Is Bitcoin a suitable research topic?

Digital Conference Seminar

Clermont-Ferrand, France
November 13th, 2014

Jordi Herrera-Joancomartí
jordi.herrera@uab.cat
Universitat Autònoma de Barcelona

1. Introduction
2. Bitcoin description
3. The decentralization model
4. Bitcoin anonymity
5. Challenges and research opportunities
6. Conclusions

Weak motivation

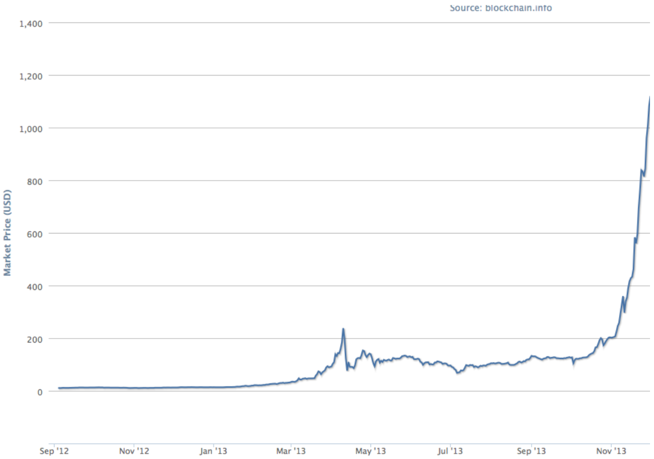


Figure: Bitcoin price evolution (blockchain.info chart)

Demotivation

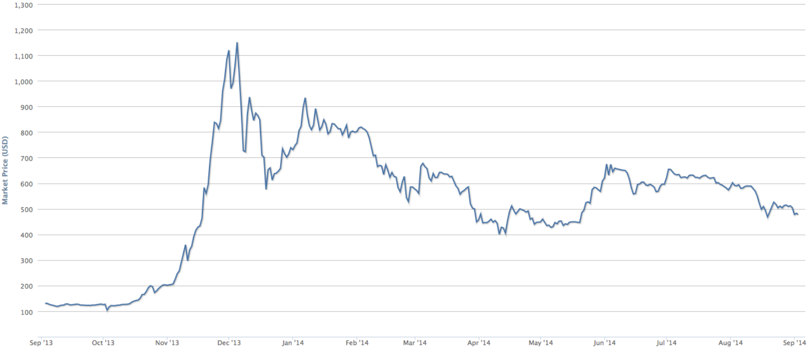


Figure: Bitcoin price evolution (blockchain.info chart)

Research motivation

- Bitcoin brings the first practical solution to the Byzantine Generals' Problem.
- The proposed solution allows the creation of a completely distributed digital currency.
- Furthermore: the solution is not limited to this specific application allowing new secure distributed applications.

1. Introduction
2. Bitcoin description
   - Bitcoin basic definitions
   - Bitcoin payments
   - The Blockchain
3. The decentralization model
4. Bitcoin anonymity
5. Challenges and research opportunities
6. Conclusions

Disclaimer

It is hard, if not impossible, to fit all bitcoin protocol description in one hour talk!

Bitcoin accounts, keys and addresses

- Bitcoins are not digital tokens but a balance in a bitcoin account.
- A bitcoin account is defined by an ECC key pair, $\{PK, SK\}$.
- The bitcoin account is publicly identified by its bitcoin address: an unidirectional function of its PK, $Addr(PK)$
- The public key allows to send bitcoins to the corresponding bitcoin account.
- The private key allows to spend the bitcoins of the account.

Bitcoin Payments

- Payments are performed through transactions between bitcoin accounts.
- A **transaction** T indicates a bitcoin movement from a source address to a destination address.
- The bitcoin address (a public value) allows to identify the destination in a transaction.
- The private key allows to spend the bitcoins of the account by means of a digital signature (ECDSA).

Payment example

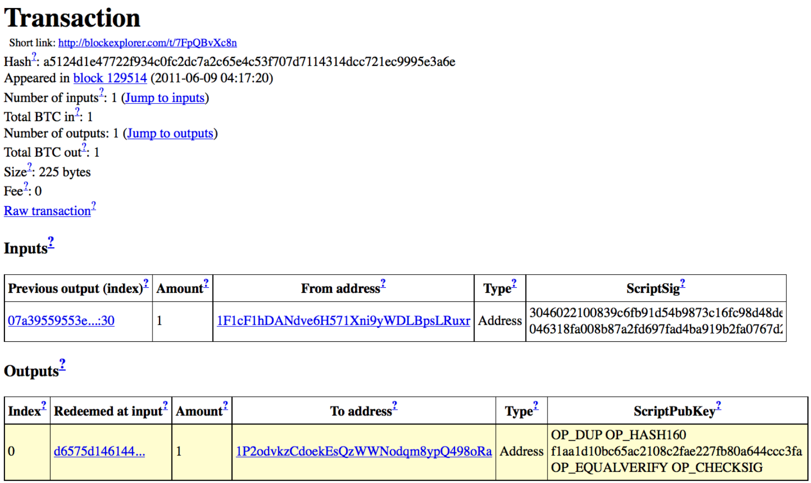
- Let $\{PK_A, SK_A\}$ be Alice public key pair (resp. $\{PK_B, SK_B\}$ Bob's keys).
- Given a previous transaction:

$$\begin{aligned} T_0 &= \{input_0, output_0\} \\ input_0 &= \{\cdots\} \\ output_0 &= \{Addr(PK_A), 25\} \end{aligned}$$

Alice may send the 25 BTC to Bob creating the following transaction T_1:

$$\begin{aligned} T_1 &= \{input_1, output_1\} \\ input_1 &= \{H(T_0), Sig_{SK_A}(T_0 + output_1), PK_A\} \\ output_1 &= \{Addr(PK_B), 25\} \end{aligned}$$

Simple transaction example



Transaction

Short link: http://blockexplorer.com/t/7FpQBvXc8n

Hash?: a5124d1e47722f934c0fc2dc7a2c65e4c53f707d7114314dcc721ec9995e3a6e
Appeared in block 129514 (2011-06-09 04:17:20)
Number of inputs?: 1 (Jump to inputs)
Total BTC in?: 1
Number of outputs: 1 (Jump to outputs)
Total BTC out?: 1
Size?: 225 bytes
Fee?: 0
Raw transaction?

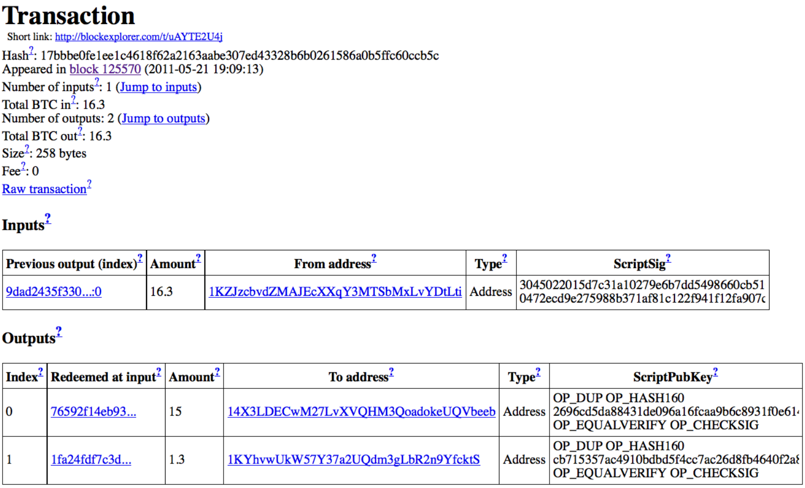
Inputs?

Previous output (index)?	Amount?	From address?	Type?	ScriptSig?
07a39559553e...:30	1	1F1cF1hDANdve6H571Xni9yWDLBpsLRuxr	Address	3046022100839c6fb91d54b9873c16fc98d48de 046318fa008b87a2fd697fad4ba919b2fa0767d

Outputs?

Index?	Redeemed at input?	Amount?	To address?	Type?	ScriptPubKey?
0	d6575d146144...	1	1P2odvkzCdoekEsQzWWNodqm8ypQ498oRa	Address	OP_DUP OP_HASH160 f1aa1d10bc65ac2108c2fae227fb80a644ccc3fa OP_EQUALVERIFY OP_CHECKSIG

Transaction example with multiple outputs



Transaction

Short link: http://blockexplorer.com/t/uAYTE2U4j

Hash?: 17bbbe0fe1ee1c4618f62a2163aabe307ed43328b6b0261586a0b5ffc60ccb5c
Appeared in block 125570 (2011-05-21 19:09:13)
Number of inputs?: 1 (Jump to inputs)
Total BTC in?: 16.3
Number of outputs: 2 (Jump to outputs)
Total BTC out?: 16.3
Size?: 258 bytes
Fee?: 0
Raw transaction?

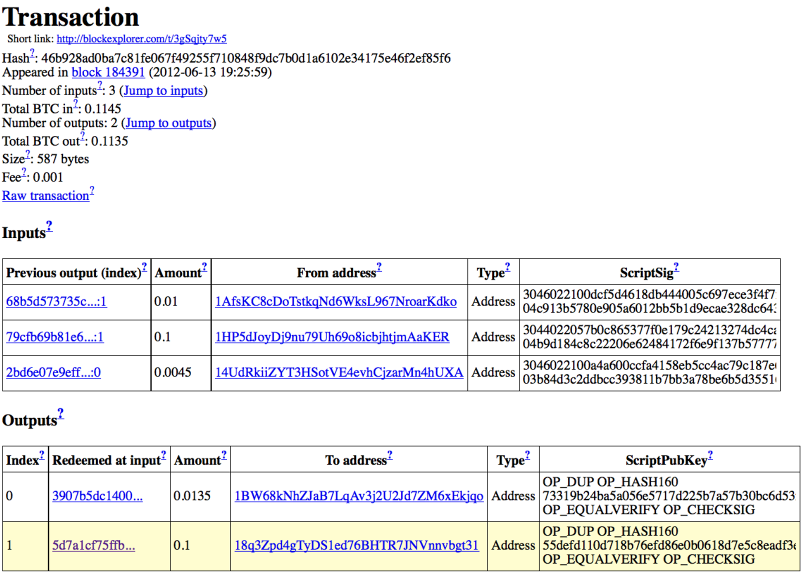
Inputs?

Previous output (index)?	Amount?	From address?	Type?	ScriptSig?
9dad2435f330...:0	16.3	1KZJzcbvdZMAJEcXXqY3MTSbMxLvYDtLti	Address	3045022015d7c31a10279e6b7dd5498660cb51 0472ecd9e275988b371af81c122f941f12fa907c

Outputs?

Index?	Redeemed at input?	Amount?	To address?	Type?	ScriptPubKey?
0	76592f14eb93...	15	14X3LDECwM27LvXVQHM3QoadokeUQVbeeb	Address	OP_DUP OP_HASH160 2696cd5da88431de096a16fcaa9b6c8931f0e61 OP_EQUALVERIFY OP_CHECKSIG
1	1fa24fdf7c3d...	1.3	1KYhvwUkW57Y37a2UQdm3gLbR2n9YfcktS	Address	OP_DUP OP_HASH160 cb715357ac4910bdbd5f4cc7ac26d8fb4640f2a OP_EQUALVERIFY OP_CHECKSIG

Transaction example with multiple inputs



Transaction

Short link: http://blockexplorer.com/t/3gSqjty7w5

Hash?: 46b928ad0ba7c81fe067f49255f710848f9dc7b0d1a6102e34175e46f2ef85f6
Appeared in block 184391 (2012-06-13 19:25:59)

Number of inputs?: 3 (Jump to inputs)

Total BTC in?: 0.1145
Number of outputs: 2 (Jump to outputs)

Total BTC out?: 0.1135

Size?: 587 bytes

Fee?: 0.001

Raw transaction?

Inputs?

Previous output (index)?	Amount?	From address?	Type?	ScriptSig?
68b5d573735c...:1	0.01	1AfsKC8cDoTstkqNd6WksL967NroarKdko	Address	3046022100dcf5d4618db444005c697ece3f4f7 04c913b5780e905a6012bb5b1d9ecae328dc64
79cfb69b81e6...:1	0.1	1HP5dJoyDj9nu79Uh69o8icbjhtjmAaKER	Address	3044022057b0c865377f0e179c24213274dc4c 04b9d184c8c22206e62484172f6e9f137b5777
2bd6e07e9eff...:0	0.0045	14UdRkiiZYT3HSotVE4evhCjzarMn4hUXA	Address	3046022100a4a600ccfa4158eb5cc4ac79c187e 03b84d3c2ddbcc393811b7bb3a78be6b5d3551

Outputs?

Index?	Redeemed at input?	Amount?	To address?	Type?	ScriptPubKey?
0	3907b5dc1400...	0.0135	1BW68kNhZJaB7LqAv3j2U2Jd7ZM6xEkjqo	Address	OP_DUP OP_HASH160 73319b24ba5a056e5717d225b7a57b30bc6d53 OP_EQUALVERIFY OP_CHECKSIG
1	5d7a1cf75ffb...	0.1	18q3Zpd4gTyDS1ed76BHTR7JNVnnvbgt31	Address	OP_DUP OP_HASH160 55defd110d718b76efd86e0b0618d7e5c8eadf3 OP_EQUALVERIFY OP_CHECKSIG

Is it possible a double spending?

Which mechanism prevents Alice to pay Charlie ($\{PK_C, SK_C\}$) creating another transaction T_2, and so spending again the $25BTC$ received in T_0 ?

$$\begin{aligned}
T_1 &= \{input_1, output_1\} \\
input_1 &= \{H(T_0), Sig_{SK_A}(T_0 + output_1), PK_A\} \\
output_1 &= \{Addr(PK_B), 25\}
\end{aligned}$$

$$\ldots$$

$$\begin{aligned}
T_2 &= \{input_2, output_2\} \\
input_2 &= \{H(T_0), Sig_{SK_A}(T_0 + output_2), PK_A\} \\
output_2 &= \{Addr(PK_C), 25\}
\end{aligned}$$

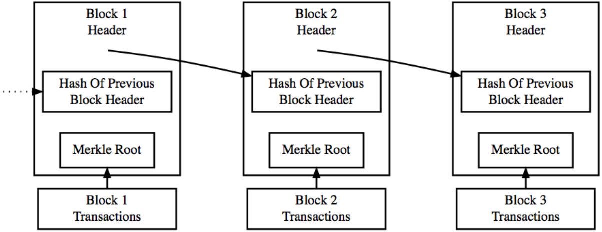
Bitcoin blocks (I)

- To prevent double spending, bitcoin publicly registers all transactions performed by the system.
- The **Blockchain** is such a unique register, generated and stored in a distributed form.
- The blockchain is an unique append-ledger that cannot be modified.

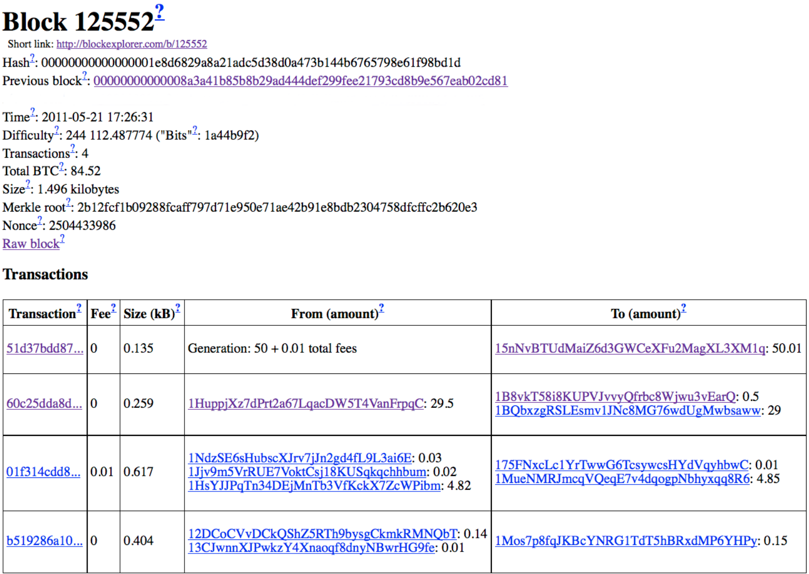
Bitcoin blocks (II)

Every block contains:

- Header
    - Pointer to the previous block
    - Nonce
    - ...
- Transactions



Bitcoin block example



Block 125552?

Short link: http://blockexplorer.com/b/125552
Hash?: 00000000000000001e8d6829a8a21adc5d38d0a473b144b6765798e61f98bd1d
Previous block?: 00000000000008a3a41b85b8b29ad444def299fee21793cd8b9e567eab02cd81

Time?: 2011-05-21 17:26:31
Difficulty?: 244 112.487774 ("Bits"?: 1a44b9f2)
Transactions?: 4
Total BTC?: 84.52
Size?: 1.496 kilobytes
Merkle root?: 2b12fcf1b09288fcaff797d71e950e71ae42b91e8bdb2304758dfcffc2b620e3
Nonce?: 2504433986
Raw block?

Transactions

Transaction?	Fee?	Size (kB)?	From (amount)?	To (amount)?
51d37bdd87...	0	0.135	Generation: 50 + 0.01 total fees	15nNvBTUdMaiZ6d3GWCeXFu2MagXL3XM1q: 50.01
60c25dda8d...	0	0.259	1HuppjXz7dPrt2a67LqacDW5T4VanFrpqC: 29.5	1B8vkT58i8KUPVJvvyQfrbc8Wjwu3vEarQ: 0.5 1BQbxzgRSLEsmv1JNc8MG76wdUgMwbsaww: 29
01f314cdd8...	0.01	0.617	1NdzSE6sHubscXJrv7jJn2gd4fL9L3ai6E: 0.03 1Jjv9m5VrRUE7VoktCsj18KUSqkqchhbum: 0.02 1HsYJJPqTn34DEjMnTb3VfKckX7ZcWPibm: 4.82	175FNxcLc1YrTwwG6TcsywcsHYdVqyhbwC: 0.01 1MueNMRJmcqVQeqE7v4dqogpNbhyxqq8R6: 4.85
b519286a10...	0	0.404	12DCoCVvDCkQShZ5RTh9bysgCkmkRMNQbT: 0.14 13CJwnnXJPwkzY4Xnaoqf8dnyNBwrHG9fe: 0.01	1Mos7p8fqJKBcYNRG1TdT5hBRxdMP6YHPy: 0.15

Mining: Including a block into the blockchain

Every bitcoin user may create a new block by:

- Collecting from the P2P bitcoin network all transactions not included in previous blocks.
- Validating the correctness of such transactions.
- Including a generation transaction (we will refer later).

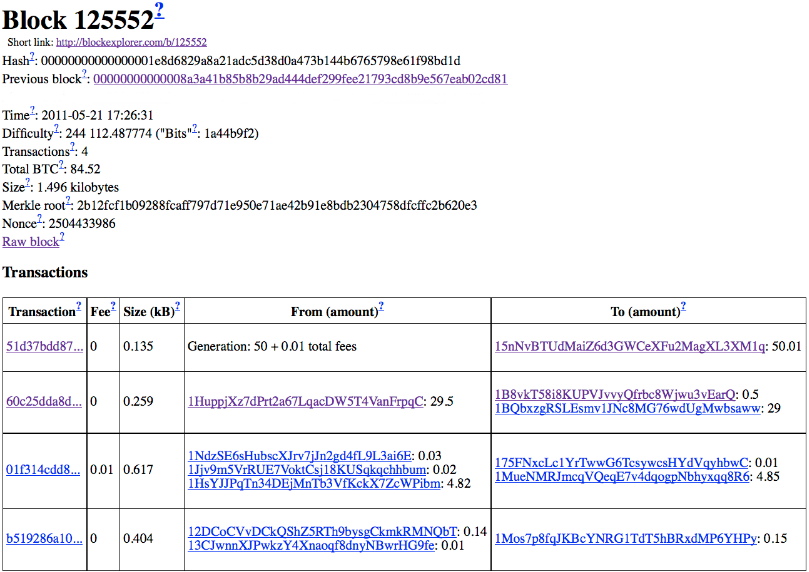
Once the block is created it has to be included in the blockchain, performing a proof-of-work, by:

- Computing the hash (SHA256) of the block such that its value is lower than a predefined target (varying the nonce field).
- Sending the obtained block to the bitcoin P2P network.

Where bitcoins come from? Mining rewards

- Obtaining the correct nonce for including a block in the blockchain is an expensive task.
- Miners should be rewarded for such task that allows to maintain up-to-date the spent transactions of the bitcoin system (and prevent double spending).
- The reward comes in bitcoin form: every new block includes a generation transaction that provides fresh new bitcoins to the miner.
- Additionally, transactions may include fees that the miner also obtain.

Generation transaction example



Block 125552?

Short link: http://blockexplorer.com/b/125552

Hash?: 00000000000000001e8d6829a8a21adc5d38d0a473b144b6765798e61f98bd1d

Previous block?: 00000000000008a3a41b85b8b29ad444def299fee21793cd8b9e567eab02cd81

Time?: 2011-05-21 17:26:31

Difficulty?: 244 112.487774 ("Bits"?: 1a44b9f2)

Transactions?: 4

Total BTC?: 84.52

Size?: 1.496 kilobytes

Merkle root?: 2b12fcf1b09288fcaff797d71e950e71ae42b91e8bdb2304758dfcffc2b620e3

Nonce?: 2504433986

Raw block?

Transactions

Transaction?	Fee?	Size (kB)?	From (amount)?	To (amount)?
51d37bdd87...	0	0.135	Generation: 50 + 0.01 total fees	15nNvBTUdMaiZ6d3GWCeXFu2MagXL3XM1q: 50.01
60c25dda8d...	0	0.259	1HuppjXz7dPrt2a67LqacDW5T4VanFrpqC: 29.5	1B8vkT58i8KUPVJvvyQfrbc8Wjwu3vEarQ: 0.5 1BQbxzgRSLEsmv1JNc8MG76wdUgMwbsaww: 29
01f314cdd8...	0.01	0.617	1NdzSE6sHubscXJrv7jJn2gd4fL9L3ai6E: 0.03 1Jjv9m5VrRUE7VoktCsj18KUSqkqchhbum: 0.02 1HsYJJPqTn34DEjMnTb3VfKckX7ZcWPibm: 4.82	175FNxcLc1YrTwwG6TcsywcsHYdVqyhbwC: 0.01 1MueNMRJmcqVQeqE7v4dqogpNbhyxqq8R6: 4.85
b519286a10...	0	0.404	12DCoCVvDCkQShZ5RTh9bysgCkmkRMNQbT: 0.14 13CJwnnXJPwkzY4Xnaoqf8dnyNBwrHG9fe: 0.01	1Mos7p8fqJKBcYNRG1TdT5hBRxdMP6YHPy: 0.15

Some other details

- Block throughput: Although the mining process is probabilistic, the target value is adjusted every 2016 blocks (2 weeks approx) in order to produce a block every 10 minutes.
- Transaction confirmation:
  - A transaction is confirmed when it appears in a block.
  - A transaction has two confirmation when it has appeared in a block and the next block has been also mined.
  - Transactions (payments) are not considered valid until 6 validations (1 hour)
- The total number of bitcoins that will be generated is fixed: 21 million.
- The rewarding mechanisms is supposed to move from bitcoin generation towards payment fees.

1. Introduction

2. Bitcoin description

3. The decentralization model
   - The bitcoin P2P network
   - Distributed tasks

4. Bitcoin anonymity

5. Challenges and research opportunities

6. Conclusions

Network nodes

- No central authority is (supposed to) control the Bitcoin system: a distributed P2P approach has been adopted.
- Every user with a full wallet becomes a network node.
- Network nodes perform different tasks to maintain the bitcoin system.

Network nodes distribution

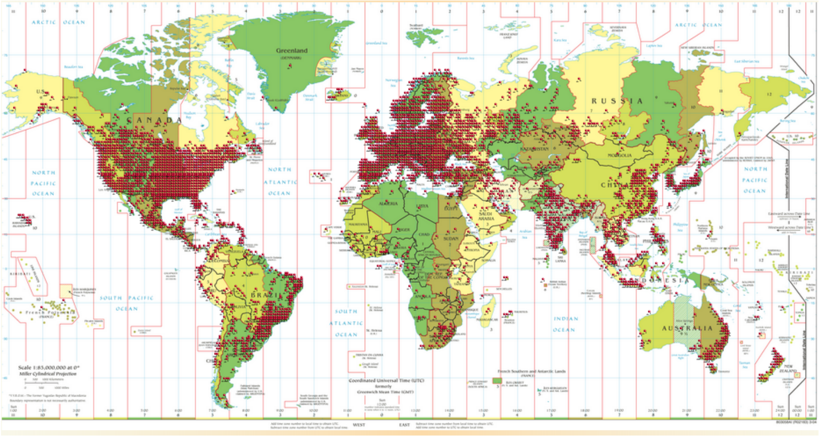


Figure: 872648 nodes retrieved from November 30th, 2013 to January 5th, 2014

Distributed tasks

- Such distributed approach has different sides:
  - data transmission
  - data storage
  - data confirmation (mining)
- Historically, first bitcoin wallets were full nodes and performed all such tasks.
- Now, with the increase of computational costs:
  - Reduction of the number of tasks that nodes perform.
  - Reduction of the number of nodes in the bitcoin network.

Data transmission

- Bitcoin network nodes are P2P connected to other nodes listening for new data to be transmitted.
- The data flowing through the bitcoin network is basically transactions and blocks.
- When a node receives a transaction or a block that he is not aware of, he broadcasts such data to the nodes he is connected.
- Before such broadcast takes place, the correctness of the transaction or the block is validated by the node.

Data storage

- Data storage presents high redundancy: all bitcoin network nodes store a complete copy of the blockchain.
- The blockchain allows the node to perform the proper validations previous to broadcast new received transactions or blocks.
- The actual size of the blockchain, 21 GB - Sep’14, is a problem for lightweight (or not so lightweight) devices.

Data confirmation (mining)

- Data confirmation (mining) is the hardest task in the bitcoin system.
- Mining can be performed by any bitcoin user but, for practical reasons, it is performed by mining pools.
- Each mining pool distributes the work between its users and so the rewards for the mining.

Mining pools hashrate distribution

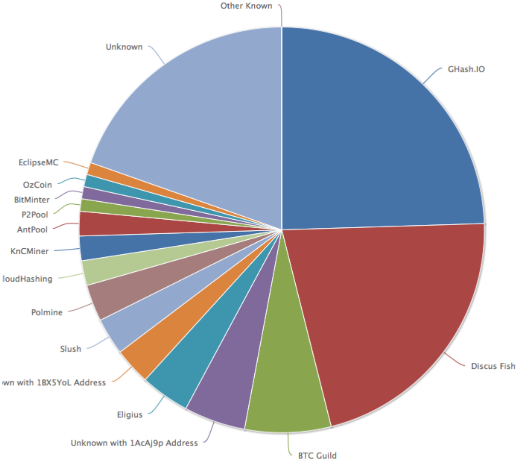


Figure: Mining pools hashrate distribution Sep'14 (source: blockchain.info)

1 Introduction

2 Bitcoin description

3 The decentralization model

4 Bitcoin anonymity
- Basic transaction analysis
- Graph mining analysis
- External identification

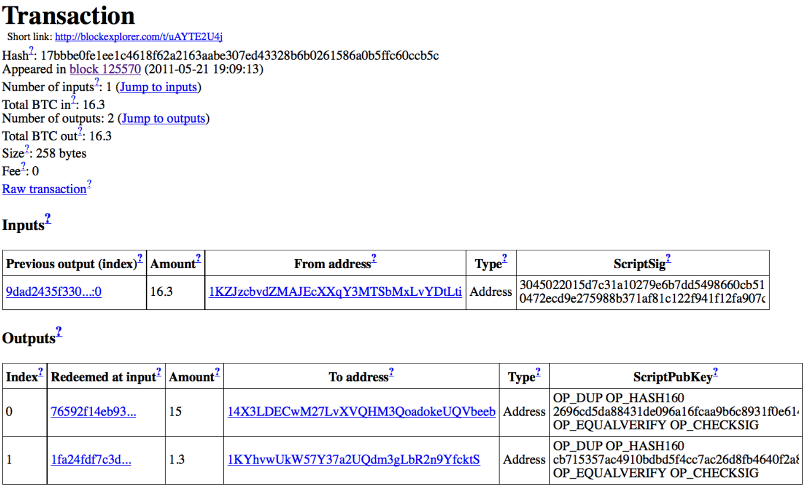
5 Challenges and research opportunities

6 Conclusions

Anonymous keys

- Anonymity is based on the fact that users can create any number of anonymous bitcoin addresses.
- It is recommended that a new address should be used in every transaction.
- Two main anonymity threads:
  - the availability of all bitcoin transactions in the blockchain
  - the underlying non-anonymous network used
  - (without forgetting the exhibitionist users!)

Please, keep the change!



Transaction

Short link: http://blockexplorer.com/t/uAYTE2U4j

Hash?: 17bbbe0fe1ee1c4618f62a2163aabe307ed43328b6b0261586a0b5ffc60ccb5c
Appeared in block 125570 (2011-05-21 19:09:13)
Number of inputs?: 1 (Jump to inputs)
Total BTC in?: 16.3
Number of outputs: 2 (Jump to outputs)
Total BTC out?: 16.3
Size?: 258 bytes
Fee?: 0
Raw transaction?

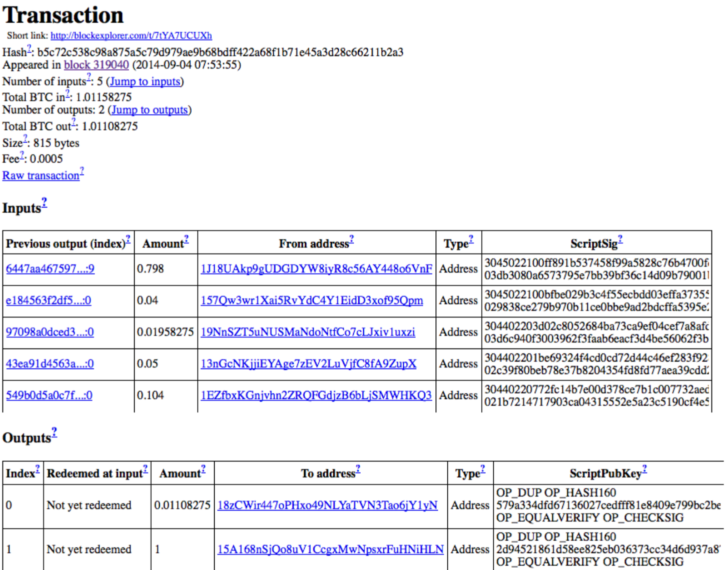
Inputs?

Previous output (index)?	Amount?	From address?	Type?	ScriptSig?
9dad2435f330...:0	16.3	1KZJzcbvdZMAJEcXXqY3MTSbMxLvYDtLti	Address	3045022015d7c31a10279e6b7dd5498660cb51 0472ecd9e275988b371af81c122f941f12fa907

Outputs?

Index?	Redeemed at input?	Amount?	To address?	Type?	ScriptPubKey?
0	76592f14eb93...	15	14X3LDECwM27LvXVQHM3QoadokeUQVbeeb	Address	OP_DUP OP_HASH160 2696cd5da88431de096a16fcaa9b6c8931f0e61 OP_EQUALVERIFY OP_CHECKSIG
1	1fa24fdf7c3d...	1.3	1KYhvwUkW57Y37a2UQdm3gLbR2n9YfcktS	Address	OP_DUP OP_HASH160 cb715357ac4910bdbd5f4cc7ac26d8fb4640f2a OP_EQUALVERIFY OP_CHECKSIG

Yes, all that addresses (probably) belong to the same user!



Transaction

Short link: http://blockexplorer.com/t/7tYA7UCUXh

Hash?: b5c72c538c98a875a5c79d979ae9b68bdff422a68f1b71e45a3d28c66211b2a3
Appeared in block 319040 (2014-09-04 07:53:55)
Number of inputs?: 5 (Jump to inputs)
Total BTC in?: 1.01158275
Number of outputs: 2 (Jump to outputs)
Total BTC out?: 1.01108275
Size?: 815 bytes
Fee?: 0.0005
Raw transaction?

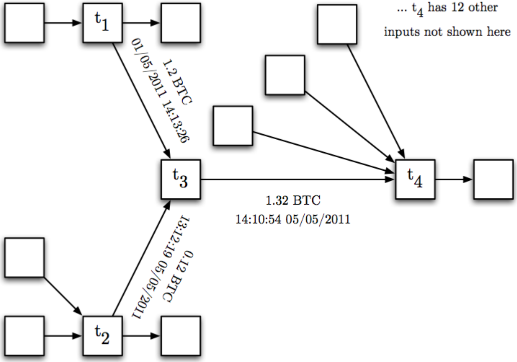
Inputs?

Previous output (index)?	Amount?	From address?	Type?	ScriptSig?
6447aa467597...:9	0.798	1J18UAkp9gUDGDYW8iyR8c56AY448o6VnF	Address	3045022100ff891b537458f99a5828c76b4700f 03db3080a6573795e7bb39bf36c14d09b79001
e184563f2df5...:0	0.04	157Qw3wr1Xai5RvYdC4Y1EidD3xof95Qpm	Address	3045022100bfbe029b3c4f55ecbdd03effa3735 029838ce279b970b11ce0bbe9ad2bdcffa5395e
97098a0dced3...:0	0.01958275	19NnSZT5uNUSMaNdoNtfCo7cLJxiv1uxzi	Address	304402203d02c8052684ba73ca9ef04cef7a8af 03d6c940f3003962f3faab6eacf3d4be56062f3b
43ea91d4563a...:0	0.05	13nGcNKjjiEYAge7zEV2LuVjfC8fA9ZupX	Address	304402201be69324f4cd0cd72d44c46ef283f92 02c39f80beb78e37b8204354fd8fd77aea39cdd
549b0d5a0c7f...:0	0.104	1EZfbxKGnjvhn2ZRQFGdjzB6bLjSMWHKQ3	Address	30440220772fc14b7e00d378ce7b1c007732aed 021b7214717903ca04315552e5a23c5190cf4e

Outputs?

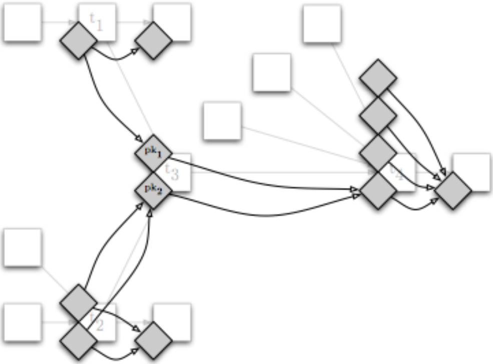
Index?	Redeemed at input?	Amount?	To address?	Type?	ScriptPubKey?
0	Not yet redeemed	0.01108275	18zCWir447oPHxo49NLYaTVN3Tao6jY1yN	Address	OP_DUP OP_HASH160 579a334dfd67136027cedfff81e8409e799bc2be OP_EQUALVERIFY OP_CHECKSIG
1	Not yet redeemed	1	15A168nSjQo8uV1CcgxMwNpsxrFuHNiHLN	Address	OP_DUP OP_HASH160 2d94521861d58ee825eb036373cc34d6d937a8 OP_EQUALVERIFY OP_CHECKSIG

Transaction network: Reid & Harrigan[1] (I)

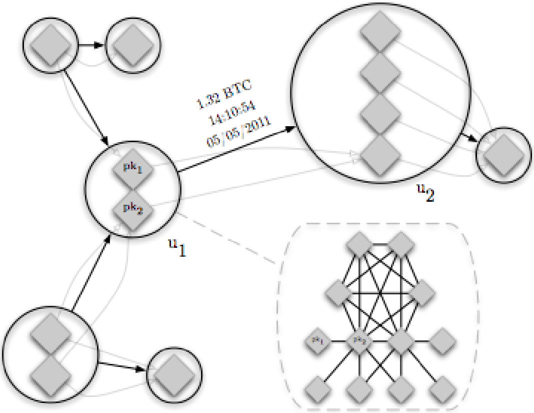


[1] Reid, F., Harrigan, M.: An analysis of anonymity in the bitcoin system. Security and Privacy in Social Networks, pp. 197-223. Springer (2013).

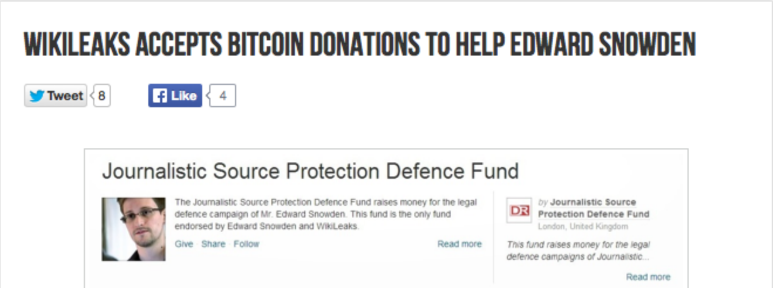
Transaction network: Reid & Harrigan (II)



Transaction network: Reid & Harrigan (III)



Publicly available identification



WIKILEAKS ACCEPTS BITCOIN DONATIONS TO HELP EDWARD SNOWDEN

Journalistic Source Protection Defence Fund

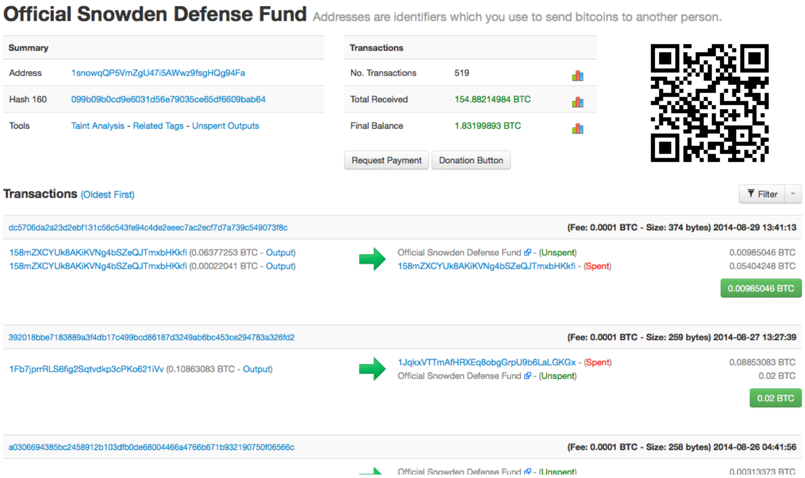
The Journalistic Source Protection Defence Fund raises money for the legal defence campaign of Mr. Edward Snowden. This fund is the only fund endorsed by Edward Snowden and WikiLeaks.

by Journalistic Source Protection Defence Fund
London, United Kingdom

This fund raises money for the legal defence campaigns of Journalistic...

To make your Bitcoin donation, all you have to do is send the desired amount to the address **1snowqQP5VmZgU47i5AWwz9fsgHQg94Fa**.

External identification



Official Snowden Defense Fund

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

Summary	
Address	1snowqQP5VmZgU47i5AWwz9fsgHQg94Fa
Hash 160	099b09b0cd9e6031d56e79035ce65df6609bab64
Tools	Taint Analysis - Related Tags - Unspent Outputs

Transactions	
No. Transactions	519
Total Received	154.88214984 BTC
Final Balance	1.83199893 BTC

Transactions (Oldest First)

dc5706da2a23d2ebf131c56c543fe94c4de2eeec7ac2ecf7d7a739c549073f8c **(Fee: 0.0001 BTC - Size: 374 bytes) 2014-08-29 13:41:13**

158mZXCYUk8AKiKVNg4bSZeQJTmxbHKkfi (0.06377253 BTC - Output)
158mZXCYUk8AKiKVNg4bSZeQJTmxbHKkfi (0.00022041 BTC - Output)

Official Snowden Defense Fund - (Unspent) 0.00985046 BTC
158mZXCYUk8AKiKVNg4bSZeQJTmxbHKkfi - (Spent) 0.05404248 BTC

0.00985046 BTC

392018bbe7183889a3f4db17c499bcd86187d3249ab6bc453ce294783a326fd2 **(Fee: 0.0001 BTC - Size: 259 bytes) 2014-08-27 13:27:39**

1Fb7jprrRLS6fig2Sqtvdkp3cPKo621iVv (0.10863083 BTC - Output)

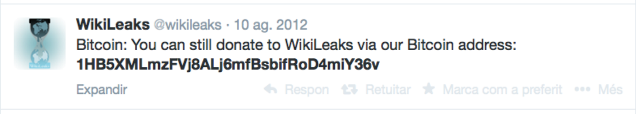
1JqkxVTTmAfHRXEq8obgGrpU9b6LaLGKGx - (Spent) 0.08853083 BTC
Official Snowden Defense Fund - (Unspent) 0.02 BTC

0.02 BTC

a0306694385bc2458912b103dfb0de68004466a4766b671b932190750f06566c **(Fee: 0.0001 BTC - Size: 258 bytes) 2014-08-26 04:41:56**

Official Snowden Defense Fund - (Unspent) 0.00313373 BTC

Graph mining and public information



WikiLeaks @wikileaks · 10 ag. 2012
Bitcoin: You can still donate to WikiLeaks via our Bitcoin address:
1HB5XMLmzFVj8ALj6mfBsbifRoD4miY36v

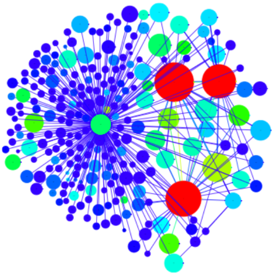


Figure: An egocentric visualization of the vertex representing WikiLeaks' public-key from (Reid & Hardigan)

1 Introduction

2 Bitcoin description

3 The decentralization model

4 Bitcoin anonymity

5 Challenges and research opportunities

- Bitcoin as a core research
- Bitcoins as tool
- Funding opportunities

6 Conclusions

Challenges and research opportunities

Important fact I

A payment system that solves the double-spending problem by keeping a list of all performed transactions surely it has room for improvements.

Important fact II

The bitcoin solution approach of the Byzantine Generals' Problem may bring interesting ideas for other distributed applications (including improved new cryptocurrencies).

Performance

- Scalability: blockchain size and transaction validation.
- Sustainability: Is there a better form of Proof-of-Work (regarding its carbon footprint)?
  - more useful: Primecoins, ...(?)...
  - more efficient: Proof-of-Stake, Proof-of-Burn, ...
- Efficiency: Is it possible to reduce the 10 minutes block throughput without affecting the system security?

Security

- Bitcoin Protocol analysis.
- Wallet assessment.
- 51% (or less[2]) attacks.
- Network partition/isolation.
- Key randomness: deterministic wallets and hierarchical deterministic wallets.

[2] Ittay Eyal and Emin Gun Sirer. *Majority is not Enough: Bitcoin Mining is Vulnerable*. Financial Cryptography and Data Security. 2014

Anonymity

- Mixing networks: be careful => Money laundry!
- Completely anonymous currencies: zerocoin[3]
- Anonymity analysis using the bitcoin P2P network information, together with blockchain info.

[3] I. Miers, C. Garman, M. Green, and A. D. Rubin, "Zerocoin: Anonymous distributed e-cash from bitcoin", Proceedings of the 2013 IEEE Symposium on Security and Privacy Pages 397-411

Blockchain applications

Bitcoins, or the blockchain approach itself, as a distributed, public, non-modifiable, append-only ledger may be used for:

- Timestamp services.
- Distributed DNS: NameCoins.
- Metacoins and financial derivatives: Mastercoins, coroledcoins
- DAO: Distributed Autonomous Organizations: NXT, Ethereum.
- Secure multiparty computation[4].
- P2P Gambling.

[4] Marcin Andrychowicz, Stefan Dziembowski, Daniel Malinowski and Lukasz Mazurek. *"Fair Two-Party Computations via Bitcoin Deposits"*. Financial Cryptography and Data Security. 2014

Bitcoin Foundation Grant program

The Bitcoin Foundation objectives are to standardize, protect and promote the use of bitcoins.

Bitcoin Foundation Grant program:

- It provides funding for bitcoin related projects.
- Calls for projects are every quarter (1st January, 1st April, 1st September).
- Grants are payed, of course, in bitcoins.
- Research projects are also welcome.
- More info: `https://bitcoinfoundation.org/about/grant-program/`

1. Introduction
2. Bitcoin description
3. The decentralization model
4. Bitcoin anonymity
5. Challenges and research opportunities
6. Conclusions

Conclusions

- Bitcoin proposes a robust cryptographic cryptocurrency completely distributed.
- The idea of a public append-only ledger may be applied to other distributed scenarios where security is needed.
- Research opportunities exist, regarding anonymity, performance and new applications.
- A lot of money (bitcoins) is moving around bitcoin ecosystem and it could be a new source or funding research.

Is Bitcoin a suitable research topic?

Digital Conference Seminar

Clermont-Ferrand, France
November 13th, 2014

Jordi Herrera-Joancomartí
jordi.herrera@uab.cat
Universitat Autònoma de Barcelona