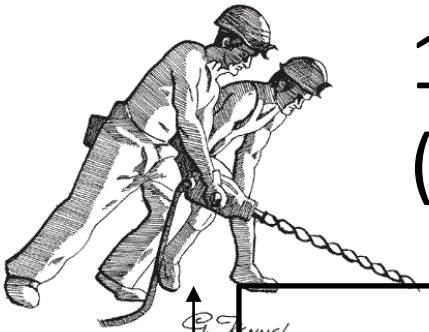
Blockchain
Bitcoin & Ethereum

Pascal.Urien@Telecom-ParisTech.fr

"Bitcoin: A Peer-to-Peer Electronic Cash System." Satoshi Nakamoto

- In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions
- 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

Mining Bitcoin



144 blocks/day
(Fix Mining Rate)

$10{,}5 \times 10^6$ BTC

4 years	50%		50 BTC/block (144x50)
4 years	25%		25 BTC/block (144x25)
4 years	12,5%		12,5 BTC/block (144x12,5)

Difficulty (i.e. costs) increases

The number of Bitcoin is finite

210,000 blocks

Initial Block Reward (IBR)

$$N_S = N_B \times \sum_{i=0}^{i=32} 50 \times 10^8 / 2^i$$

(in satoshi)

1 BTC = 10^8 satoshi

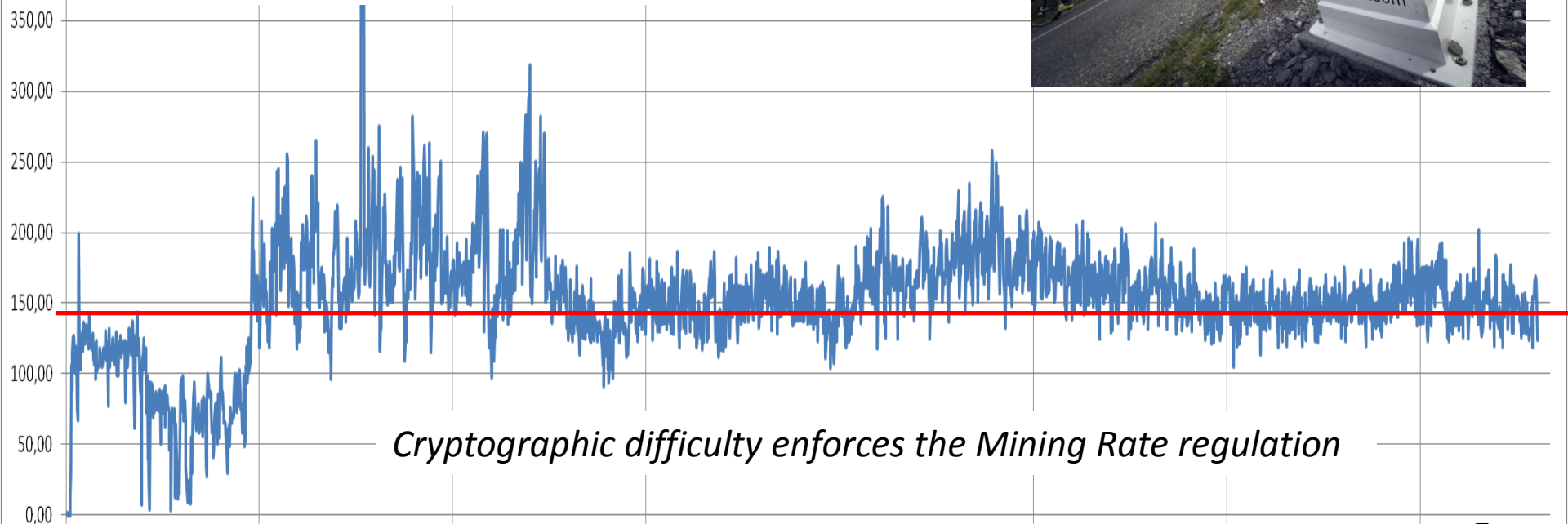
The block reward started at 50 BTC in 2009

It halves every 210,000 blocks (about 4 years, = 144x 1461)

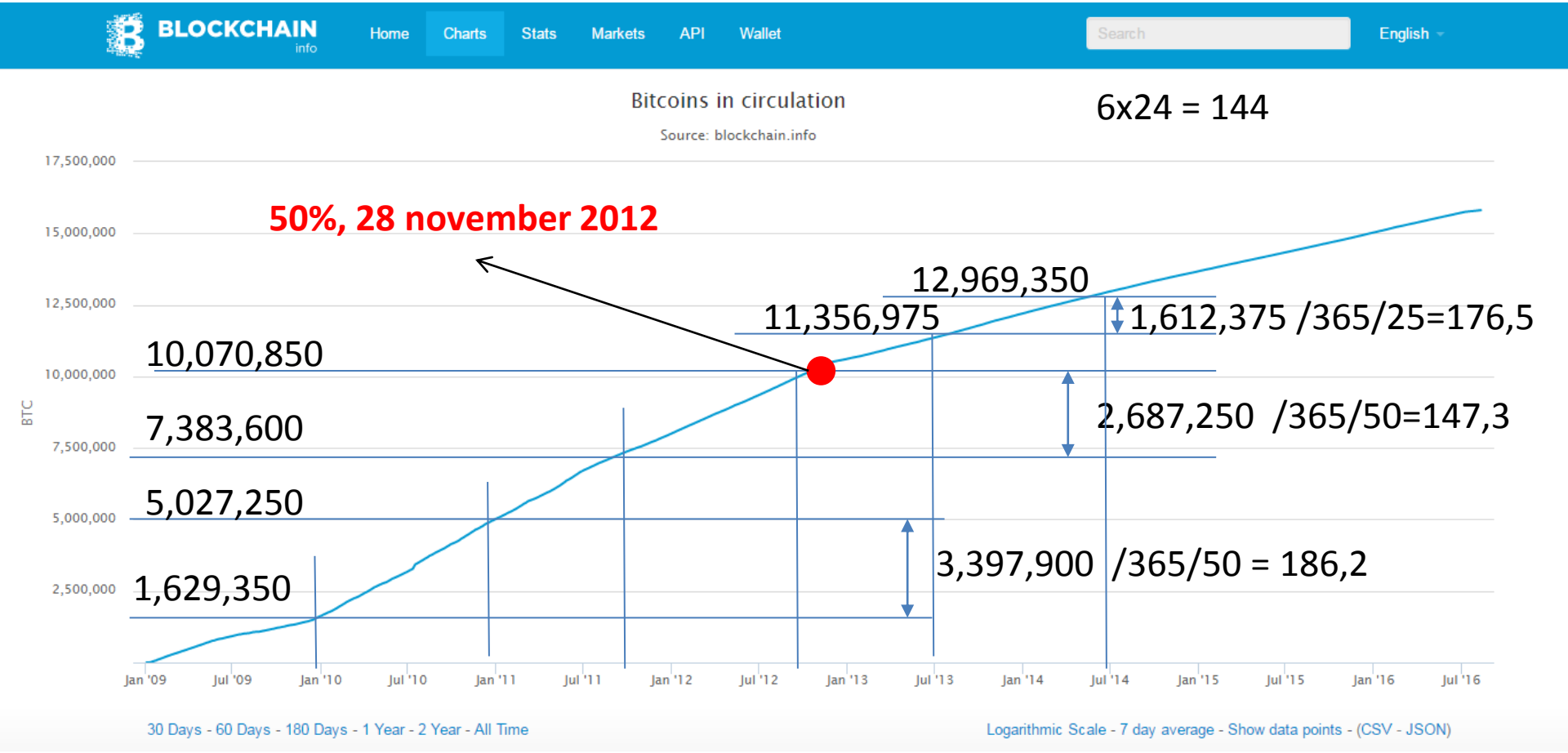
It will stop with the block number 6,930,000 (=33x 210,000, $33 = 1 + \log_2(5.10^9)$)

This mechanism limits the total number of Bitcoins in circulation to 21 millions (210,000 x 50 x 2)

The Mining Rate:
6x24 = 144 blocks / day



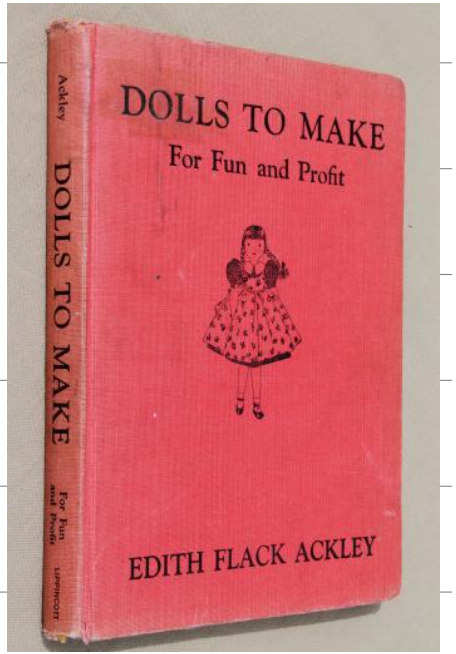
Cryptographic difficulty enforces the Mining Rate regulation


BLOCKCHAIN info
Home
Charts
Stats
Markets
API
Wallet
Search
English
Bitcoins in circulation
Source: blockchain.info
6x24 = 144
50%, 28 november 2012
17,500,000
15,000,000
12,500,000
10,000,000
7,500,000
5,000,000
2,500,000
BTC
12,969,350
11,356,975
1,612,375 /365/25=176,5
10,070,850
2,687,250 /365/50=147,3
7,383,600
5,027,250
3,397,900 /365/50 = 186,2
1,629,350
Jan '09
Jul '09
Jan '10
Jul '10
Jan '11
Jul '11
Jan '12
Jul '12
Jan '13
Jul '13
Jan '14
Jul '14
Jan '15
Jul '15
Jan '16
Jul '16
30 Days - 60 Days - 180 Days - 1 Year - 2 Year - All Time
Logarithmic Scale - 7 day average - Show data points - (CSV - JSON)

The Difficulty of the PoW

- A nonce value that make a double SHA-256 hash of the block's header that is less
  - (65535 << 208) / difficulty
- So the entropy of this calculation is closed to 32+log2(difficulty), about 70 bits in August 2016.
- The difficulty is scaled every 2016 blocks in order to maintain a block production every 10 minutes, i.e. about 144 (6x24) per day.

The Profit (Bitcoin/day)



9300 (50 btc /block)

7365 (50 btc / block)

4412 (25 btc /block)

Blockchain: a public ledger

Bitcoin 12LZjvQBy31ABRpqvMZQbu7S9K5SxaifjW in Block 96188

Full Bitcoin Block 96188

Share:

block, address, transaction | Search

PREVIOUS BLOCK

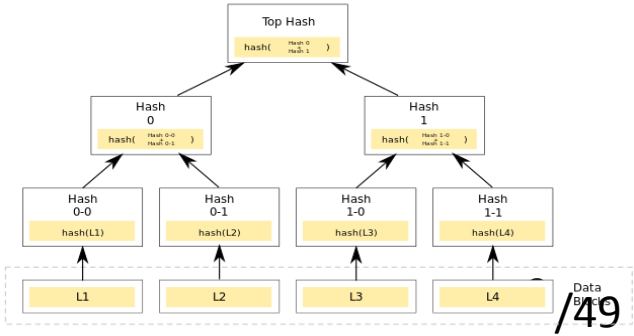
NEXT BLOCK

Number Of Transactions	4
Output Total	91.24 BTC
Height	96188
Time	2010-12-07 13:57:40
Difficulty	8,078.19525793
Bits	453516498
Version	1
Nonce	944968343
Block Reward	50 BTC
Days Destroyed	2

PoW

Hash	000000000004d6e22b42bf66fd9cad1977bdee13abab1e51a2d03ca22e6f71af
Previous Block	0000000000027c094bf08f7c27a6debcb5f36419bf53390e3e1c40a653e2195c
Next Block(s)	0000000000042c9d08f3f06d502a247f090625fb6c7623cf956a38e987c59e0f
Merkle Root	26ab6b697b8e06416b2fe5047f558c997af0a9c36e6a6eae79ff59745b5065a1

Transaction identifiers are stored in a Merkle Tree

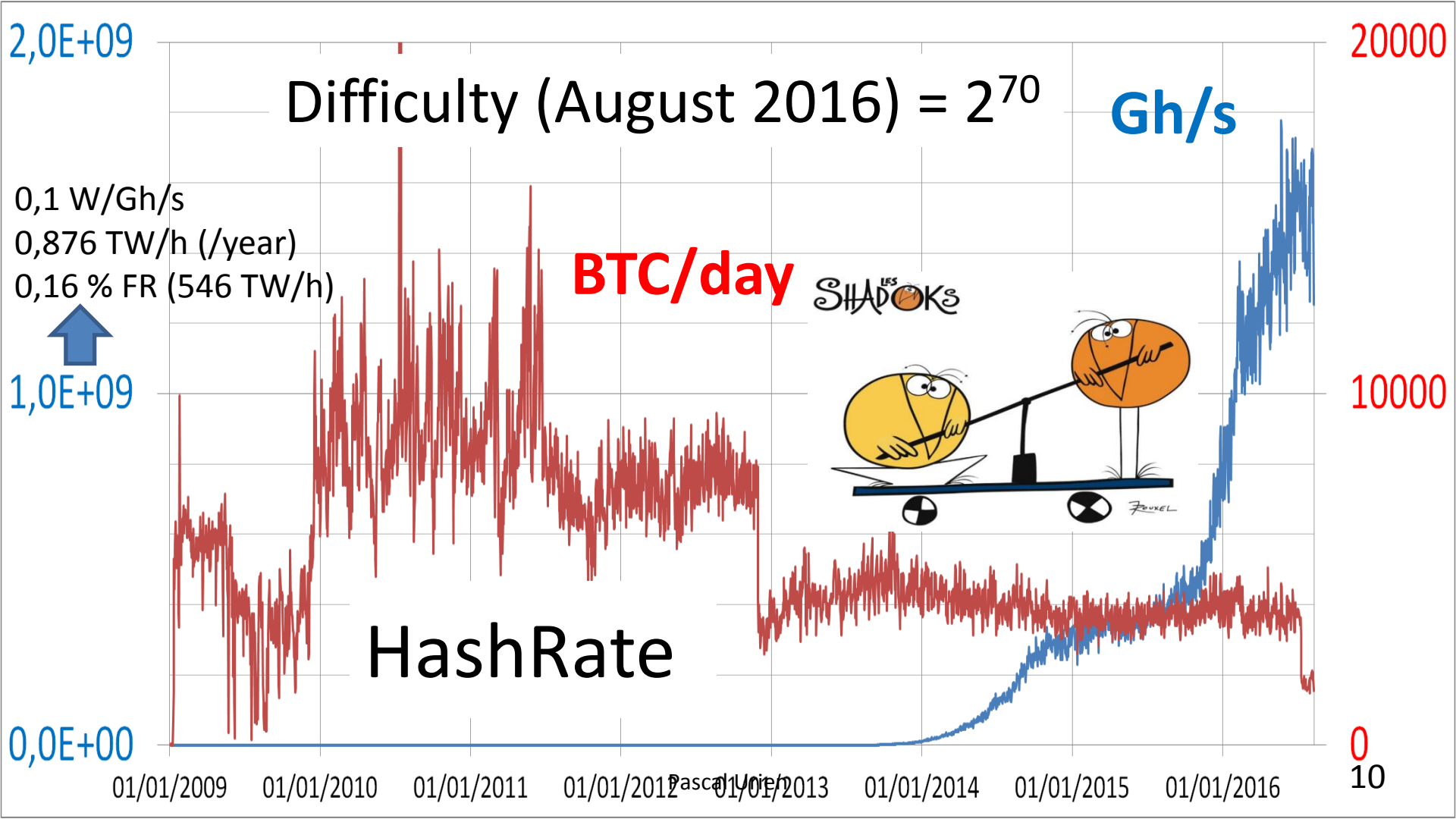


tx:d4a73f51ab7ee7acb4cf0505d1fab34661666c461488e58ec30281e2becd93e2 33.59 BTC Fee: 0 BTC

prev tx 1689LPUuixaxSchENLMNaNbS3hYVgdpaSS	-33.59 BTC	13RoCeq4K8ddPW6ugcheFoXK4GC2BLVuET	0.05 BTC next tx
		12LZjvQBy31ABRpqvMZQbu7S9K5SxaifjW	33.54 BTC next tx

https://bitinfocharts.com/bitcoin/search.html

Pascal Urien


2,0E+09
1,0E+09
0,0E+00
20000
10000
0
Difficulty (August 2016) = 2^70
Gh/s
0,1 W/Gh/s
0,876 TW/h (/year)
0,16 % FR (546 TW/h)
BTC/day
HashRate
LES SHADOKS
01/01/2009
01/01/2010
01/01/2011
01/01/2012
01/01/2013
01/01/2014
01/01/2015
01/01/2016
Pascal Urien
10

The HashRate Cost (estimation)

Energy Rig Cost/day

Year	C_1=W/Gh/s	C_2=$/Gh/s/day
2009-2010	4000	68,5
2011	500	2,73
2012	100	2,05
2013	10	0,055
2014	1	$2,3\ 10^{-3}$
2015-2017	0,1	$1,6\ 10^{-4}$

Bitcoin double SHA256 ASIC mining hardware

Product	Advertised Mhash/s	Mhash/J	Mhash/s/$	Watts	Price (USD)	Currently shipping	Comm p
AntMiner S9 [9]	14,000,000	10182	5833	1,375	2,400	Yes	Ethernet
AntMiner S7 [8]	4,860,000	4000	2666	1,210	1,823	No	Ethernet
[illegible] [7]	[illegible]	[illegible]	[illegible]	[illegible]	2,307	No	Ethernet
					370	Discontinued	Ethernet
					2075	Discontinued	Ethernet
					1309[2]	Discontinued	Ethernet
					2235	Discontinued	Ethernet
					4121	Discontinued	Ethernet
		1429	1429	1400	1400	Discontinued	Ethernet
KnC Neptune [24]	3,000,000				2995 [24]	Discontinued	Ethernet
BFL Monarch 700GH/s[19]	700,000				379	Yes	PCIe, USB
ASICMiner BE Prisma [15]	1,400,000				00[2]	Discontinued	Proprietary
AntMiner S3 [4]	441,000				82[2]	Discontinued	Ethernet
bi*fury	5,000				09	Discontinued	USB
Twinfury	4,500				16	Discontinued	USB
Spondooliestech SP10	1,400,000	1120	492	1250	2845	Discontinued	Ethernet

The Costs (Estimation)

Year	2009 2010	2011	2012	2013	2014	2015 2016
C_1 x E $/Gh/s	14,4	1,8	$3,6\ 10^{-1}$	$3,6\ 10^{-2}$	$3,6\ 10^{-3}$	$3,6\ 10^{-4}$
C_2 $/Gh/s	68,5	2,73	2,05	$5,5\ 10^{-2}$	$2,3\ 10^{-3}$	$1,6\ 10^{-4}$

$E = 0,0036 = 0,15\ 10^{-3} \times 24$ $\quad$ $0,15\ \$ / KWh = 0,15\ 10^{-3}\ \$ / Wh$

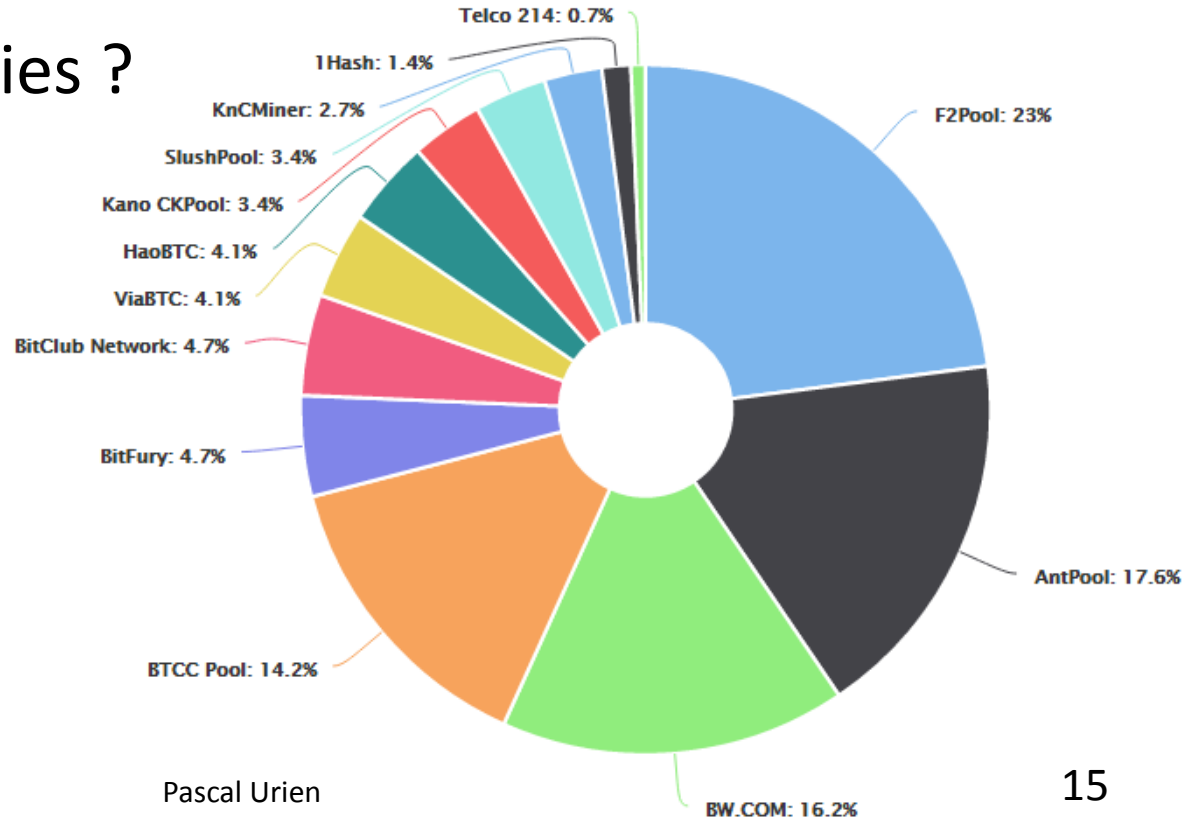
$$TotalCosts = C_1 \times E \times HashRate + C_2 \times HashRate$$

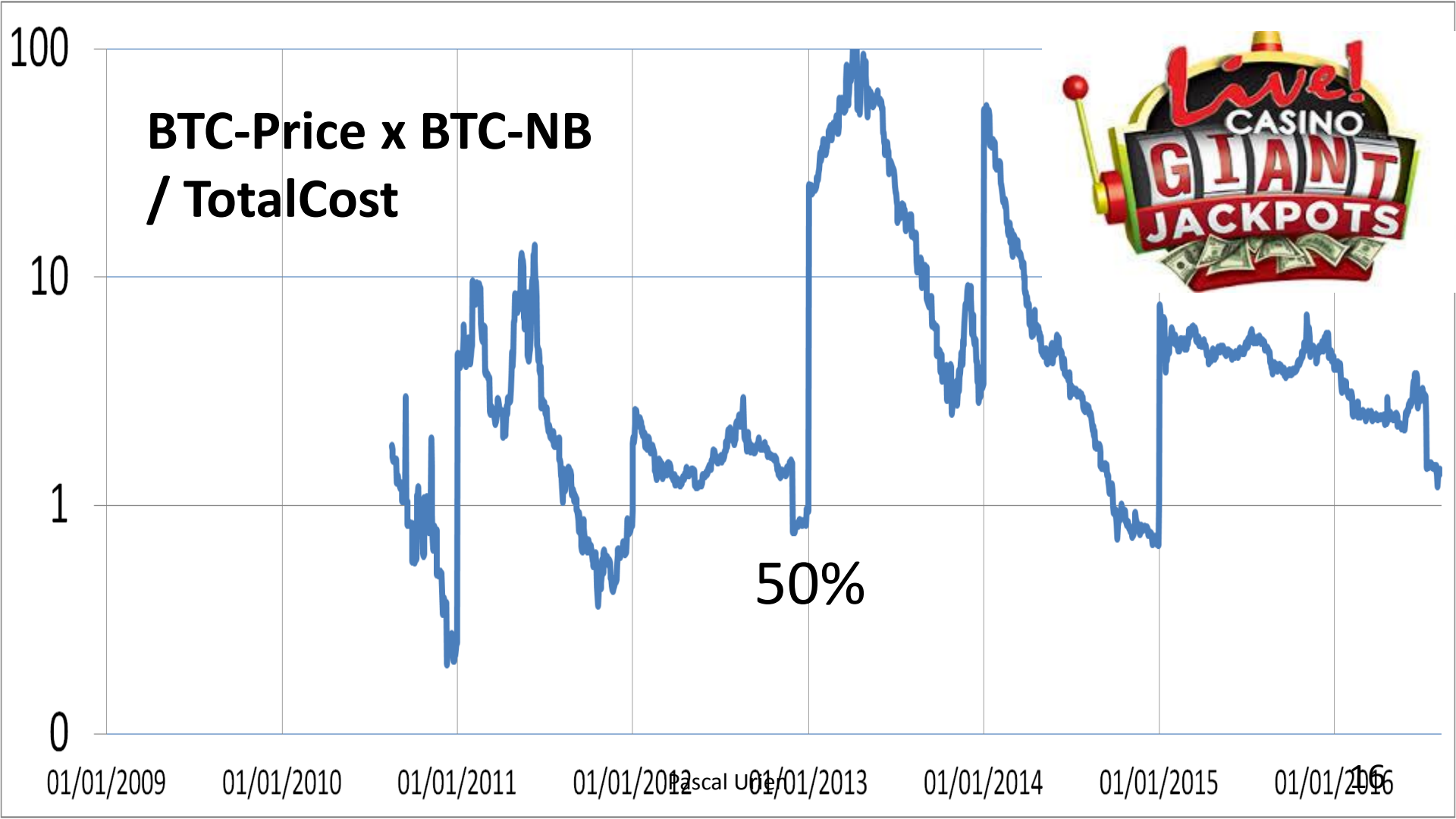
Mid August 2016 (estimation)

- Market capitalization: 9,6 billion$ (BTC-price x #BTC)
- Total energy cost: 0,36 billion$.
- Total rig cost: 0,24 billion$.

The Actors of the HashRate

No Trusted Third Parties ?




BTC-Price x BTC-NB
/ TotalCost
100
10
1
0
50%
01/01/2009
01/01/2010
01/01/2011
01/01/2012
01/01/2013
01/01/2014
01/01/2015
01/01/2016
Live! CASINO GIANT JACKPOTS

Trading: The Jean Mira Formula

$$BTC\text{-}Price(t) = EnergyCost(t) + \varepsilon1(t) + \varepsilon2(t) + \varepsilon3(t)$$

EnergyCost= C_1 x E x hashrate / BTC-NB

ε1 = C_2 x hashrate / BTC-NB

ε2 = Market Prime

ε3 = BTC-Price x Transaction-Fees / BTC-NB

August 12nd 2016
BTC-Price: 589.23 $,
Hashrate: 1,585,714,220 GH/s,
BTC-NB: 1975
Transaction-Fees: 70 BTC

EnergyCost= 289 $
ε1 = 128 $ (3 years)
ε3 = 21 $
Market Prime = 151,23 $

The Bitcoin Address

- A *Bitcoin Address* is computed from a 160-bit hash (called *Hash160*) of the public portion of a public/private ECDSA key pair. The elliptic curve is the sepc256k1.

```
Sepc256k1 PublicKey:
04
9C02BFC97EF236CE6D8FE5D94013C721
E915982ACD2B12B65D9B7D59E20A8420
05F8FC4E02532E873D37B96F09D6D451
1ADA8F14042F46614A4C70C0F14BEFF5
```

Hash160:
1689LPUuixaxSchENLMNaNbS3hYVgdpaSS

Bitcoin address:
12PNZxbhBzDXTZJzZEkrynszzQr9bB

http://bitcoinvalued.com/tools.php

Transaction

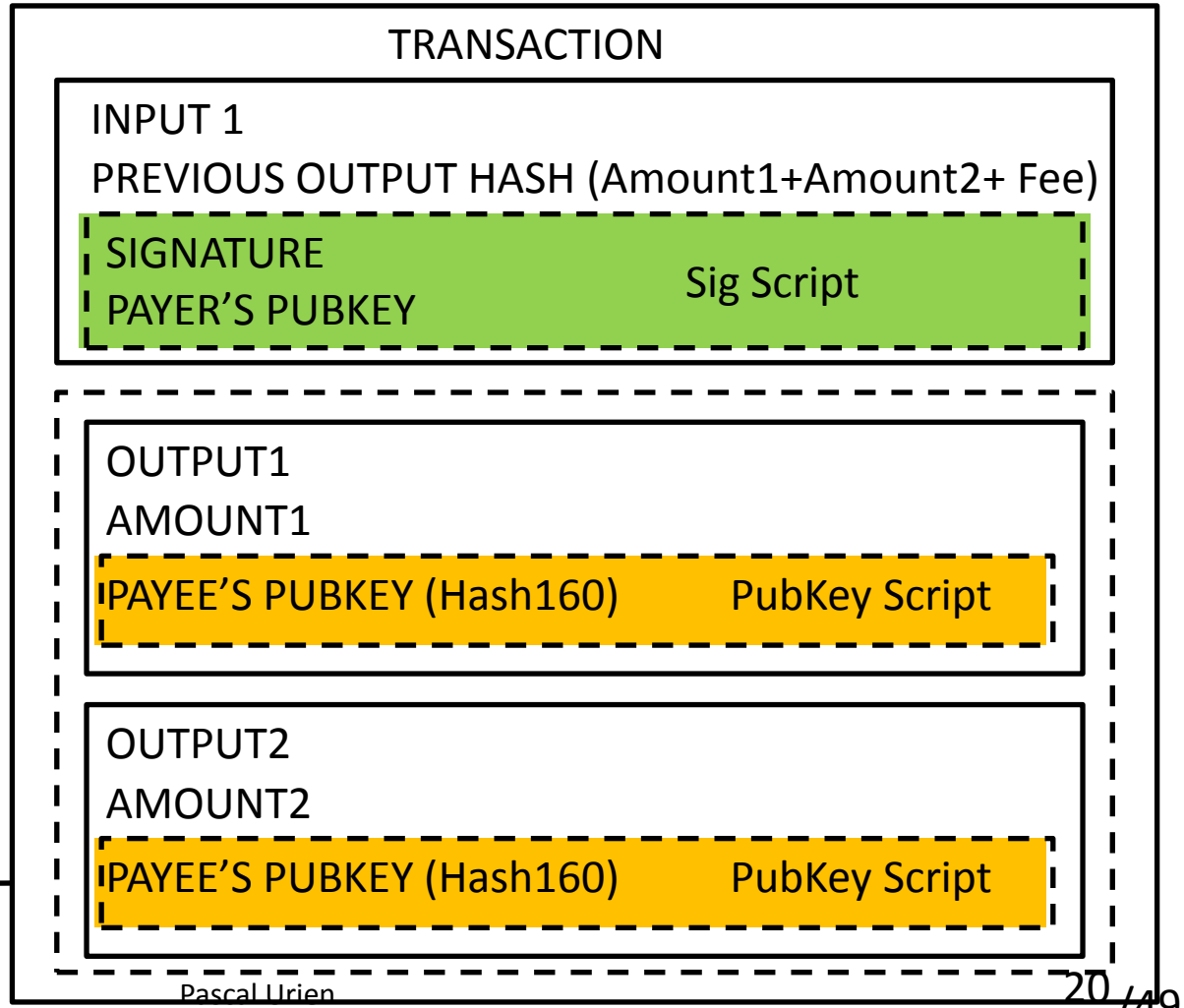
- A bitcoin address is associated to a set of *Unspent Transaction Output*, or UTXO.
- Transaction are identified by a hash (SHA256) value (tx, transcation identifier)
- All UTXOs included in a transaction must be spent.
- A transaction message typically includes
  - an ECDSA signature generated by the input address,
  - the payer's public key,
  - a previous transaction hash (UTXO),
  - and Bitcoin transfer operations (outputs) in which every payee is identified by its Hash160 attribute, computed from its associated public key.
- The transaction fee is the difference (if any) between the sum of input amounts (UTXOs) and output transfers.
- In a transaction two kinds of scripts are executed
  - Input script (signature checking)
  - Output script (address checking)

Transaction

Σ input =
Σ output + Fee

Fee= Σ input
- Σ output

txHash



Transaction Example

- Transaction ID
  - d4a73f51ab7ee7acb4cf0505d1fab34661666c461488e58ec30281e2becd93e2
  - https://blockchain.info/tx/d4a73f51ab7ee7acb4cf0505d1fab34661666c461488e58ec30281e2becd93e2
- Payer
  - 1689LPUuixaxSchENLMNaNbS3hYVgdpaSS
  - UTXO
    - 2936ee6a0db4e4901988503bb6e966128dd5fa01bcf08451f78a1d5b08dbbd6d
    - Amount 33,59 BTC
- Payee
  - 12LZjvQBy31ABRpqvMZQbu7S9K5SxaifjW, Amount 33,54
  - 13RoCeq4K8ddPW6ugcheFoXK4GC2BLVuET, Amount 0,05

```
Message header: transaction

F9 BE B4 D9 //main network magic bytes
74 78 00 00 00 00 00 00 00 00 00 00 // "tx" command
02 01 00 00 // payload is 258 bytes long
E2 93 CD BE //checksum of payload Transaction:
01 00 00 00 // version
Inputs:
01       // number of transaction inputs    tx# 2936ee6a0db4e4901988503bb6e966128dd5fa01bcf08451f78a1d5b08dbbd6d  33,59 BTC
Input 1: // hash de la transaction précédente
6D BD DB 08 5B 1D 8A F7 51 84 F0 BC 01 FA D5 8D  previous output (!!! Big Endian)
12 66 E9 B6 3B 50 88 19 90 E4 B4 0D 6A EE 36 29

00 00 00 00  //index output of previous tx

8B (length)
48 (length)          INPUT SCRIPT (SigScript)
 30 45
  02 21 //r (ECDSA)
     00 F3 58 1E 19 72 AE 8A C7 C7 36 7A 7A 25 3B C1
     13 52 23 AD B9 A4 68 BB 3A 59 23 3F 45 BC 57 83
     80
   02 20 //s (ECDSA)
     59 AF 01 CA 17 D0 0E 41 83 7A 1D 58 E9 7A A3 1B
     AE 58 4E DE C2 8D 35 BD 96 92 36 90 91 3B AE 9A

01 41 // Public Key 1689LPUuixaxSchENLMNaNbS3hYVgdpaSS
     04
     9C 02 BF C9 7E F2 36 CE 6D 8F E5 D9 40 13 C7 21 // Gx
     E9 15 98 2A CD 2B 12 B6 5D 9B 7D 59 E2 0A 84 20
     05 F8 FC 4E 02 53 2E 87 3D 37 B9 6F 09 D6 D4 51 // Gy
     1A DA 8F 14 04 2F 46 61 4A 4C 70 C0 F1 4B EF F5

FF FF FF FF sequence
```

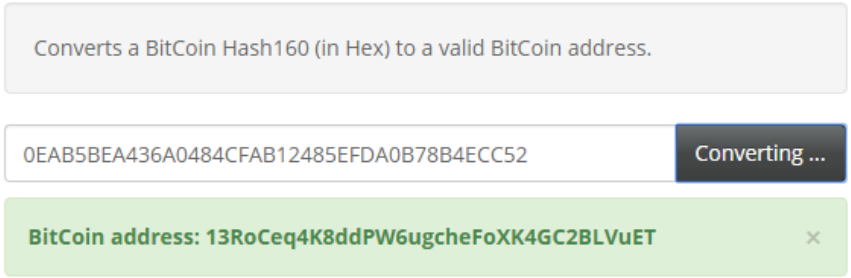
https://en.bitcoin.it/wiki/Transaction

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.

https://bitcoin.org/en/developer-guide#transactions

```
Outputs:
02  // 2 Output Transactions


Output 1:
80 FA E9 C7 00 00 00 00 // 33,54 BTC (satoshi little indian)
19                      // scriptPubkey is 25 bytes long
// pk_script: 12LZjvQBy31ABRpqvMZQbu7S9K5SxaifjW
76 A9 14
1A A0 CD 1C BE A6 E7 45 8A 7A BA D5 12 A9 D9 EA 1A FB 22 5E
88 AC

Output 2:
40 4B 4C 00 00 00 00 00 // 0,05 BTC, (satoshi little indian)
19              // script Pubkey is 25 bytes long
// pk_script: 13RoCeq4K8ddPW6ugcheFoXK4GC2BLVuET
76 A9 14
0E AB 5B EA 43 6A 04 84 CF AB 12 48 5E FD A0 B7 8B 4E CC 52
88 AC

Locktime:
00 00 00 00 // locktime

Hash_type code
01 00 00 00
```

http://bitcoinvalued.com/tools.php



1AA0CD1CBEA6E7458A7ABAD512A9D9EA1AFB225E
12LZjvQBy31ABRpqvMZQbu7S9K5SxaifjW

0EAB5BEA436A0484CFAB12485EFDA0B78B4ECC52
13RoCeq4K8ddPW6ugcheFoXK4GC2BLVuET

```
scriptPubkey: OP_DUP=76 OP_HASH160=A9 longueur=20 <pubkeyHash> OP_EQUALVERIFY=88 OP_CHECKSIG=AC
scriptSig:    <signature> <pubkey>
```

https://en.bitcoin.it/wiki/OP_CHECKSIG

https://blockchain.info/tx/d4a73f51ab7ee7acb4cf0505d1fab34661666c461488e58ec30281e2becd93e2?show_adv=true

Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary	
Address	1689LPUuixaxSchENLMNaNbS3hYVgdpaSS
Hash 160	38327f6c788fa75d420fa0b5785f6d7db404de34
Tools	Taint Analysis - Related Tags - Unspent Outputs

Transactions	
No. Transactions	2
Total Received	33.59 BTC
Final Balance	0 BTC

Request Payment | Donation Button

Transactions (Oldest First)

Filter

d4a73f51ab7ee7acb4cf0505d1fab34661666c461488e58ec30281e2becd93e2 — 2010-12-07 12:57:40

1689LPUuixaxSchENLMNaNbS3hYVgdpaSS	13RoCeq4K8ddPW6ugcheFoXK4GC2BLVuET	0.05 BTC
	12LZjvQBy31ABRpqvMZQbu7S9K5SxaifjW	33.54 BTC
		-33.59 BTC

input

2936ee6a0db4e4901988503bb6e966128dd5fa01bcf08451f78a1d5b08dbbd6d — 2010-12-07 11:21:25

1MjuzaQqFwn3bqVKNzAVDKVU9bQj6VWBiJ	1689LPUuixaxSchENLMNaNbS3hYVgdpaSS	33.59 BTC
		33.59 BTC

Block

Bitcoin 12LZjvQBy31ABRpqvMZQbu7S9K5SxaifjW in Block 96188

Full Bitcoin Block 96188

Share:

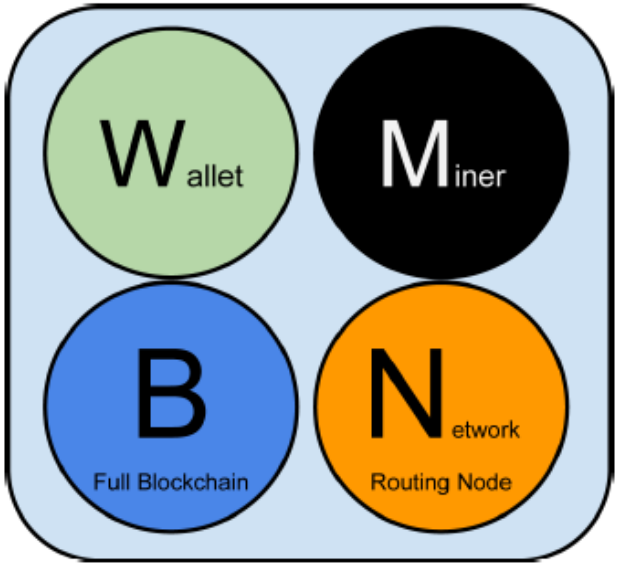
block, address, transaction Search

Number Of Transactions	4
Output Total	91.24 BTC
Height	96188
Time	2010-12-07 13:57:40
Difficulty	8,078.19525793
Bits	453516498
Version	1
Nonce	944968343
Block Reward	50 BTC
Days Destroyed	2
Hash	000000000004d6e22b42bf66fd9cad1977bdee13abab1e51a2d03ca22e6f71af
Previous Block	0000000000027c094bf08f7c27a6debcb5f36419bf53390e3e1c40a653e2195c
Next Block(s)	0000000000042c9d08f3f06d502a247f090625fb6c7623cf956a38e987c59e0f
Merkle Root	26ab6b697b8e06416b2fe5047f558c997af0a9c36e6a6eae79ff59745b5065a1

tx d4a73f51ab7ee7acb4cf0505d1fab34661666c461488e58ec30281e2becd93e2 33.59 BTC Fee: 0 BTC

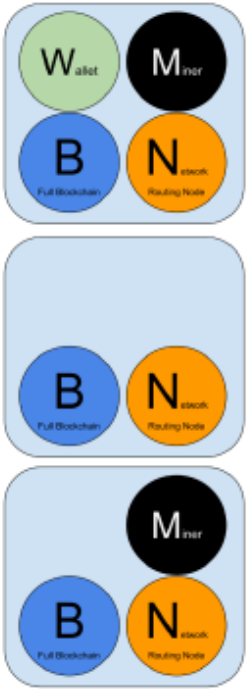
prev tx	1689LPUuixaxSchENLMNaNbS3hYVgdpaSS -33.59 BTC	13RoCeq4K8ddPW6ugcheFoXK4GC2BLVuET	0.05 BTC next tx
		12LZjvQBy31ABRpqvMZQbu7S9K5SxaifjW	33.54 BTC next tx

Network



A bitcoin node is a collection of functions:
- Routing ,
- Blockchain database,
- Mining,
- Wallet Services.

Network



Reference Client (Bitcoin Core)

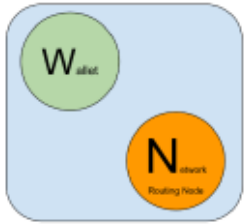
Contains a Wallet, Miner, full Blockchain database, and Network routing node on the bitcoin P2P network.

Full Block Chain Node

Contains a full Blockchain database, and Network routing node on the bitcoin P2P network.

Solo Miner

Contains a mining function with a full copy of the blockchain and a bitcoin P2P network routing node.



Lightweight (SPV) wallet

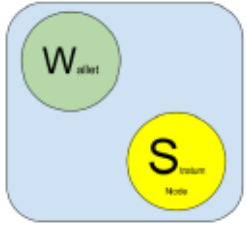
Contains a Wallet and a Network node on the bitcoin P2P protocol, without a blockchain.

Pool Protocol Servers

Gateway routers connecting the bitcoin P2P network to nodes running other protocols such as pool mining nodes or Stratum nodes.

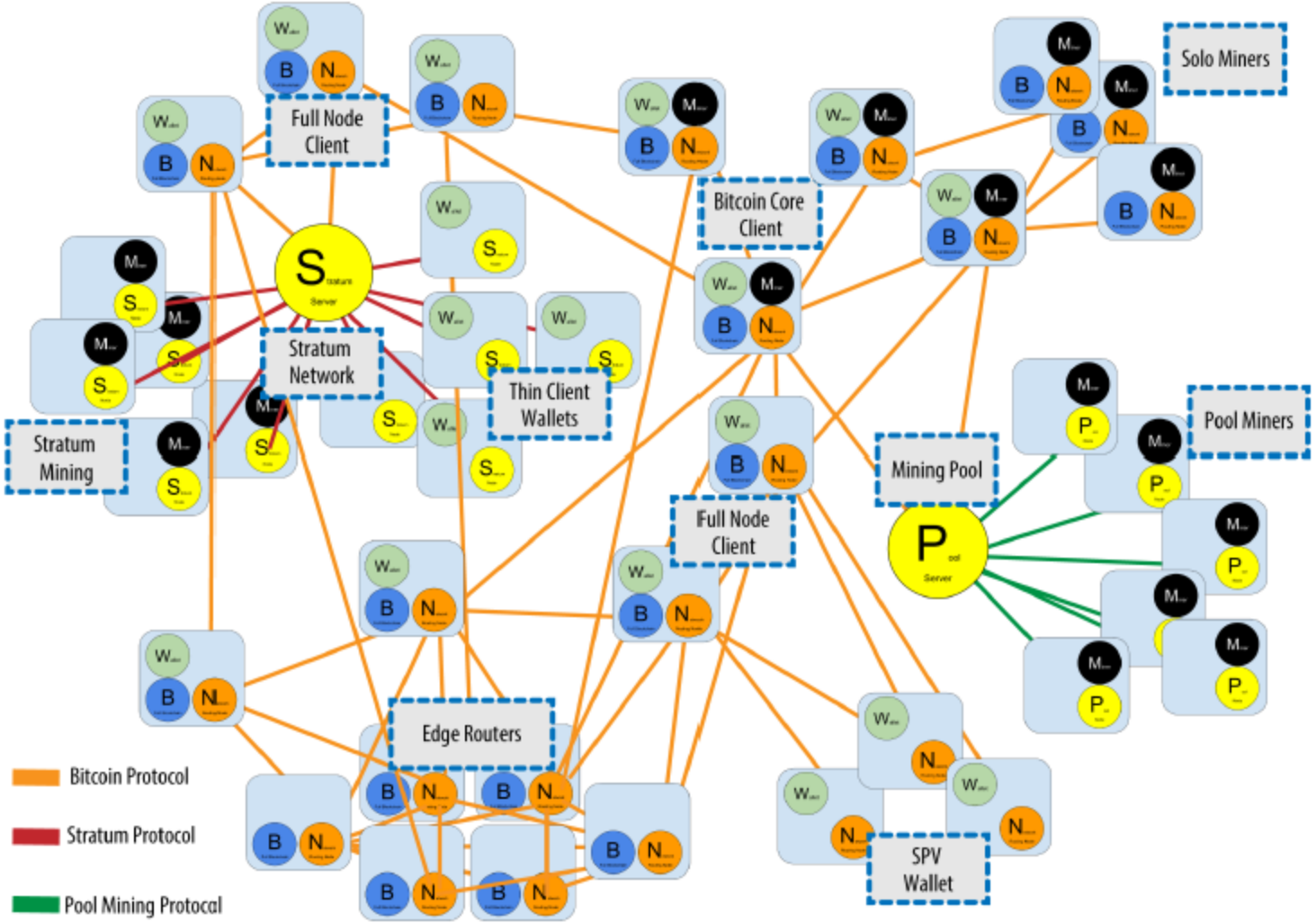
Mining Nodes

Contain a mining function, without a blockchain, with the Stratum protocol node (S) or other pool (P) mining protocol node.



Lightweight (SPV) Stratum wallet

Contains a Wallet and a Network node on the Stratum protocol, without a blockchain.


Solo Miners
Full Node Client
Bitcoin Core Client
Stratum Network
Thin Client Wallets
Stratum Mining
Pool Miners
Mining Pool
Full Node Client
Edge Routers
SPV Wallet
Bitcoin Protocol
Stratum Protocol
Pool Mining Protocal

About Ethereum

- Ethereum was introduced in a white paper by Vitalik Buterin in 2013
- The Ethereum software project was initially developed in early 2014 by the Swiss company, *Ethereum Switzerland GmbH,* and a a Swiss non-profit foundation, the Ethereum Foundation (*Stiftung Ethereum*).
- Ethereum's live blockchain was launched on 30 July 2015
- Ethereum is a blockchain platform supporting a digital currency *the Ether* and distributed applications called *Smart Contrats* written in *Serpent* or other languages.
  - The Ethereum Virtual Machine (EVM) supports a Turing complete language
- 1 ETHER = 10^{18} Wei.

Ethereum is a BlockChain

- A new block is mined every 14,0 s
- The Block reward is 5 Ethers
- Transactions are stored in the blockchain
- Every account is defined by a pair of keys (ECC sepc256k1), a private key and public key.
  - Accounts are indexed by their *address* which is derived from the public key by taking the last 20 bytes.

Account

- An Ethereum account contains four fields:
  - The **nonce**, a counter used to make sure each transaction can only be processed once
    - A scalar value equal to the number of transactions sent by the sender
  - The account's current **Ether balance**
  - The account's **contract code**, if present
  - The account's **storage** (empty by default)

Transactions Structure

- The recipient of the message
- A signature identifying the sender
- A nonce: a scalar value equal to the number of transactions sent by the sender
- Value:
  - a scalar value equal to the number of Wei to be transferred to the message call's recipient
  - or in the case of contract creation, as an endowment to the newly created account
- An optional data field
  - a contract creation transaction contains an unlimited size byte array specifying the EVM-code for the account initialization procedure
  - A message call transaction contains an unlimited size byte array specifying the input data of the message
- A STARTGAS value, representing the maximum number of computational steps the transaction execution is allowed to take
- A GASPRICE value, representing the fee the sender pays per computational step
  - A scalar value equal to the number of Wei to be paid per unit of gas
  - Transactors are free to specify any gasPrice that they wish, however miners are free to ignore transactions as they choose.

Mining

- Ethash is the PoW algorithm for Ethereum 1.0.
  - It is based on the sha3_512 hash function
- Proof of stake is a consensus algorithm for public blockchains which is intended to serve as an alternative to proof of work.
- The successful PoW miner receives a static block reward that of 5 Ether.
- The successful miner will also receive all the gas in fees that it generates from the transactions in the block that it verifies.
- The miner also receives an award of 1/32 per Uncle block included.
- The uncle reward formula is (U_n + 8 - B_n) * R / 8 where R is the static reward of 5, U_n is the uncle number and B_n is the block number
  - (U_n + 8 - B_n) * 5 / 8
  - Uncle 0 : 4.375 ETH = 7/8 * 5
  - Uncle 1 : 3.750 ETH = 6/8 * 5
- The reward for contract processing is
  - STARTGAS * GASPRICE

For both reasons, there are two important goals of the proof-of-work function; firstly, it should be as accessible as possible to as many people as possible. The requirement of, or reward from, specialized and uncommon hardware should be minimized. This makes the distribution model as open as possible, and, ideally, makes the act of mining a simple swap from electricity to Ether at roughly the same rate for anyone around the world.
Secondly, it should not be possible to make super-linear prots, and especially not so with a high initial barrier. Such a mechanism allows a well-funded adversary to gain a troublesome amount of the network's total mining power and as such gives them a super-linear reward (thus skewing distribution in their favour) as well as reducing the network security.
One plague of the Bitcoin world is ASICs. These are specialized pieces of compute hardware that exist only to do a single task. In Bitcoin's case the task is the SHA256 hash function. While ASICs exist for a proof-of-work function, both goals are placed in jeopardy. Because of this, a proof-of-work function that is ASIC-resistant (i.e. difficult or economically inefficient to implement in specialized compute hardware) has been identified as the proverbial silver bullet.

Ether Transaction

Block Information

Height:	< Prev 100004 Next >
TimeStamp:	535 days 7 hrs ago (Aug-17-2015 08:12:48 AM +UTC)
Transactions:	1 transaction and 0 contract internal transactions in this block
Hash:	0xf93283571ae16dcecbe1816adc126954a739350cd1523a1559eabeae155fbb63
Parent Hash:	0x73d88d376f6b4d232d70dc950d9515fad3b5aa241937e362fdbfd74d1c901781
Sha3Uncles:	0x2fa1a023371ad24d50a93e91accf6344c7516ab78690ea6487a495a36dcef6bc
Mined By:	0x909755d480a27911cb7eeeb5edb918fae50883c0 IN 9 secs
Difficulty:	3,849,295,379,889
Total Difficulty:	169,441,428,916,529,325
Size:	1202 bytes
Gas Limit:	3,141,592
Gas Used:	21,000
Nonce:	0x1a455280001cc3f8
Block Reward:	5.157396364338084 Ether (5 + 0.001146364338084 + 0.15625)
Uncles Reward:	3.75 Ether (1 Uncle at Position 0)
Extra Data:	Geth/v1.0.1-98100f47/linux/go1.4 (Hex:0x476574682f76312e302e312d393831303066343 72f6c696e75782f676f312e34)

Transaction Gas Fee

Static Block Reward

5 ether/32 / uncle

Transaction Information

TxHash:	0x6f12399cc2cb42bed5b267899b08a847552e8c42a64f5eb128c1bcbd1974fb0c
Block Height:	100004 (3010043 block confirmations)
TimeStamp :	535 days 7 hrs ago (Aug-17-2015 08:12:48 AM +UTC)
From:	0xcf00a85f3826941e7a25bfcf9aac575d40410852
To:	0xd9666150a9da92d9108198a4072970805a8b3428
Value:	5 Ether ($53.10)
Gas:	90000
Gas Price:	0.000000054588778004 Ether
Gas Used By Transaction:	21000
Actual Tx Cost/Fee:	0.00114636433808 Ether ($0.01)
Cumulative Gas Used:	21000
Nonce:	25
Input Data:	0x

Transaction Details

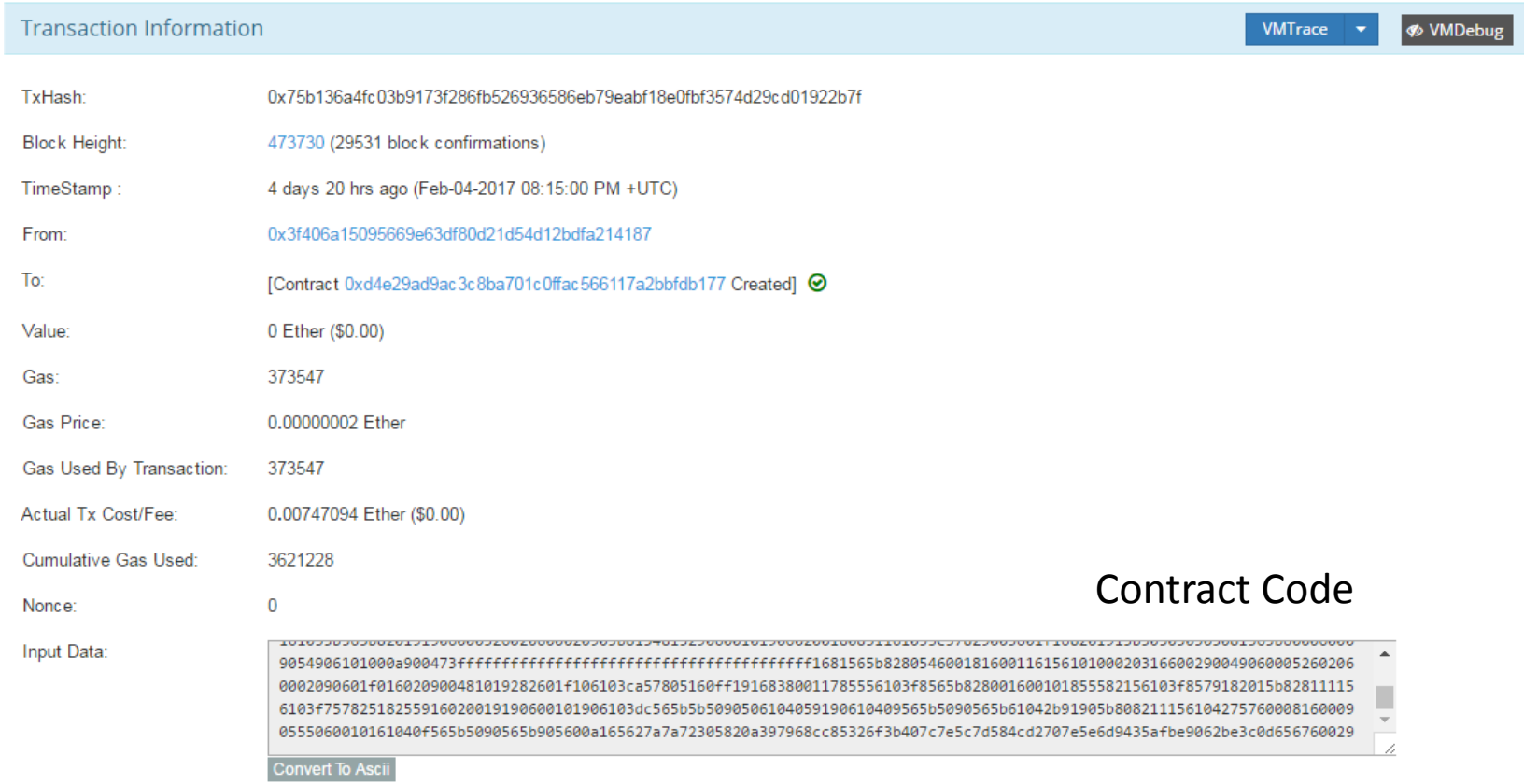
Pascal Urien

Transaction Information

TxHash:	0x79d910cc067334514e1f37ed2a3f2e1ad4ac13e46e97c208baa3f897bb74b336
Block Height:	2961230 (148972 block confirmations)
TimeStamp :	24 days 15 hrs ago (Jan-09-2017 12:42:49 AM +UTC)
From:	0xcafb10ee663f465f9d10588ac44ed20ed608c11e (Bitfinex_1)
To:	Contract 0xab7c74abc0c4d48d1bdad5dcb26153fc8780f83e
Value:	399,900 Ether ($4,254,936.00)
Gas:	122423
Gas Price:	0.00000002 Ether
Gas Used By Transaction:	22423
Actual Tx Cost/Fee:	0.00044846 Ether ($0.0048)
Cumulative Gas Used:	98037
Nonce:	437
Input Data:	0x

Contract Transaction

Creating a Contract



Contrat Source

```
pragma solidity ^0.4.2;
address public owner;
string public log;
function storer()
{
    owner = msg.sender ;
}
modifier onlyOwner
{
        if (msg.sender != owner)
            throw;
        _;
}
function store(string _log) onlyOwner()
{
    log = _log;
}
function kill() onlyOwner()
{
  selfdestruct(owner); }
}
```

Contrat Transaction

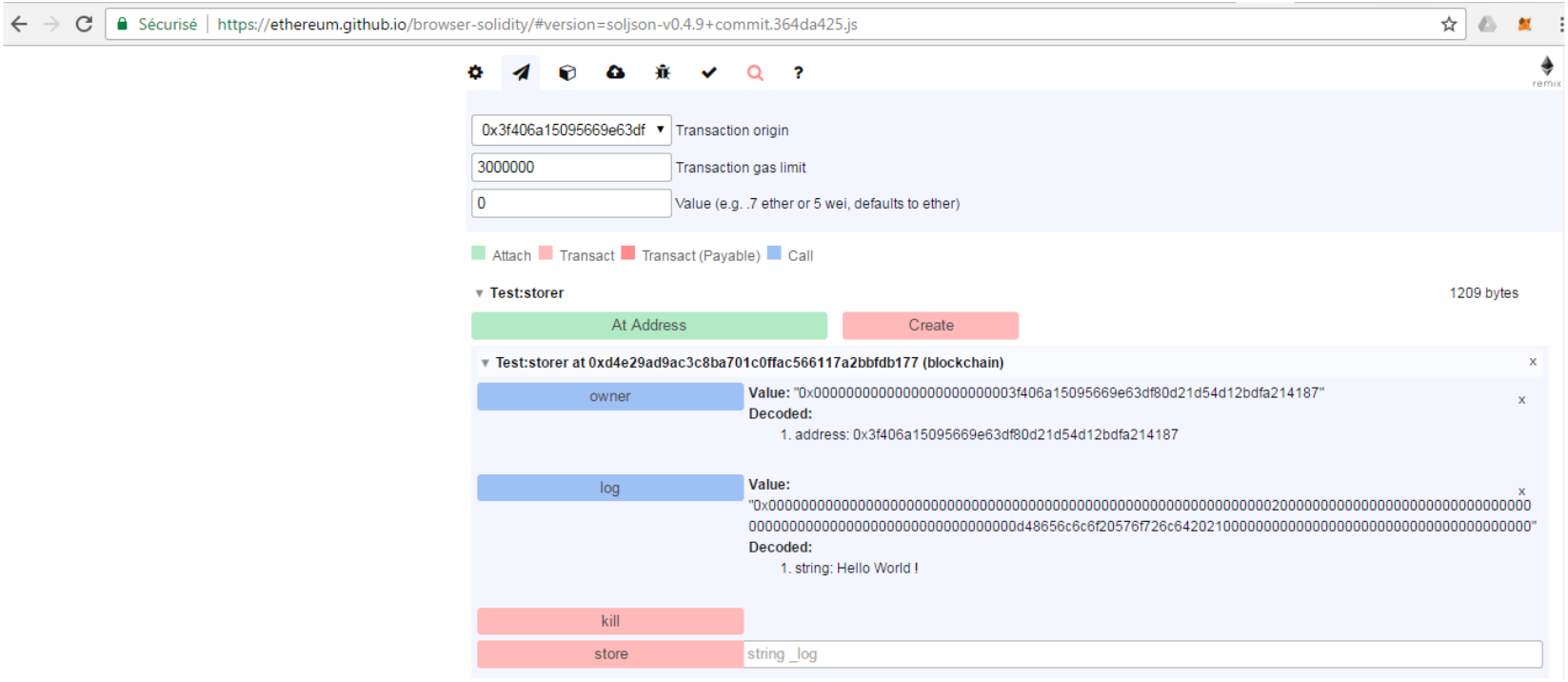
Transaction Information — VMTrace | VMDebug

TxHash:	0xda74659ce8125db72103a30e34165f3ec82a6b7691f2f03cc483bfd9d3aab54c
Block Height:	473742 (29557 block confirmations)
TimeStamp :	4 days 20 hrs ago (Feb-04-2017 08:17:39 PM +UTC)
From:	0x3f406a15095669e63df80d21d54d12bdfa214187
To:	Contract 0xd4e29ad9ac3c8ba701c0ffac566117a2bbfdb177
Value:	0 Ether ($0.00)
Gas:	43744
Gas Price:	0.00000002 Ether
Gas Used By Transaction:	43744
Actual Tx Cost/Fee:	0.00087488 Ether ($0.00)
Cumulative Gas Used:	3166176
Nonce:	1
Input Data:	0x131a068000000000000000000000000000000000000000000000000000000000000000200000000000000000000000000000000000000000000000000000000000000000d48656c6c6f20576f726c64210000000000000000000000000000000000000000

Hello World

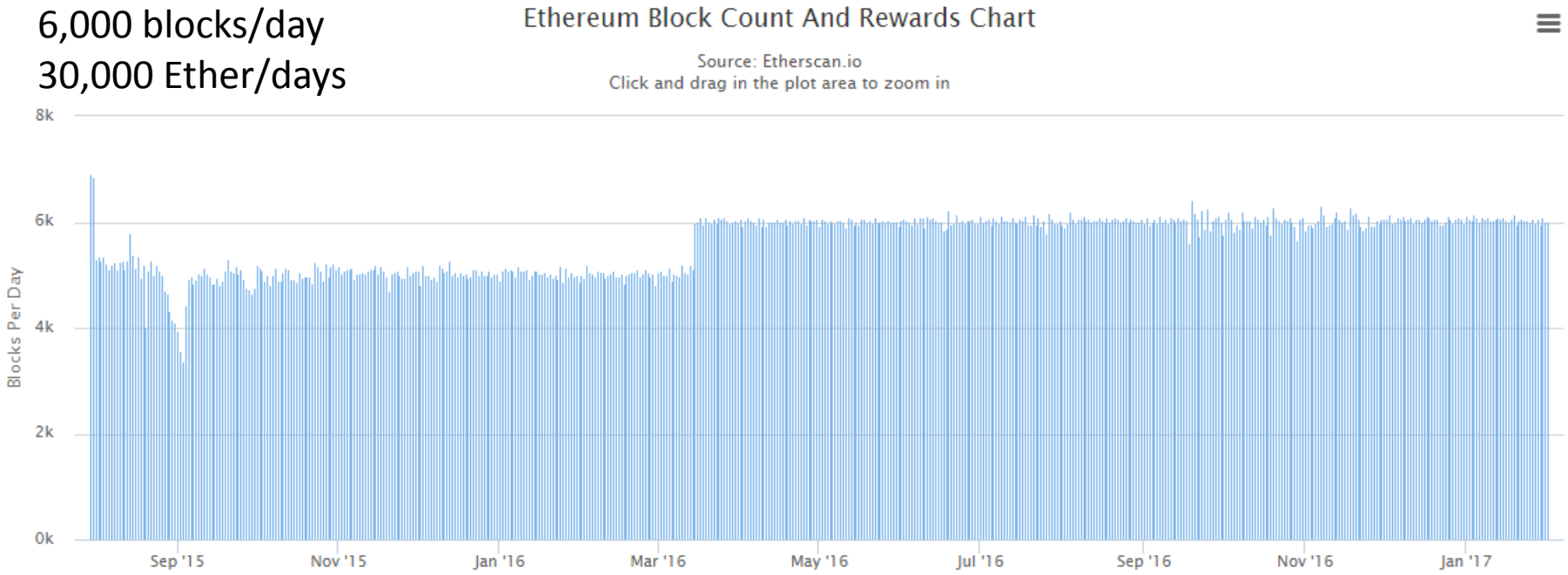
Convert To Ascii

Contract Transaction



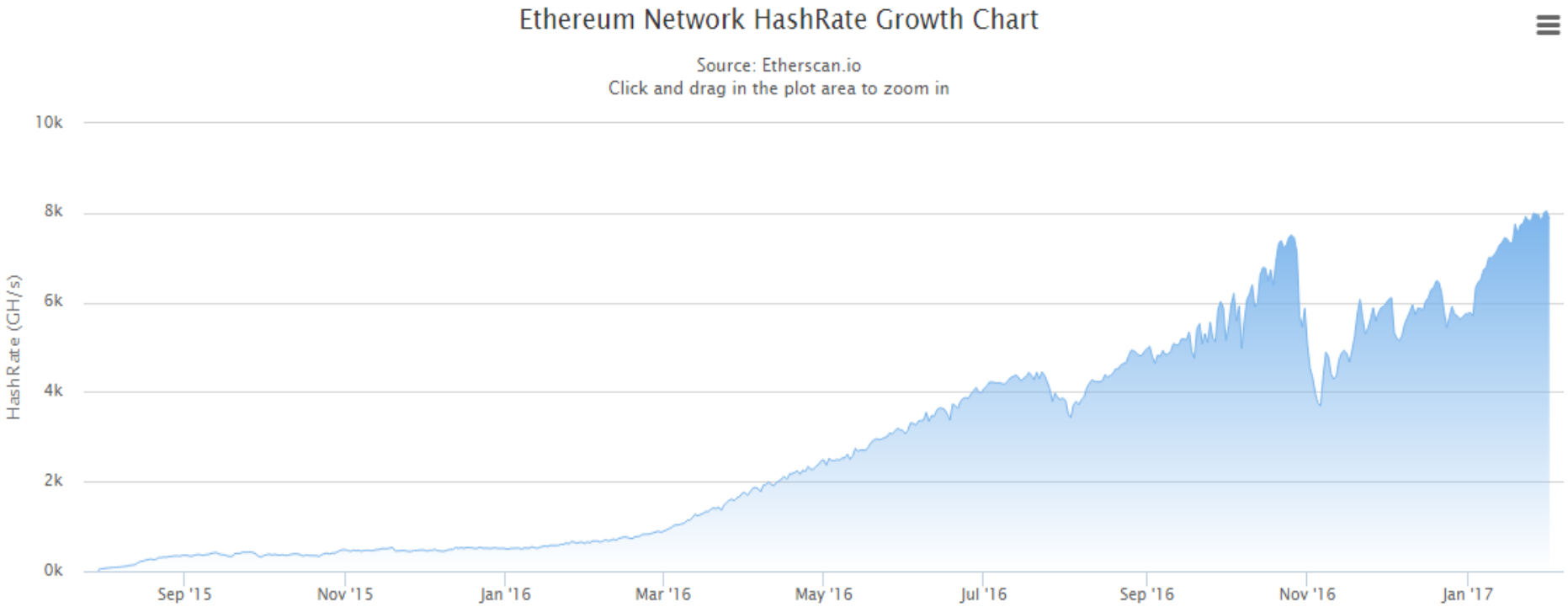
https://etherscan.io/charts

6,000 blocks/day
30,000 Ether/days

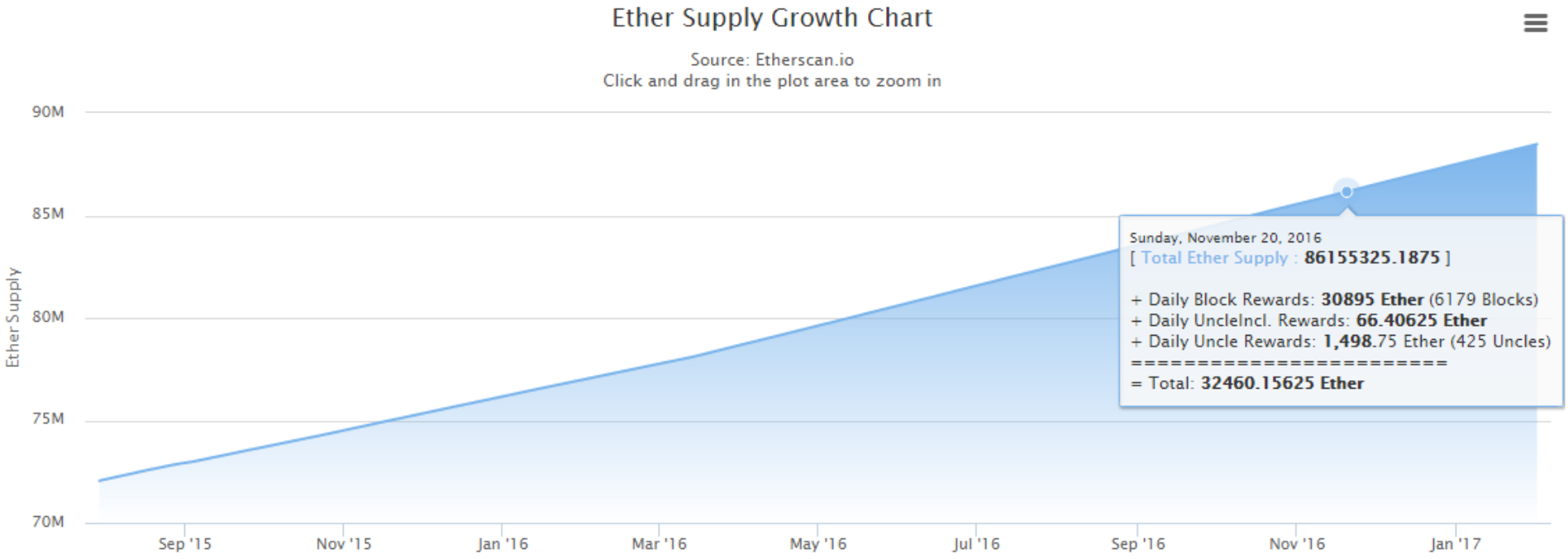


Market Capitalization

Hash Rate


Ethereum Network HashRate Growth Chart
Source: Etherscan.io
Click and drag in the plot area to zoom in
HashRate (GH/s)
10k
8k
6k
4k
2k
0k
Sep '15
Nov '15
Jan '16
Mar '16
May '16
Jul '16
Sep '16
Nov '16
Jan '17

Ether Supply



https://badmofo.github.io/ethereum-mining-calculator/

Calculator*

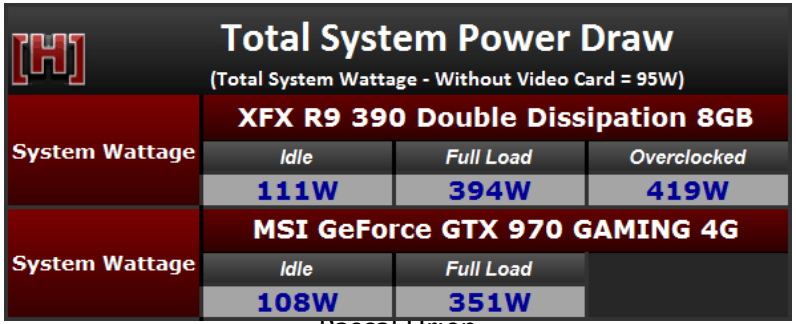
Pick GPU..	XFX R9 390 - Windows x64
..or enter hashrate manually	29.0
Network hashrate	8135.626995998334
Blocktime	14.109375
1 ETH price	10.5145

*Calculate how much Ether (ETH) **should** be mined with a specific hashrate.

Earnings (ETH)

Period	ETH	USD
Minute	0.000076	$0.00
Hour	0.004547	$0.05
Day	0.109140	$1.15
Week	0.763978	$8.03
Month	3.274192	$34.43
Year	39.836007	$418.86

450€, 400 W, 29 MH/s



February 3rd 2017

- Total Reward: 29950+58,3 + 1265 = 31273,3
  - 5990 blocks mined (14,42s / block)
  - Block Reward 5990 x 5 = 29950 ether
- 34,2 Ether (Gaz)
  - Gaz Used 1,519.30 10^{6}
  - 22508635957 10^{-18} Average Gaz Price

The Jean Mira Formula for Ethereum

Ether-Price(t) = EnergyCost(t) + ε1(t) + ε2(t) + ε3(t)

EnergyCost= C_1 x E x hashrate / Ether-NB

ε1 = C_2 x hashrate / Ether-NB

ε2 = Market Prime

ε3 = Ether-Price x Gaz-Used / Ether-NB

https://etherscan.io/charts

February 3rd 2017

Ether-Price: 10,78 $

Hashrate: 7,901.97 Gh/s

Ether-NB: 31273,3

Gas-Used: 34,2 Ether

EnergyCost= 12,55 $

ε2 = 11,50 $ (1 year)

ε3 = 0,12 $

Market Prime = -13,39 $

https://badmofo.github.io/ethereum-mining-calculator/

Year	C_1=W/Gh/s	C_2=$/Gh/s/day	C_1 x E= $/Gh/s
2017-2018 GPU: XFX-R9-390	400W/0,029 = 13,800	450$ / 0,029 / 365 = 45.5	13,800 x 0,0036 = 49,68 0,15 $ / KWh

Question