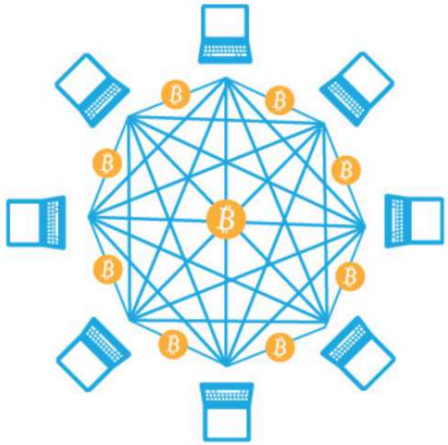
4 mai 2017 – EPFL – Lausanne - Switzerland

Blockchain: du Bitcoin au Smart Contract

EPFL ALUMNI GiTi Le GRIFES itvalley SWISS ENGINEERING ROMANDIE

16h30 – 16h45	**La Blockchain, visite en coulisses** Philippe Thévoz, SICPA, Executive VP eGovernment Systems
16h45 – 17h15	**Hyperledger Fabric: Rethinking Permissioned Blockchains** Marko Vukolic, IBM Research Staff Member
17h15 – 17h45	**Blockchain – from experiments to production** Veronica Lange, UBS, Head of Innovation, Group CTO
17h45 – 18h15	**Pause**
18h15 – 18h45	**Blockchain and Telcos** David Watrin, Swisscom, Head of Security & Intelligence
18h45 – 19h15	**Les « blockchains » à l'assaut des notaires** Xavier Comtesse, Entrepreneur
19h15 – 19h45	**Table ronde**, animée par Philippe Thévoz, suivie d'un Apéritif

EPFL ALUMNI GiTi Le GRIFES itvalley SWISS ENGINEERING ROMANDIE



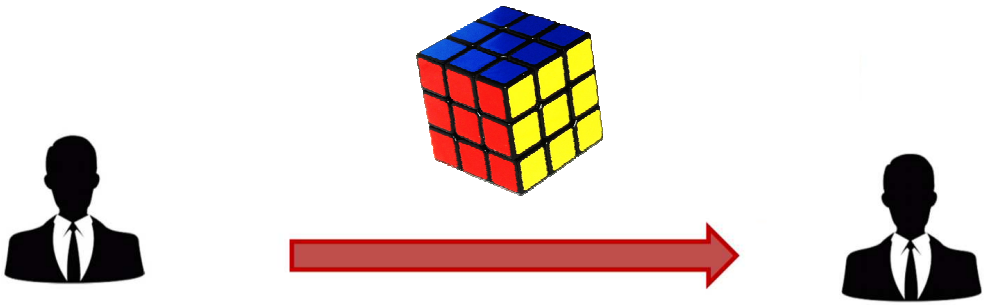
Blockchain
Visite en coulisses

Philippe Thévoz
SICPA – Executive Vice-President eGovernment Systems
thevoz.philippe@gmail.com

The usage or distribution of these slides should not be done without the prior written consent of the author. Thank you.

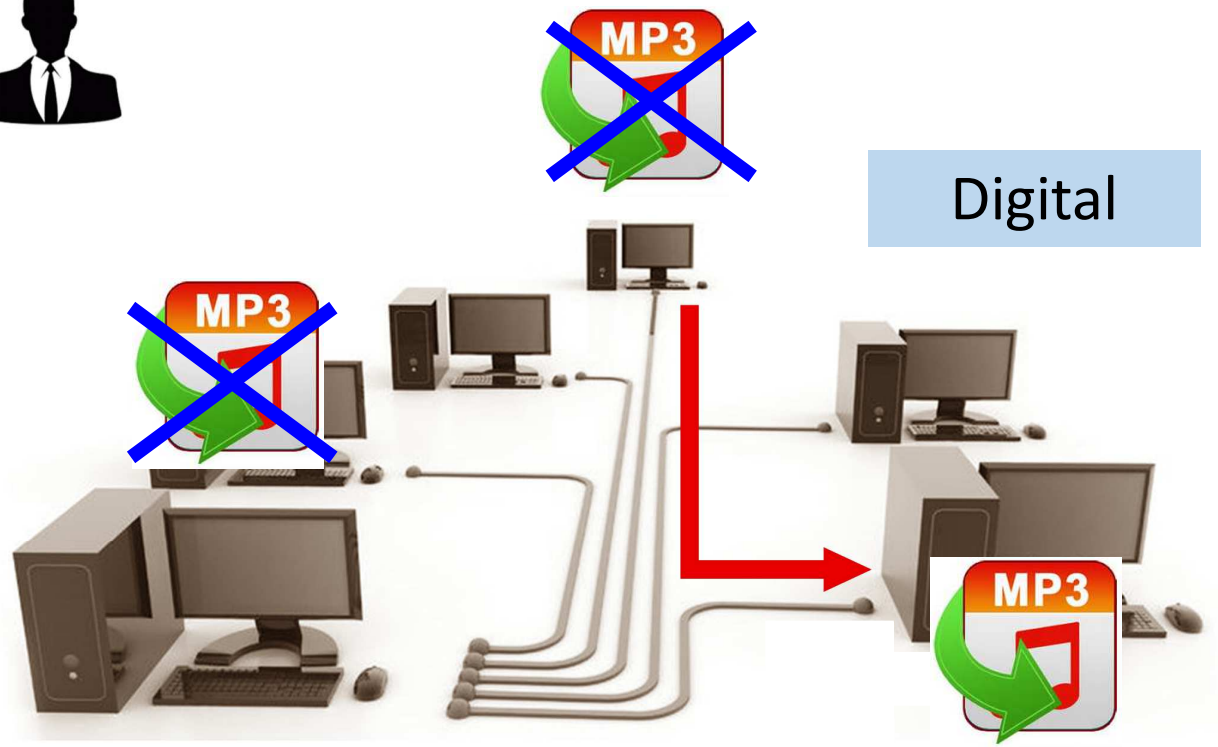
Philippe Thévoz
thevoz.philippe@gmail.com
linkedin.com/in/philippethevoz
Twitter : @PhilippeThevoz

Physical vs Digital



Physical

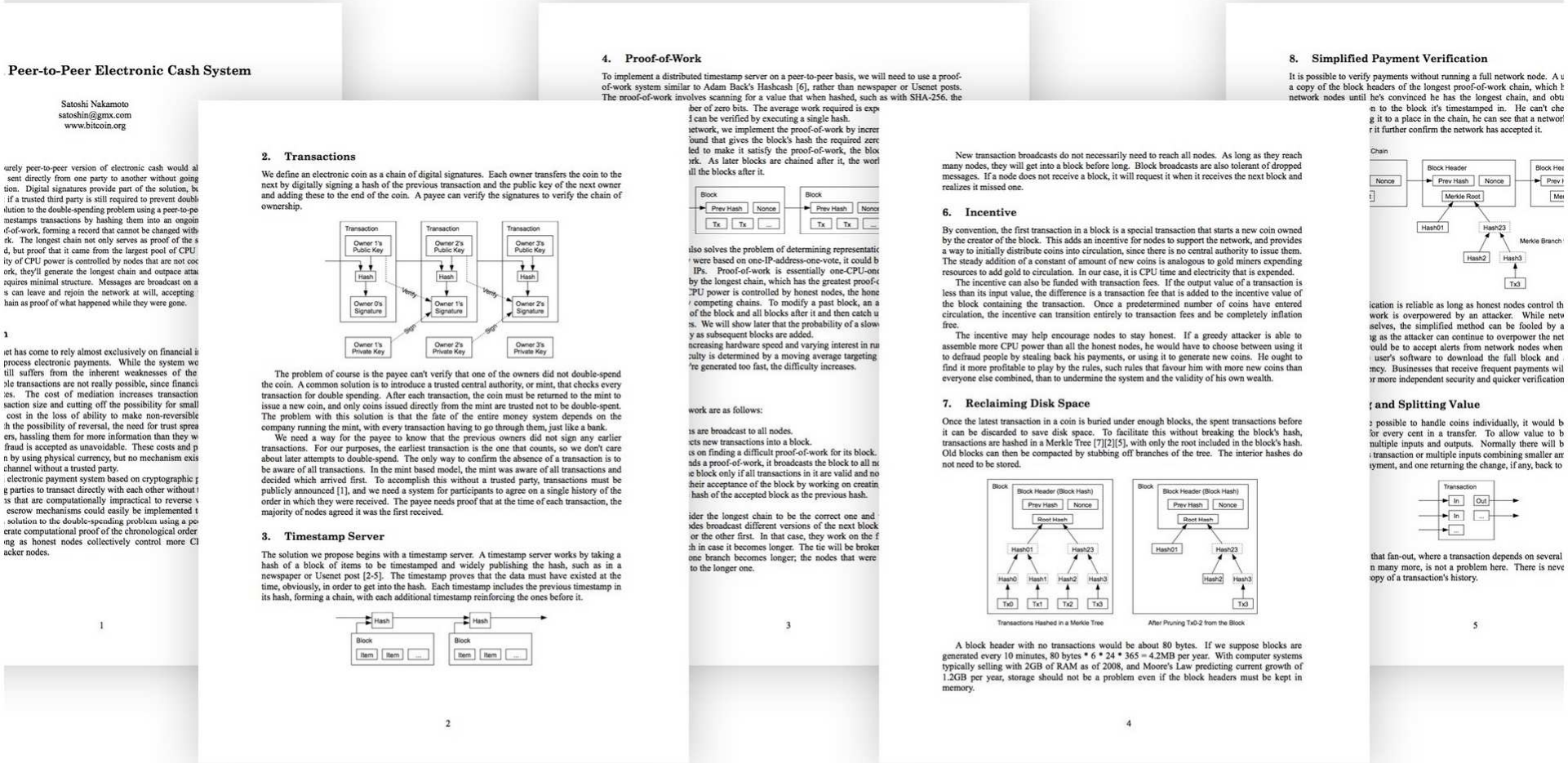
Internet is a fantastic
«**Copy machine**»



Digital

The Blockchain is solving the
«**Double Spend Problem**»
in the Digital world

Original Paper from Satoshi Nakamoto – Oct. 31, 2008



Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

2. Transactions

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.

The problem of course is the payee can't verify that one of the owners did not double-spend the coin. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double-spent. The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank.

We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions. In the mint based model, the mint was aware of all transactions and decided which arrived first. To accomplish this without a trusted party, transactions must be publicly announced [1], and we need a system for participants to agree on a single history of the order in which they were received. The payee needs proof that at the time of each transaction, the majority of nodes agreed it was the first received.

3. Timestamp Server

The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.

4. Proof-of-Work

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the

New transaction broadcasts do not necessarily need to reach all nodes. As long as they reach many nodes, they will get into a block before long. Block broadcasts are also tolerant of dropped messages. If a node does not receive a block, it will request it when it receives the next block and realizes it missed one.

6. Incentive

By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them. The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended.

The incentive can also be funded with transaction fees. If the output value of a transaction is less than its input value, the difference is a transaction fee that is added to the incentive value of the block containing the transaction. Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free.

The incentive may help encourage nodes to stay honest. If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.

7. Reclaiming Disk Space

Once the latest transaction in a coin is buried under enough blocks, the spent transactions before it can be discarded to save disk space. To facilitate this without breaking the block's hash, transactions are hashed in a Merkle Tree [7][2][5], with only the root included in the block's hash. Old blocks can then be compacted by stubbing off branches of the tree. The interior hashes do not need to be stored.

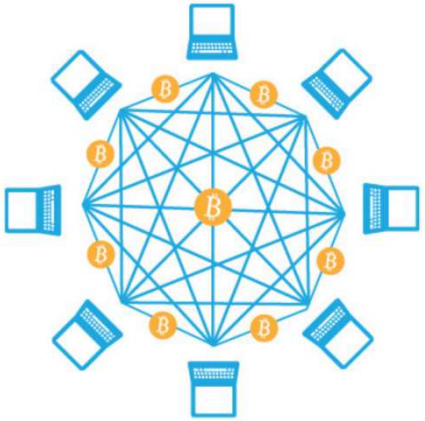
A block header with no transactions would be about 80 bytes. If we suppose blocks are generated every 10 minutes, 80 bytes * 6 * 24 * 365 = 4.2MB per year. With computer systems typically selling with 2GB of RAM as of 2008, and Moore's Law predicting current growth of 1.2GB per year, storage should not be a problem even if the block headers must be kept in memory.

8. Simplified Payment Verification

https://bitcoin.org/bitcoin.pdf

Blockchain in a few words

The **blockchain** is :



- a ledger

that is

- distributed,
- cryptographically secure

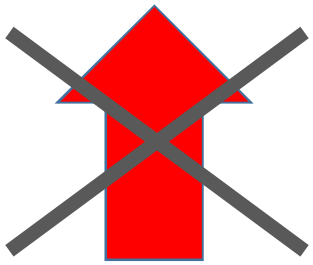
and

- immutable

Quelques bases de cryptographie

«Hash» code (algorithme SHA-256) – empreinte digitale

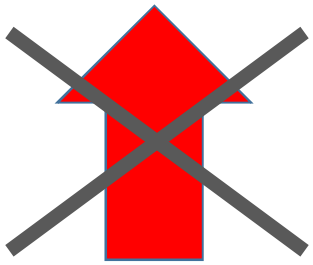
SHA-256



94dfbabefc05247d1f5e3d2f2362be2f08d08334295ee9f1b5577339fb9822e9

«Hash» code (algorithme SHA-256) – empreinte digitale

SHA-256

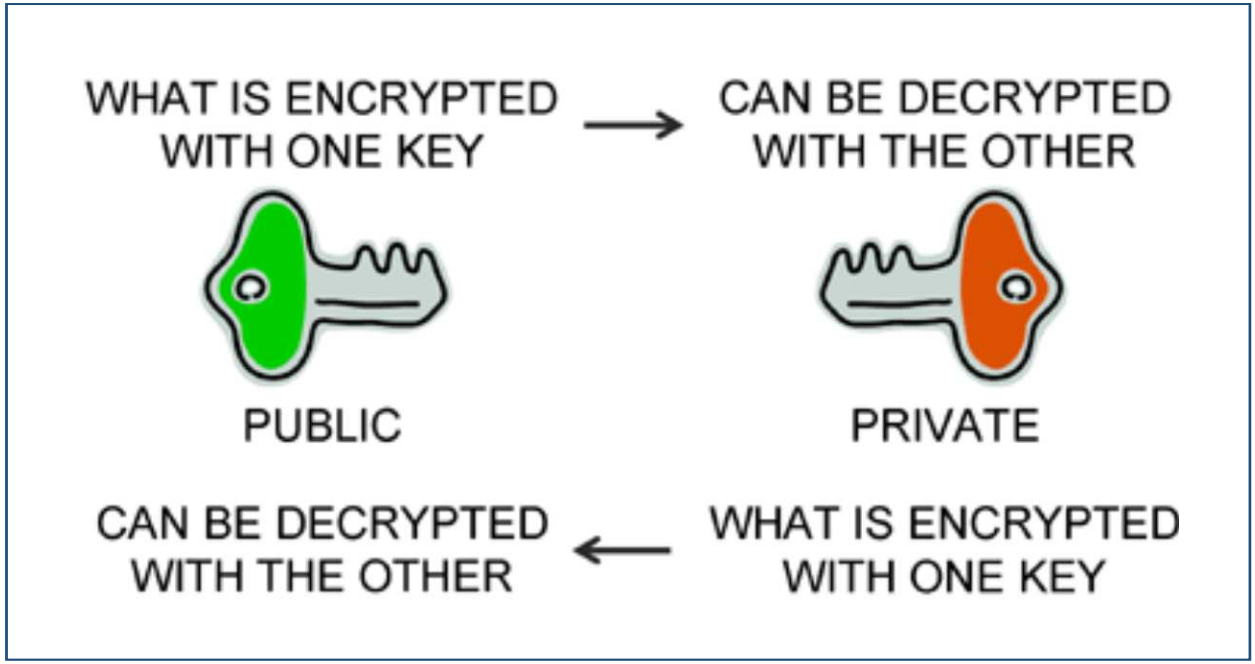


~~94dfbabefc05247d1f5e3d2f2362be2f08d08334295ee9f1b5577339fb9822e9~~

1ec3cc7497ee0fed85a095775a7e6bf2ada83da6e5c0d127eb9abd9aaeaf00b4

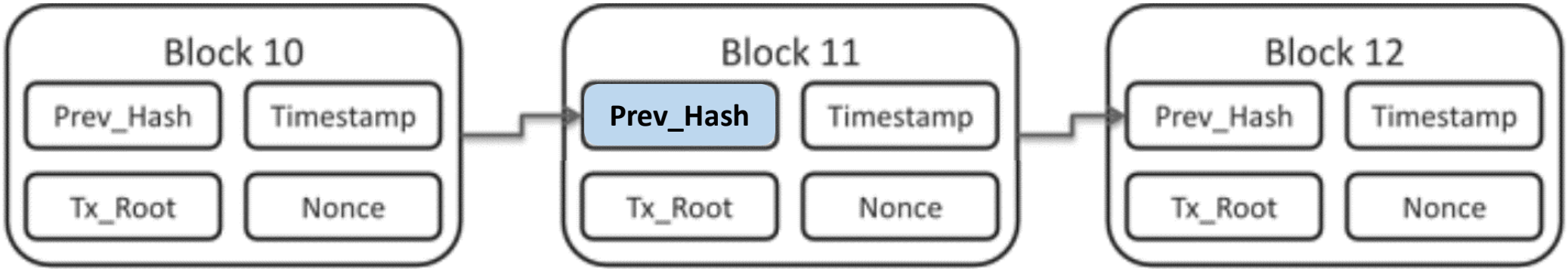
Encryptage asymétrique : Signature Digitale

KEY PAIR



La Structure de la Blockchain

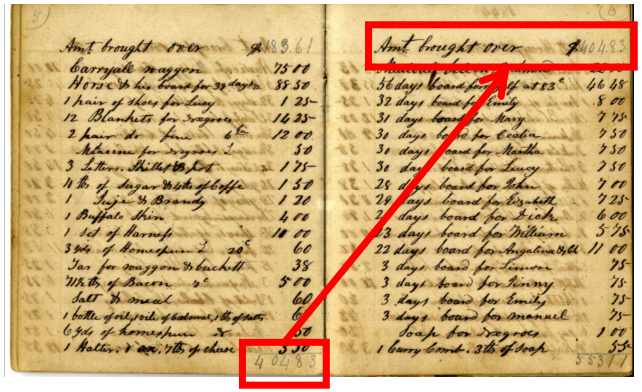
Blockchain Structure

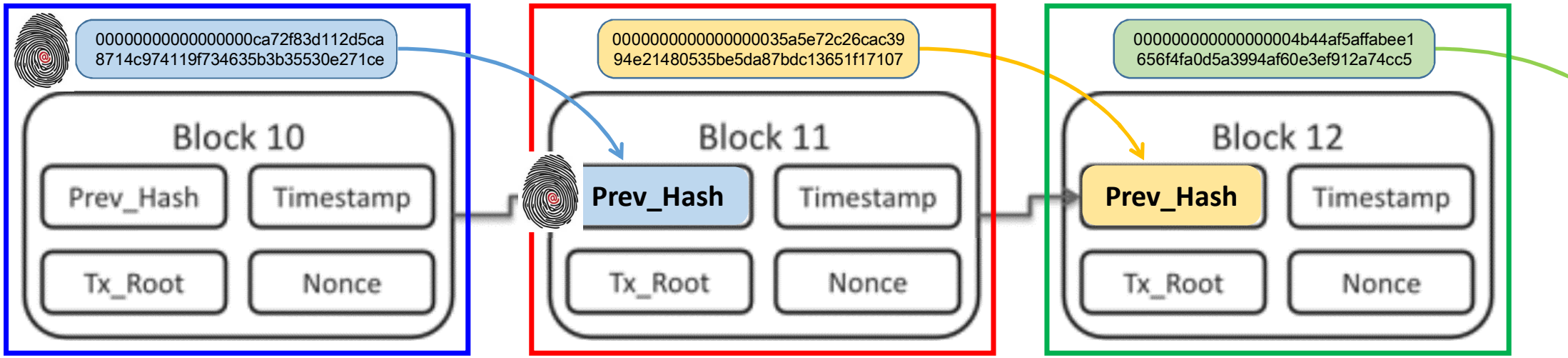


Each Block contains a Header with the following information :

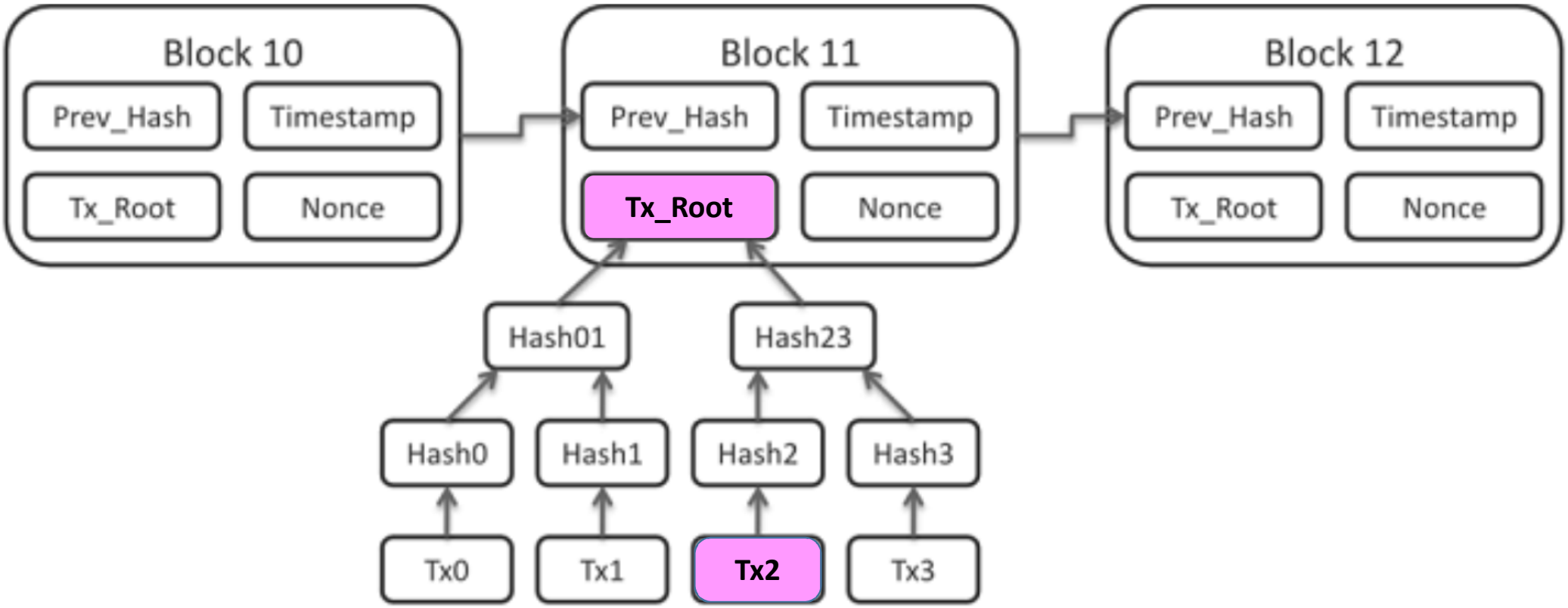
- ***Prev_Hash*** : «Signature/Hash» of the previous Block
- ***Tx_Root*** : «Signature/Merkel Tree» of all the Transactions of the Block
- ***Timestamp*** : Time at which the Block has been created
- ***Nonce*** : Proof that the block has been well validated (result of the PoW – Proof of Work)

Le principe de la chaîne





Transaction in the Blockchain

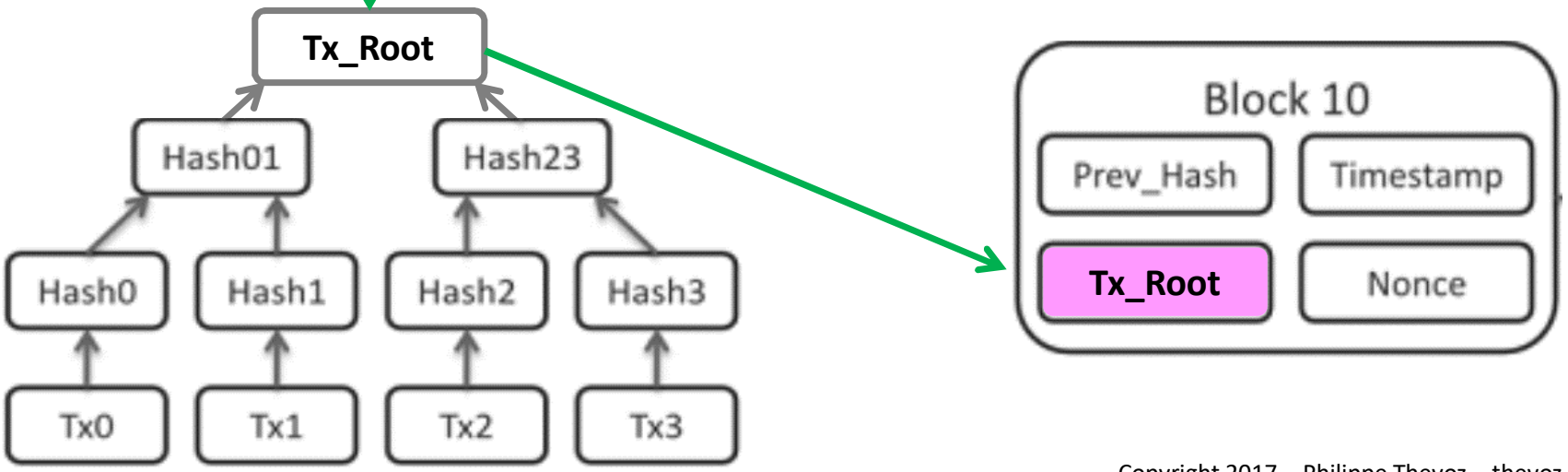


Transactions - Merkel Tree

```
Tx0 -> Hash0 : a7af08b04d86df90104c1cb52988e105f8b0c5e41afcb49dbb624928c23ceed7
Tx1 -> Hash1 : 55f743d0d1b9bd86bbd96a46ba4272ddde19f09e3f6e47832e34bb2779a120b5
Tx2 -> Hash2 : 80ed43f7a11b3295850dd90cc0cfc9a80334f433af8d3d88a1c5e78aff14988f
Tx3 -> Hash3 : 13288c2ba4bbc9af05aa9ccd39b0cc603dc9e30471d97565c9ef3c3604b7ca23

Hash01       : b88ef7a07b91cc4d9d6b81a1b17e4f08b31185bed41d71fe6036d2be55945984
Hash23       : 46a920ea0df1972748e87d3cf74759a9f94d4f65a6260531a3b85064e86b814d

Tx_Root      : 561e964c28335b1c99255d0f80cccc9025789c087e5d388247fef9275f1cbeb1
```

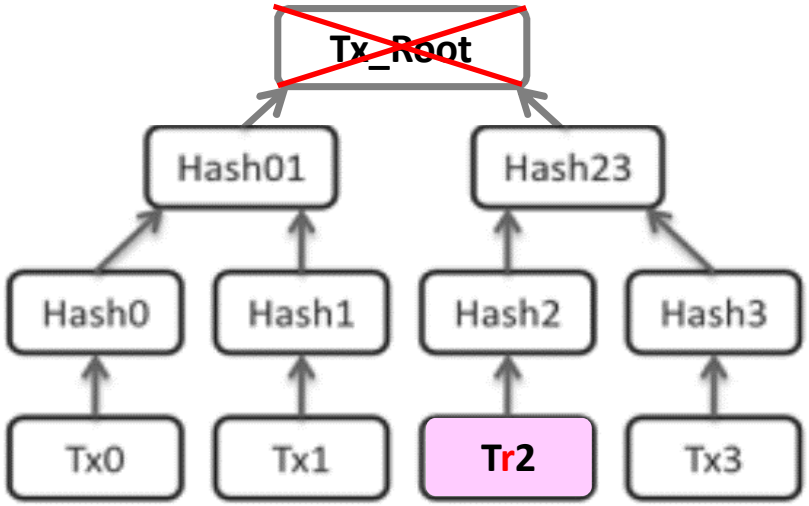


Transactions - Merkel Tree

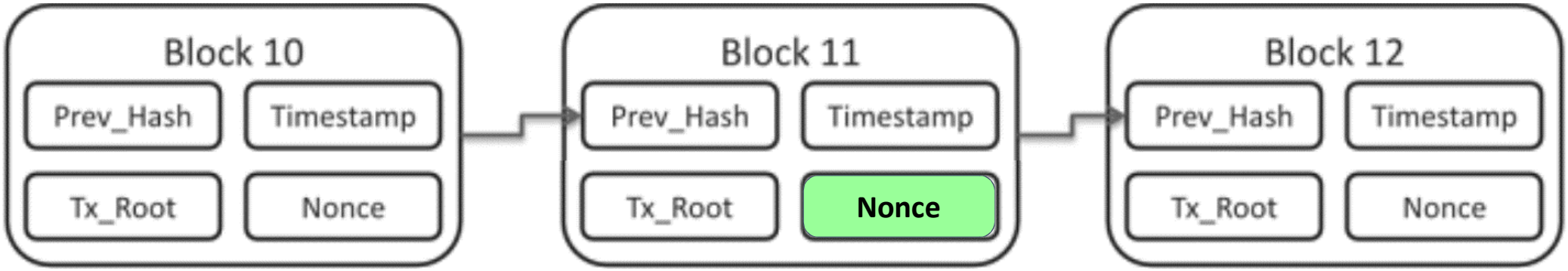
Tx0 -> Hash0 : a7af08b04d86df90104c1cb52988e105f8b0c5e41afcb49dbb624928c23ceed7
Tx1 -> Hash1 : 55f743d0d1b9bd86bbd96a46ba4272ddde19f09e3f6e47832e34bb2779a120b5
Tr2 -> Hash2 : 31b6be0266a8be6c1570e7ae79e13b1f2339c12723be2d9bfba1cb9bf6e753be
Tx3 -> Hash3 : 13288c2ba4bbc9af05aa9ccd39b0cc603dc9e30471d97565c9ef3c3604b7ca23

Hash01 : b88ef7a07b91cc4d9d6b81a1b17e4f08b31185bed41d71fe6036d2be55945984
Hash23 : 8e48fa97e0d8a00e78363e9080befa5dda1e3f1b6aa192bfc8b5aee76aa6ec11

Tx_Root : d92eed688f508d916946afcb49c9afa0d7e05e6098e51a80385d0ef411a9e4f6



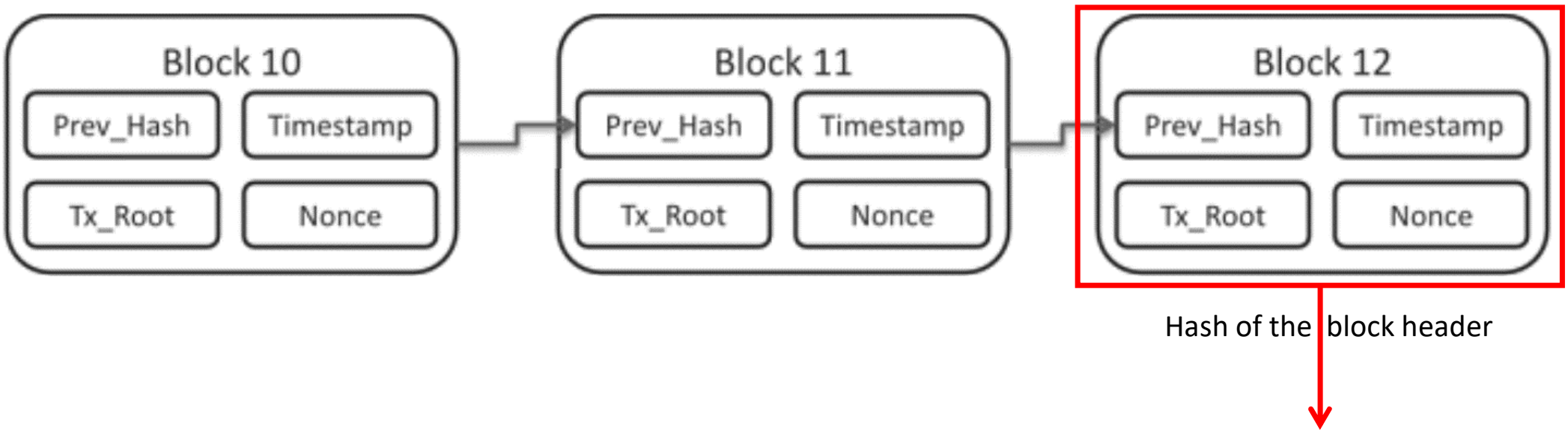
Block validation – Proof of Work (PoW)



Each Block contains a Header with the following information :

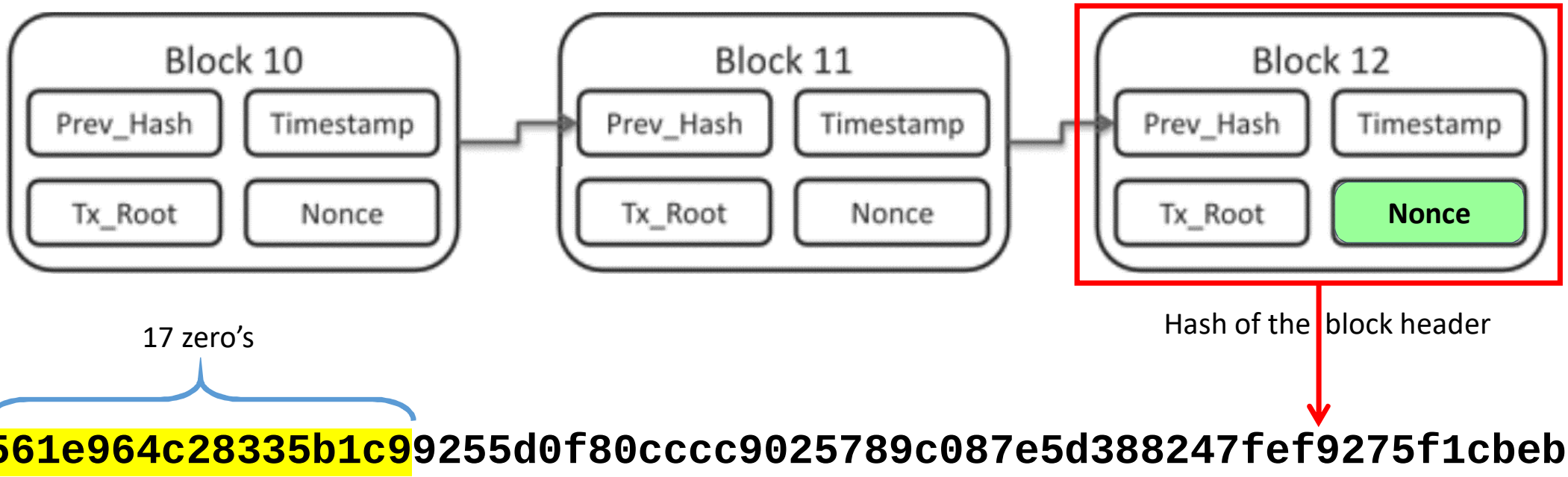
- ***Prev_Hash*** : «Signature/Hash» of the previous Block
- ***Tx_Root*** : «Signature/Merkel Tree» of all the Transactions of the Block
- ***Timestamp*** : Time at which the Block has been created
- ***Nonce*** : Proof that the block has been well validated (result of the PoW – Proof of Work)

Block validation – Proof of Work (PoW)

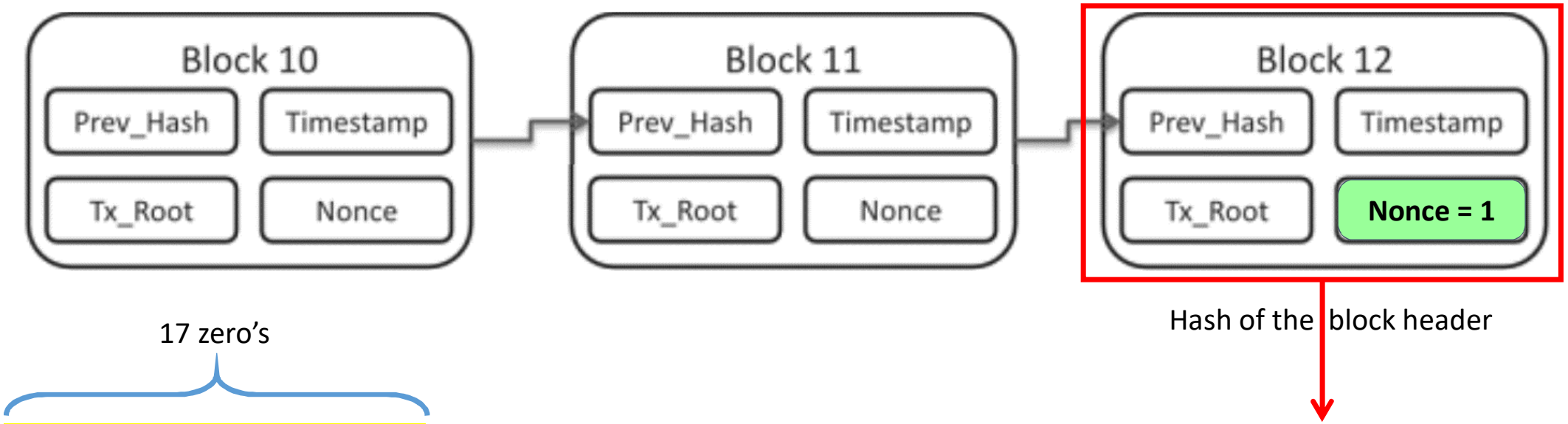


561e964c28335b1c99255d0f80cccc9025789c087e5d388247fef9275f1cbeb1

Block validation – Proof of Work (PoW)

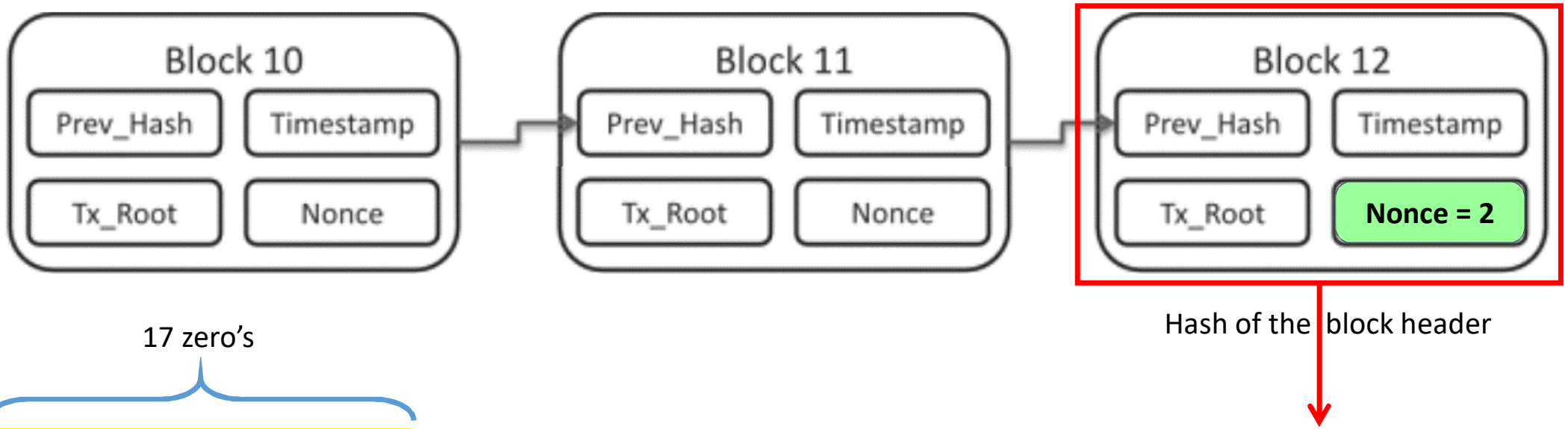


Block validation – Proof of Work (PoW)



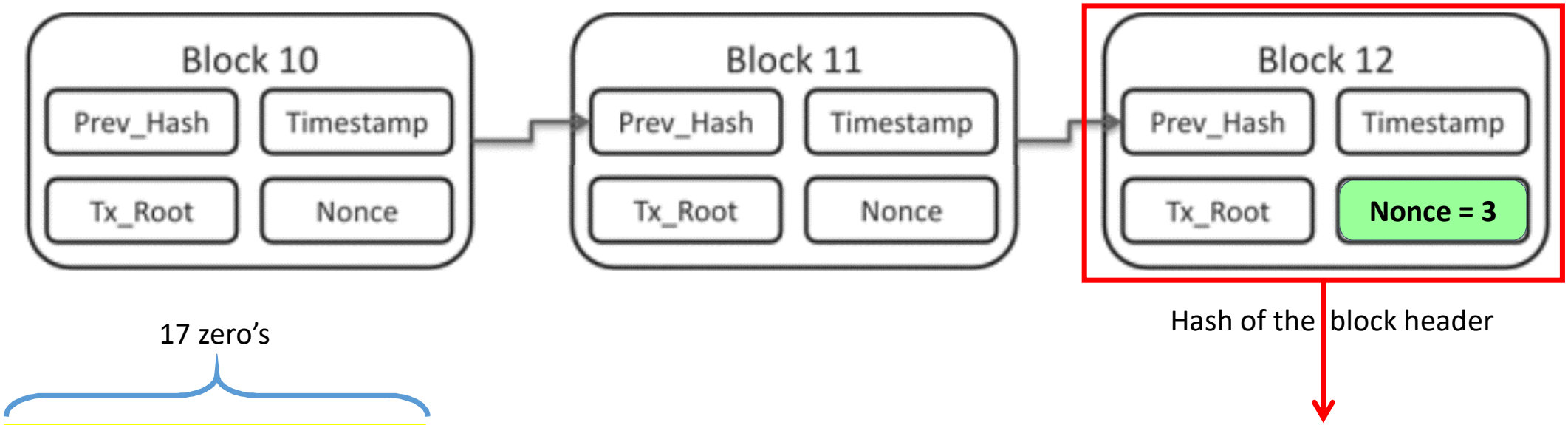
Nonce = 1

Block validation – Proof of Work (PoW)



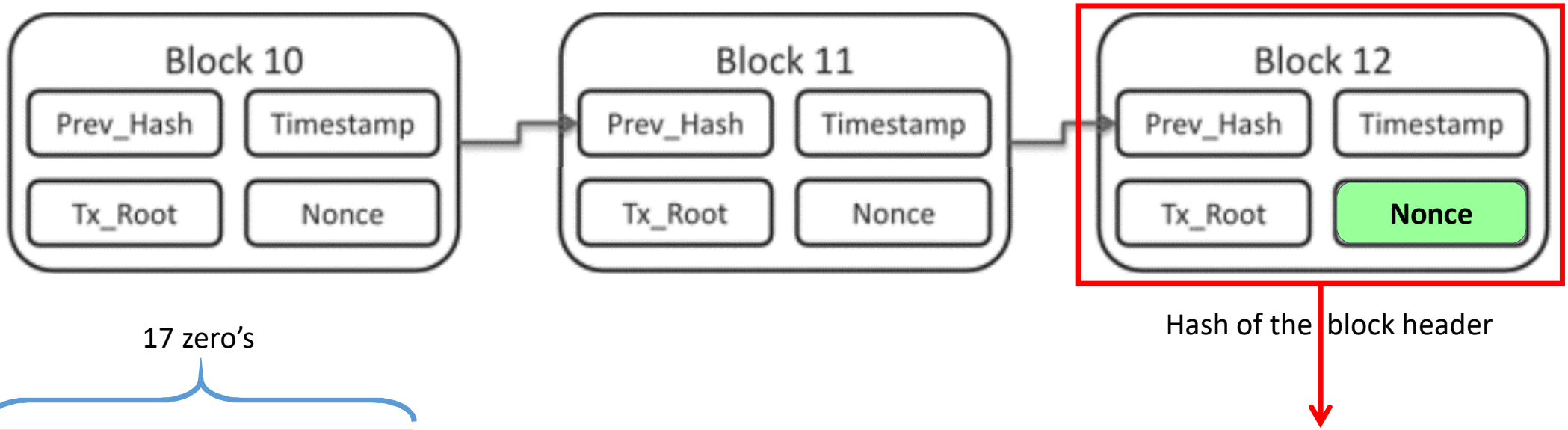
Nonce = 2

Block validation – Proof of Work (PoW)



Nonce = 3

Block validation – Proof of Work (PoW)



Nonce = 2'289'308'096

Summary of a Transaction on the Blockchain

Transaction & Block in the Blockchain

BLOCKCHAIN info — Home Charts Stats Markets API Wallet — Search — English

Transaction View information

6b21f48c4496835ba59fb9f934105db68be828546df6102

19JfeGkrFp9K9uAqCCmoBzGyPUhSQ6ZHx3 (0.00

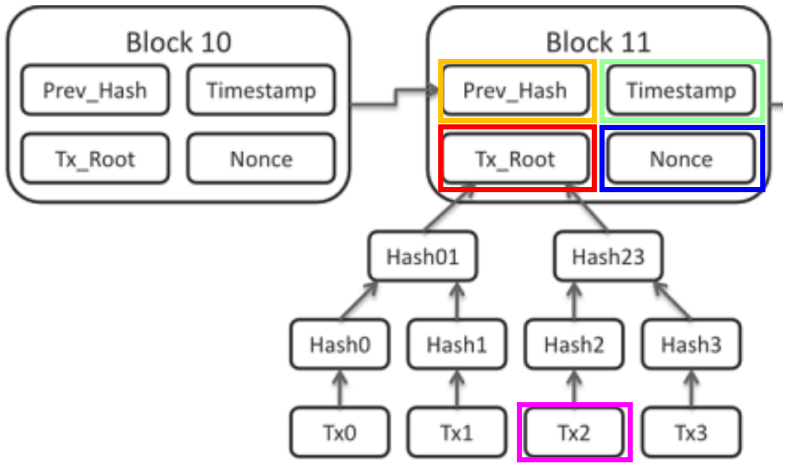
Summary	
Size	191 (bytes)
Received Time	2016-06-09 12:38:34
Included In Blocks	415507 (2016-06-09
Confirmations	8 Confirmations
Relayed by IP	84.200.84.195 (whoi

BLOCKCHAIN info — Home Charts Stats Markets API Wallet — Search — English

Block #415507

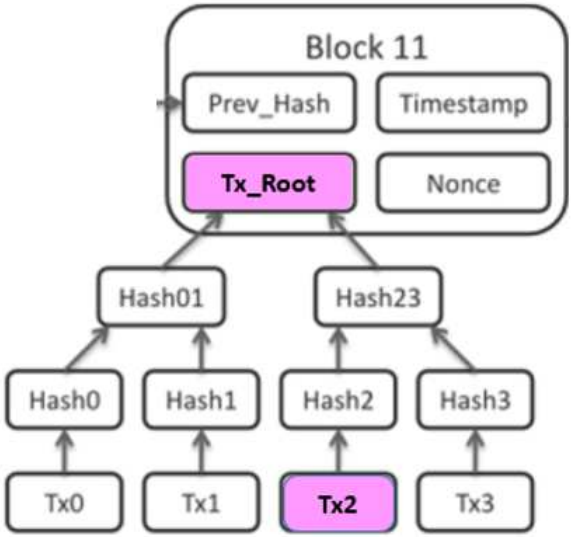
Summary	
Number Of Transactions	3017
Output Total	24,171.50114946 BTC
Estimated Transaction Volume	4,172.99559207 BTC
Transaction Fees	0.76132697 BTC
Height	415507 (Main Chain)
Timestamp	2016-06-09 12:40:49
Received Time	2016-06-09 12:40:49
Relayed By	Slush
Difficulty	196,061,423,939.65
Bits	403020704
Size	998.027 KB
Version	536870913
Nonce	2289308096
Block Reward	25 BTC

Hashes	
Hash	00000000000000000050649f271cb884980e85956d8a281216f8db7bf48c3f092
Previous Block	00000000000000000020cc713e0d0ce5ccba54b8d45505526794f4ff92b43cfaf
Next Block(s)	00000000000000000440dd4b7da778e708ac1ac9bf3b63029fc46639802b795c
Merkle Root	24dff5788539d5122274a6f49edc59a5994b5aa6aeda03ed03458c62901f959d



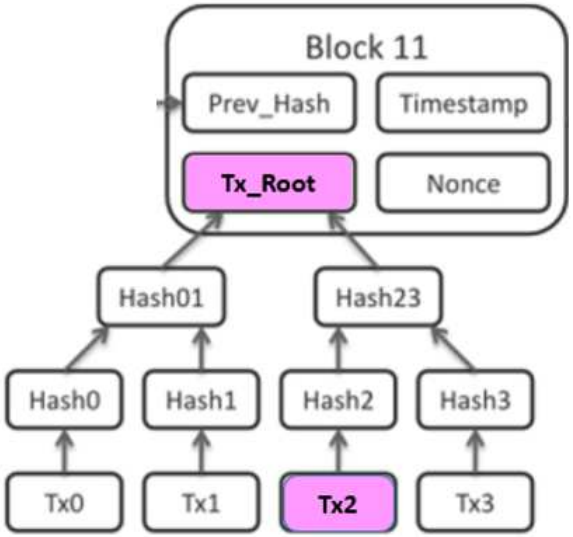
Transactions & Applications

Transactions & Applications



- Enregistrement d'un transfert de valeur

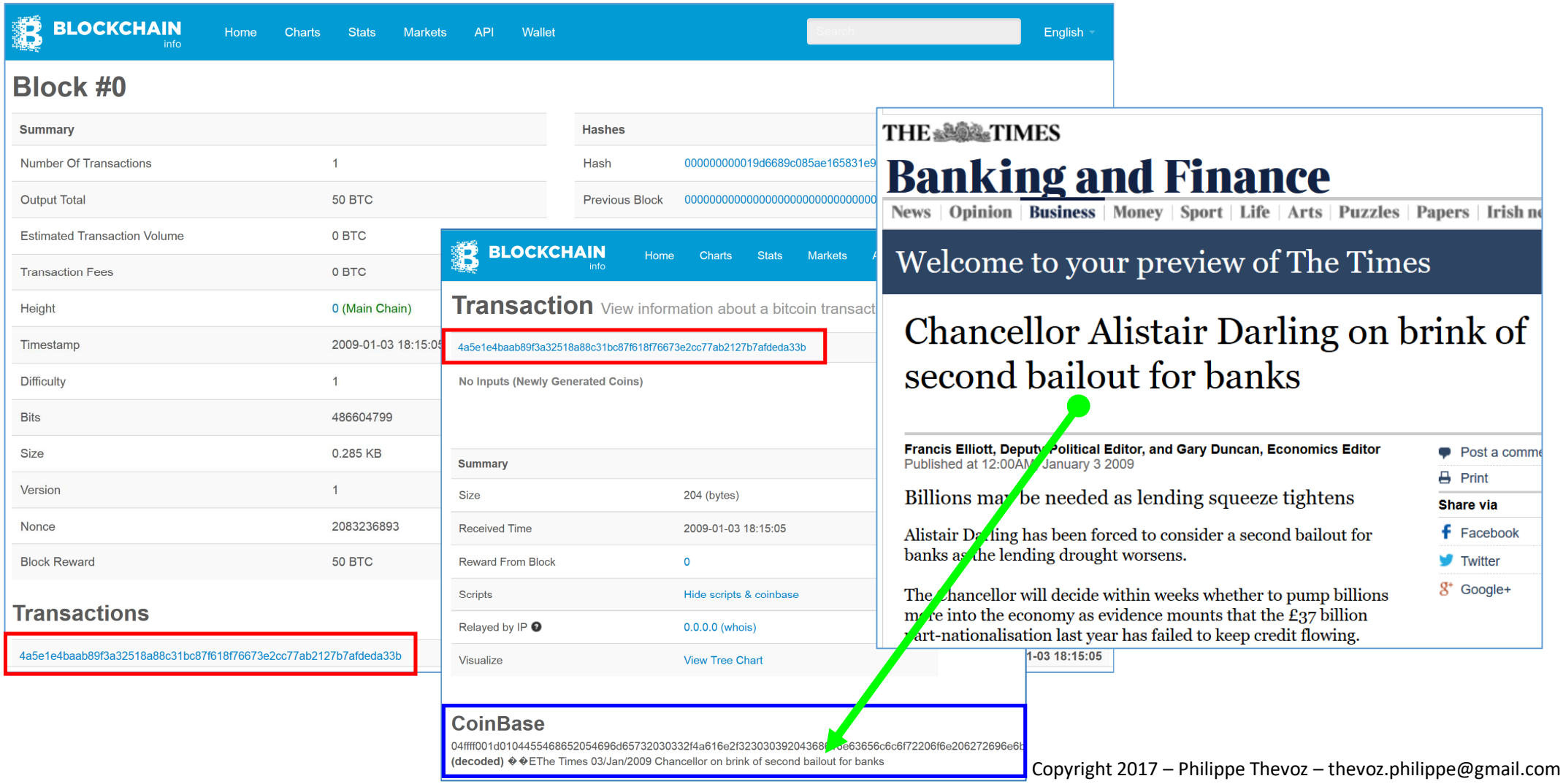
Transactions & Applications



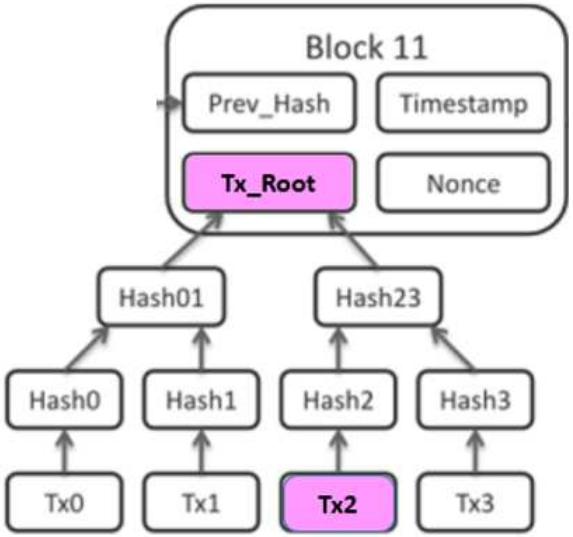
- Enregistrement d'un transfert de valeur

- Enregistrement d'une chaîne de caractères

Text in Block 0 of the Bitcoin Blockchain



Transactions & Applications



- Enregistrement d'un transfert de valeur

- Enregistrement d'une chaîne de caractères
  (e.g "Hash" dans la Blockchain du Bitcoin)

University Degree certification


UNIVERSITY OF NICOSIA

CERTIFICATE OF ACCOMPLISHMENT

This is to certify that

Philippe Thevoz

has successfully completed the University of Nicosia course

DFIN-511 INTRODUCTION TO DIGITAL CURRENCIES

This course introduced students to decentralized digital currencies (cryptocurrencies), such as Bi
It covered the relevant theories and practice, including examples of basic transactions, and disc
the likely interaction with the banking, financial, legal and regulatory system, examining digi
currencies within a framework of innovation and development.

Evaluation Score:

The student has completed at least 9 of 12 quizzes and has passed the Final Examination with a grade

Dr Andreas Polemitis
Senior Vice-Rector

Date: 24 May 2016

Verify the authenticity of this certificate by comparing its SHA-256 hash to the list of valid hashes within
certificate index document "DFIN511-Index5.pdf", available at http://digitalcurrency.unic.ac.cy/free-introdu
mooc/academic-certificates-on-the-blockchain/ and as otherwise distributed by the University of Nicosia.
index document's SHA-256 hash can be found, prepended with "UNicDC" in the OP_RETURN field in a Bit
transaction originating from address 1zwFAkdz8ZprKdmmXR6yekjAnzRbKLdyNC. The University of Nicosi
authenticated this individual's participation in the course.

Hash of the Index

1ec3cc7497ee0fed85a095775a7e6bf2……..

CERTIFICATES OF ACCOMPLISHMENT

SHA 256 hashes of certificates awarded

137c2a21f5c9601346c8aa4015ee2b809feacd74eed36cf6c0cdd93b28a45cae
1f9e4e28428032b043eaf9ff46678a34ef7bbd56685bc60e6ae083a918c32298
f1d40778baecf262fb237
66c440c74a341aedc7e7
7fc744257280fb5dc5ee4
0bb942699625cbfb2cd6
b7a5c33dd3fbe6ef93e66
8e2bd4b25e36979e9c13
82b2afa75a3617a3672b
6f1f5daa8a6d3d5fdfe8f1
ca92fb3bf1888630219ce
4eca4e3f3307090365b5
2492aa467cbab14db4e2
60c775478165bccd2760
fe14fac85c8eb90d5ad2c
0c23f263e260942f27d974394d7b3cf0f0aaa2ccfb013eec035dab29e0d40d3f
dd0595376d7a6c4a4b893cf5dce242157dd0f7511d6b00d0a7eb9dadf9da03b1
3e9dcb75ebc744f8be916357aa120e5261fafb4fc3e825822f17d3d2dbdca11c
92c7ba6fa5dc507c1937cf5d2b09d4f2476db83b7e8d37e9669188a003860dfb
94dfbabefc05247d1f5e3d2f2362be2f08d08334295ee9f1b5577339fb9822e9
8aac8f6806881a3aad32ce80af0f3ab391aa50f3eb4503c05565307d18633545
4ed974fd04dfa6305e223f15357547740a79b56220cf31e11eb830bd7b535d6f
77dcfa242e3db7c05168eb30e3a25d992048ba4a00e562898e2b5c07544a732b
86a789c9f9f0590ac95835e73b4978379ed794d353afcf026a3f9ab024427453

Output Scripts

OP_DUP OP_HASH160 153a6a28f73ffdee6d7f61acada576a3481b990e OP_EQUALVERIFY OP_CHECKSIG

OP_DUP OP_HASH160 6e03dbf2109692fdcf21e8dbb0569ba376c1c955 OP_EQUALVERIFY OP_CHECKSIG

OP_RETURN 554e6963444320 1ec3cc7497ee0fed85a095775a7e6bf2ada83da6e5c0d127eb9abd9aaeaf00b4
(decoded) UNicDC ��t��턻wZ~k=����'쩘����

Hash of the Certificate

94dfbabefc05247d1f5e3d2f2362be2f0…….

http://bit.ly/2b2WO46

eGovernment

Dubai Wants All Government Documents on Blockchain By 2020

Michael del Castillo (@DelRayMan) | Published on October 5, 2016 at 16:40 BST

NEWS

934 686 58

The Crown Prince of Dubai announced a strategic plan today that would see all government documents secured on a blockchain by 2020.

Revealed at an event hosted by the Dubai Future Foundation and the Smart Dubai Office, the final goal of the government-led initiative is to open the blockchain platform to other cities around the world.

In remarks, Sheikh Hamdan bin Mohammed bin Rashid Al Maktoum explained the effort is part of a larger bid by the emirate, one of seven in the larger UAE, to set the "standard" for smart cities.

He said:

> *"The emirate is building on that achievement by constantly working to foresee the future and keep up with the fourth industrial revolution and all the prospects of increased efficiency that come along with it."*

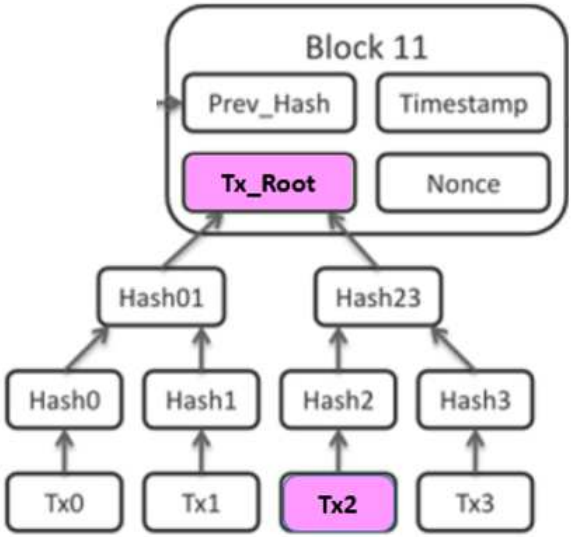
Bitland: Blockchain Land Registry Against 'Corrupt Government'

By ***Jamie Redman*** - May 26, 2016 4970 1

A new project piloted in West Africa, called Bitland, is using blockchain technology as a decentralized land registry.

http://bit.ly/2e5s98X

Transactions & Applications

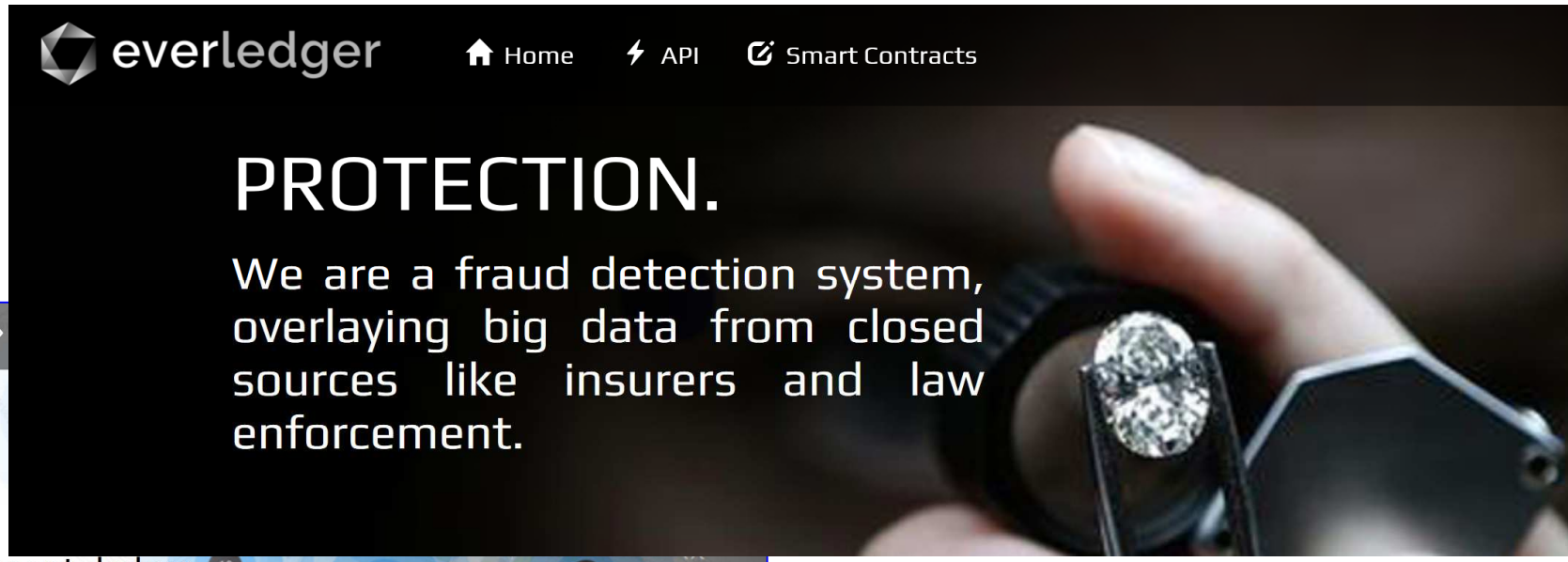


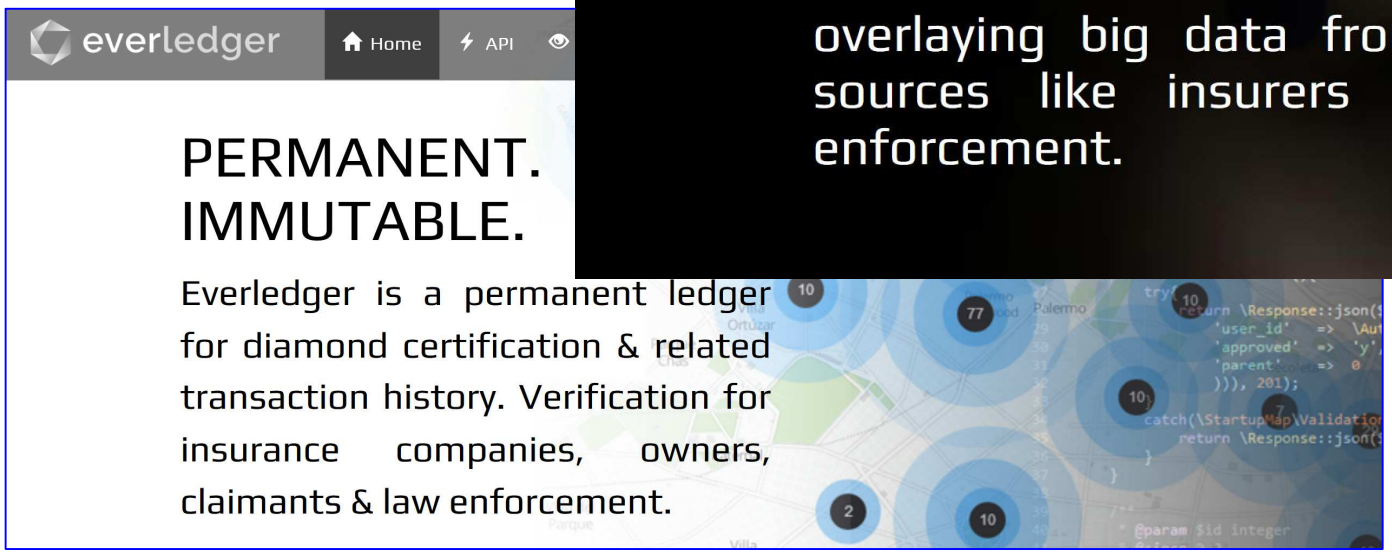
- Enregistrement d'un transfert de valeur

- Enregistrement d'une chaîne de caractères (e.g "Hash" dans la Blockchain du Bitcoin)

- Smart Contract (Ethereum)

Everledger – Diamond certification &tracking on the Blockchain

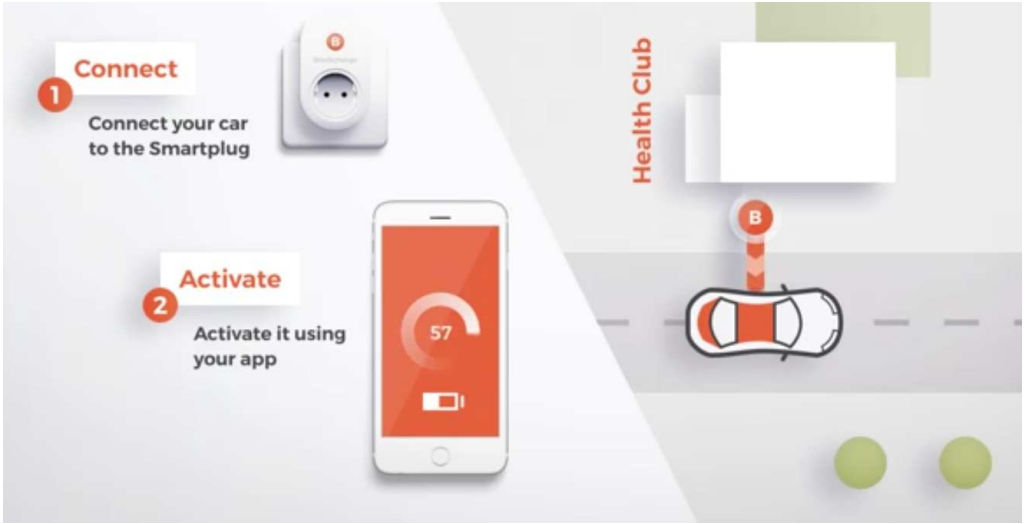




Micro-facturation électrique par un Smart Contract

slock.it

RWE
The energy to lead



http://bit.ly/2euwuyj

Conclusion

Comment démarrer ?

Comment démarrer ?

bread wallet

BITY
bity.com