A

Merci!

LinkedIn : Jonathan Hamel
Email :
jhamel404@gmail.com