Cryptography principles in cryptocurrency

Pavel Kravchenko

About

PhD in information security

10 years in software engineering and security

Used to work at Stellar

Chief cryptographer at Tembusu Systems

Agenda

1. General terms in information security
2.“Myths”
3. Crypto algorithms in Bitcoin

General terms

Information security – state of information when certain properties of the information is ensured

Confidentiality – information can be accessed only by authorized users

Integrity - information can't be modified without being noticed

Availability – authorized users can access information with required level of quality

There should be explicit statement of what the system can ensure in terms of security.

Otherwise after any accident users will think that it is broken.

What Bitcoin can and cannot?

Protect integrity of transactions

Prevent double-spending

Control money supply

Ensure authenticity of sender and recipient

Prevent counterfeiting

Prevent network attacks

Prevent keys from theft

Prevent impersonating of the user (MITM)

Weak key generation

Ensure anonymity

Crypto algorithms

1. Key generation
2. Key distribution
3. Encryption
4. Hash function
5. Digital signature
6. Zero knowledge proof
7. Key agreement
8. Secret sharing
9. Ring signature
10. Group signature

Key generation

Key generation is the process of generating random keys

RNG - natural entropy usage - atmospheric noise, thermal noise etc

PRNG – predefined algorithm and seed, keys could be reproduced on the same PC

CSPRNG – seed value is some random value, hard to guess

Principles:

1. Quality of randomness is crucial
2. Seed data should be truly random

Idea: Hardware key generator and storage

Key distribution

Is a process of secure exchanging of keys between users

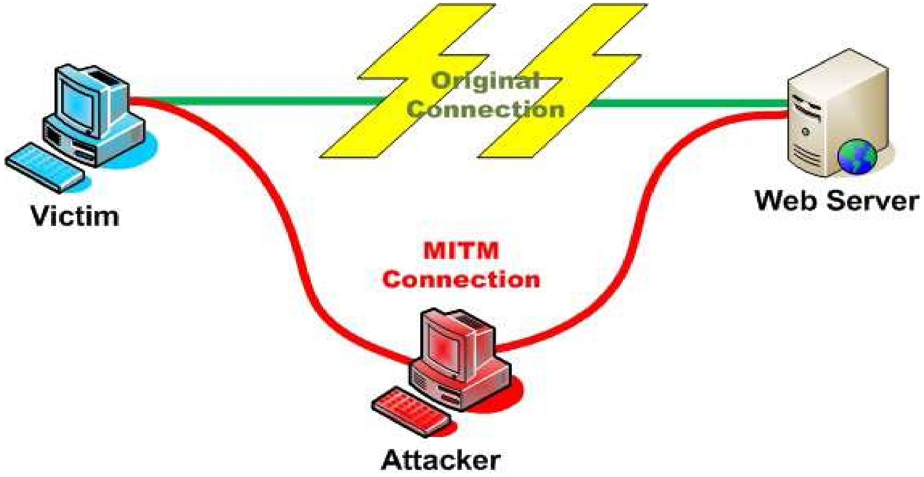
Principles:

Secure only if uses

1) earlier distributed key

2) face-to-face meeting

3) trusted party



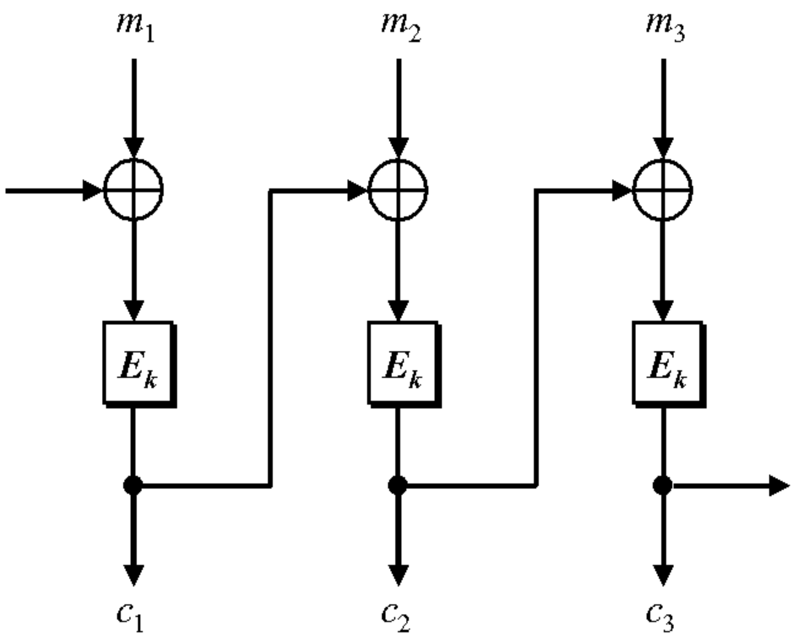
Idea: PKI for cryptocurrencies

Encryption

Encryption is a process of transforming a piece of information into an incomprehensible form with a key.

Principles:

1. Protects only confidentiality
2. Encryption of the same message gives different result
3. For each session new key is used

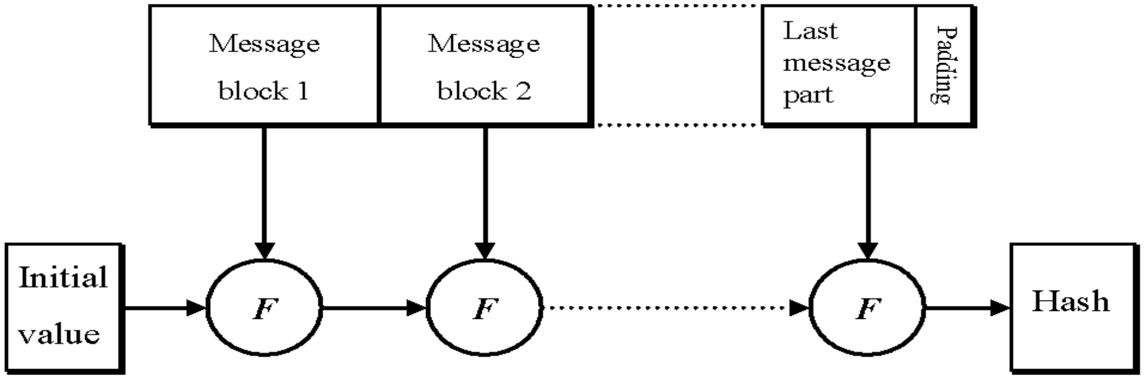


Hash

Technique that allows creating unique digital fingerprint of a message.

Principles:

1. Output is similar to random number
2. Impossible to find two messages that give the same result
3. Impossible to recover message from its hash
4. Changing one bit in the message changes hash dramatically



Digital signature

A **digital signature** is an analogue of handwritten signature and added to the message to demonstrate its authenticity.

Principles

1. Even small change in a message or signature leads to rejecting signature
2. It is impossible to create 2 different messages which produce equal signature
3. Ensures integrity and non-repudiation
4. Group signatures, proxy signatures, undeniable signatures etc

Zero knowledge proof

Zero knowledge proof protocol helps to convince other user that you know some particular secret without revealing it.

Principles:

1. Zero knowledge proof requires interaction between users

2. User that obtained a proof cannot convince third party

Zero-knowledge proofs

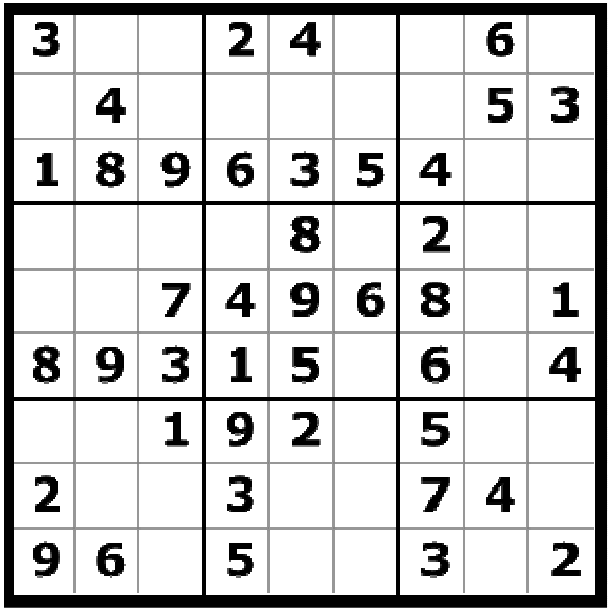
You can prove that:

Key has some length (2^{64} < key < 2^{128})

That you have 3 out of 5 private keys

That you know solution for sudoku :)

You paid certain amount of taxes :(



3			2	4			6	
	4						5	3
1	8	9	6	3	5	4		
				8		2		
		7	4	9	6	8		1
8	9	3	1	5		6		4
		1	9	2		5		
2			3			7	4	
9	6		5			3		2

Key agreement

Two users communicate over open channel about shared secured key

Principles

1. Eavesdropper cannot extract any information about the shared key
2. Integrity of communication should be ensured

Idea: Stealth addresses

Secret sharing

Key is split between group of people and all of them are needed to recover it.

Principles

1. It is possible to meet requirements of any access matrix
2. Amount of shares less than threshold doesn't give any information about the secret
3. It is possible to create groups and give them different power

Ideas: Smart contracts, decision making, key protection

Group signature. Features

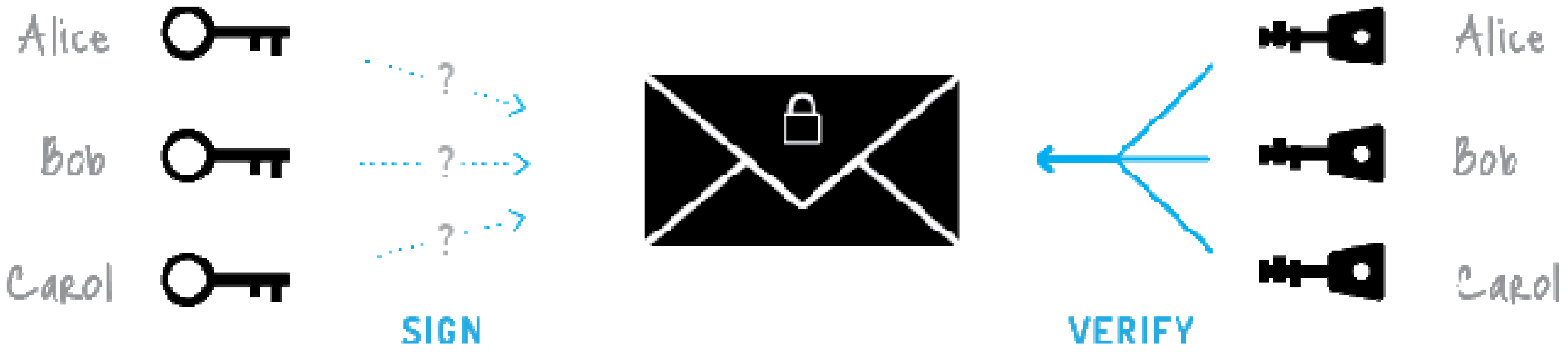
Only member of the group can sign

Anyone can check the signature

Verifier can **only** understand that member of the group signed

Nobody can forge signature of the user

Only group manager can understand who produced a signature

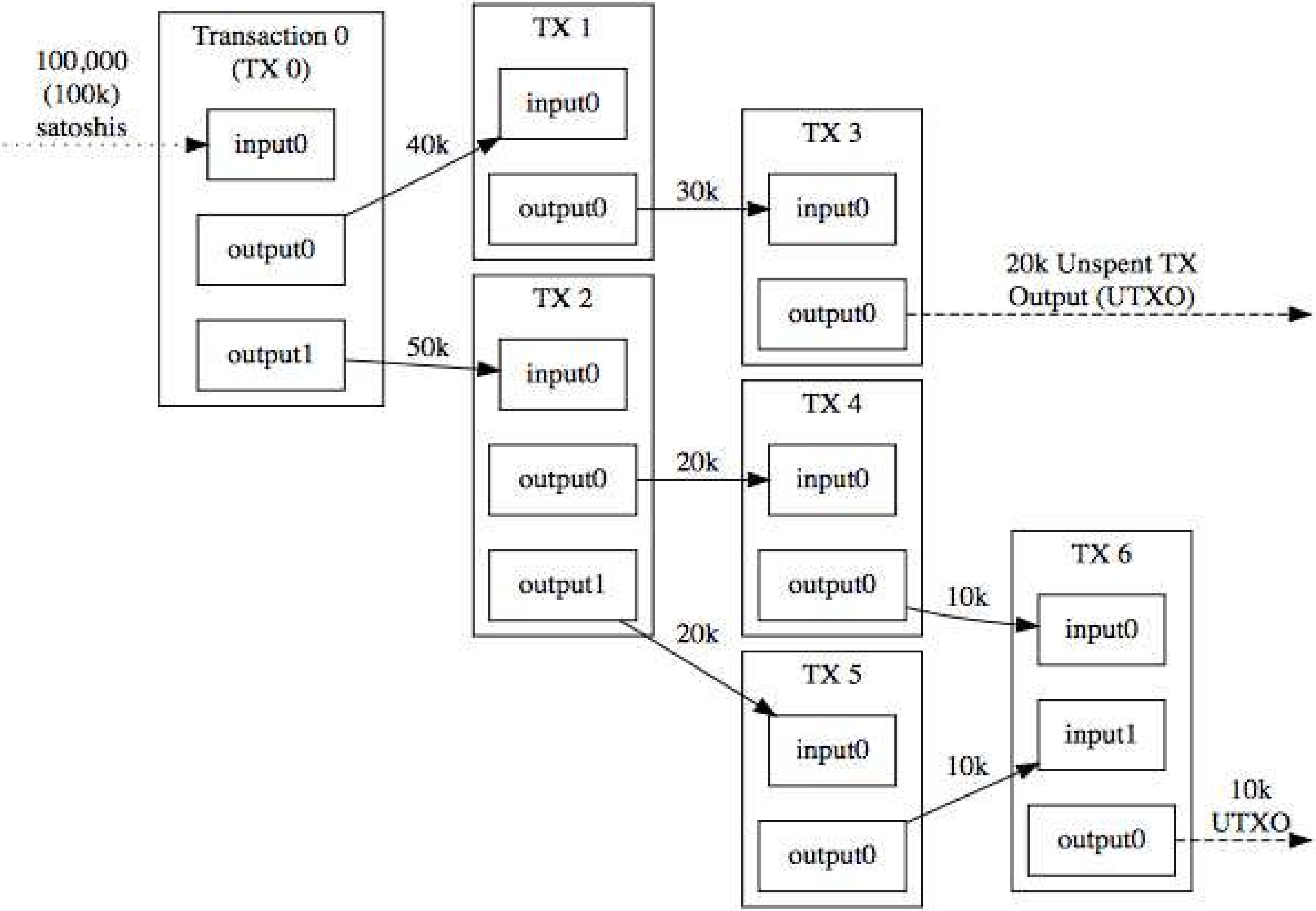


Ring signatures

In a ring signature scheme there are no prearranged groups of users - all user needs is knowledge of others' public keys.

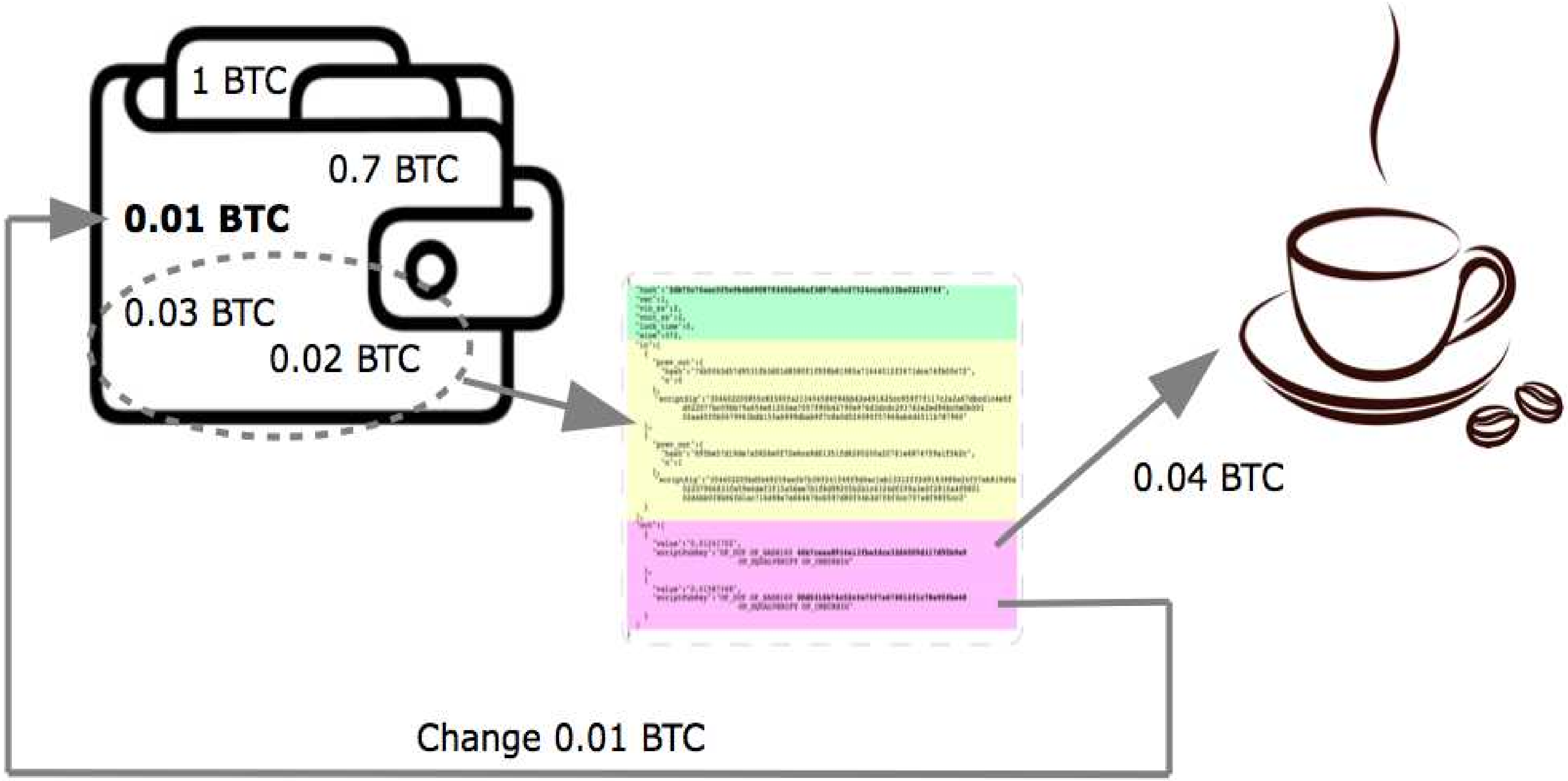
Traceable (or linkable) ring signatures - If the signer used his private key twice (or k times), everyone can see that the two signatures are linked.

```
{
  "hash":"2db75c76aac5f5a9b4b6908793492e66af3d97eb3c27524cca5b33ba0221974f",
  "ver":1,
  "vin_sz":2,
  "vout_sz":2,
  "lock_time":0,
  "size":372,
  "in":[
    {
      "prev_out":{
        "hash":"74b5043d57d9531fb3d01d8380f1f938b81985a71644012f2671dca74fb00c72",
        "n":0
      },
       "scriptSig":"304402205855c83580fa213404588f84bb42e491625cc959f7f117c2a2a67dbcd1c4e5f
             d022077bc09bb79a654e81202ea7057f90b42790e976d3dcdc293762e2ed96bc0e0b501
             02aa45f0b5679963bdb155a6899dbab9f7c8a0d526090f57868ab4d4511b787960"
    },
    {
      "prev_out":{
        "hash":"895be57d19de7a5826e0f72e6ca9d61351fd8280200a20761e6874759a1f562c",
        "n":1
      },
       "scriptSig":"304402205bd5b49259aefb7b389241f48f9d4ac1eb13312ff2d9183888e24f07eb819d0a
             02207966833fe59e6def3f15a56ee7b1f6d99205b2b1c6324df299a3e0f2810a4f9801
             02d4bb0f8b86fd1ac716d98e7e664676cb597d80f04b3d7f8f0cc707a8f98f5cc3"
    }
  ],
  "out":[
    {
      "value":"0.01241702",
      "scriptPubKey":"OP_DUP OP_HASH160 46b7ceaa8916e13fbefdca32d4009d117d95b9e9
                    OP_EQUALVERIFY OP_CHECKSIG"
    },
    {
      "value":"0.01587348",
      "scriptPubKey":"OP_DUP OP_HASH160 00d5316b74c52cfe75f7e676812f1c78e95fbe48
                    OP_EQUALVERIFY OP_CHECKSIG"
    }
  ]
}
```



Triple-Entry Bookkeeping (Transaction-To-Transaction Payments) As Used By Bitcoin

How transaction is formed. Change.



1 BTC
0.7 BTC
0.01 BTC
0.03 BTC
0.02 BTC
0.04 BTC
Change 0.01 BTC