Charade (Stanley Donen, 1963)
1. Money and cash
2. Three threat models
3. Bitcoin in practice
4. A crypto-cash future?
"Spam" is both a technical object and a negotiation.
"'Moneyness,' whatever that is, is a systematic property that depends upon the rules of the game."

Martin Shubik
Store of value
Medium of exchange
Unit of account
Store of value
Medium of exchange
Unit of account
Storage of (social network!) data
A sense of realness
The London Fix
A brief aside about the development of coinage
Fei ch'ien
"Political Money"
Tally Sticks

87 cow rights among 23 owners (on one Alp!)
But let us say you need to pay an army of foreign mercenaries ... (and collect taxes!)
CASH is a pointer to money (with many liabilities)
1. Money and cash
2. Three threat models
3. Bitcoin in practice
4. A crypto-cash future?
THREAT MODEL 1: Small-timers (relatively speaking)
Dr. Mabuse, the Gambler (Fritz Lang, 1922)
COST/THREAT

the counterfeit tradeoff
EASY TO PRODUCE
HARD TO REPRODUCE

EASY TO VERIFY
HARD TO "SOLVE"

(Or, the P≠NP of stuff)
High-resolution banknote images for professional users

The increasing use of personal computers and digital imaging software in counterfeiting banknotes poses a threat to the paper currency. As a response, the Central Bank Counterfeit Deterrence Group, an international group of 27 central banks, has developed the Counterfeit Deterrence System (CDS), which prevents personal computers and digital imaging software from capturing or reproducing the images of protected banknotes.

This system has been implemented voluntarily by several hardware and software producers. This increases the likelihood that legitimate users of banknote images will encounter the CDS in the course of their work.

For users who have a legitimate interest in reproducing euro banknote images, the ECB has produced CDS-disabled digital images (300 dpi; TIFF format and marked “Specimen”), which do not trigger the CDS.

To obtain such images, the user must:
- require the banknote images for professional purposes
- have a personal computer or digital imaging software which includes the CDS
- sign a Confidentiality Declaration

Please send your request for the Confidentiality Declaration form to:

Mr. Vicente Ventura
Directorate Banknotes
EUROPEAN CENTRAL BANK
Kaiserstrasse 29
D-60311 Frankfurt am Main

e-mail: info@ecb.int
THREAT MODEL 2: Inter-state warfare
Bank of England

$20 D M 07432 to pay the Bearer on demand
the Sum of Twenty Pounds

1934 Sept. 20 London 20 Sept. 1934

Twelve

For the Gov. and Compt of the Bank of England

H.O. Peppiatt
Chief Cashier
Bei echten US$ fehlt Linie  

Super $ Fälschung
THREAT MODEL 3: The state itself?
Inflation: Zum Abholen der riesigen Mengen Papiergeld waren Reisefürbe nötig
Variaciones anualizadas del INPC
Años 2012 - 2013
(%)
Private key will be destroyed on 11/24/2013 7:36 PM

Time left 71:58:56

Payment for private key

Choose a convenient payment method and click «Next»:

Bitcoin

Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.

You have to send 0.5 BTC to Bitcoin address 1gVIl7gzmJEP3e2us25CYXvJlzHvKeFlH and specify the Transaction ID on the next page, which will be verified and confirmed.

Home Page
Getting started with Bitcoin

<< Back  Next >>
Bitcoin P2P e-cash paper

Satoshi Nakamoto  Sat, 01 Nov 2008 16:16:33 -0700

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
HELLO?

YES, THIS IS SATOSHI
Running bitcoin

7:33 PM - 10 Jan 09

Don’t miss any updates from halfin
Join Twitter today and follow what interests you!

Full name  Email  Password

Text follow halfin to 40404 in the United States

Sign up
In a sentence: Bitcoins are entries in a distributed database that persistently tracks ownership by address.
Simply, 1:
You use your private key to transact bitcoins from your address to another address on the Bitcoin network.
(A Bitcoin address is just the shortened form of a public key.)
(If you lose your private key, tough luck.)
Simply, 2:
This transaction is broadcast out to the whole Bitcoin peer-to-peer network. There are multiple steps which verify that you have the bitcoin to spend (among other conditions), and the transaction gets added to a block of other recent transactions.
Simply, 3:
This block is then validated as being accurate (including your transaction) and added to the blockchain, the shared public ledger of all transactions. This validation takes about 10 minutes (-ish) and is called mining.
Simply, 4: Why "mining?" To keep people from validating fake transactions (double-spending), adding a block to the blockchain takes computational work: finding an arbitrary, increasingly difficult hash of the block. To make that computational work worthwhile, validating a block rewards you with new bitcoins. Hence, mining.
Simply, 5:
(To put it another way: to mess up the blockchain, you can't merely have a lot of nodes on the Bitcoin network — you must control more than half of the total computing power on the network, which is quite a bit, to solve problems faster than everyone else and get your malicious blocks in the ledger.)
Simply, 6: The problems to solve get progressively more difficult, to slow the disbursement of new bitcoins, and only a finite number will be produced. (Transaction fees will take up the mining-compensation slack.)
Each transaction is actually a program in Script!
Meeting the threat models:

1. Double-spending
   Proof-of-work
   Transaction visibility
2. Mining pools
   Informal agreements
3. Inherently deflationary
   Open source
Some interesting problems:
1. Address correlation
2. Traders and exchanges
3. Mining pools
4. Frisbee-on-the-roof
5. Transaction malleability
Address Correlation

Or, extracting the user network from the transaction network

Traders and exchanges
### Bitcoin Address
Addresses are identifiers which you use to send bitcoins to another person.

<table>
<thead>
<tr>
<th>Summary</th>
<th>Transactions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>No. Transactions: 623</td>
</tr>
<tr>
<td>Hash 160</td>
<td>Total Received: 782,558.72529011 BTC</td>
</tr>
<tr>
<td>Tools</td>
<td>Final Balance: 0.00010161 BTC</td>
</tr>
<tr>
<td>Taint Analysis</td>
<td>Request Payment</td>
</tr>
<tr>
<td>Related Tags</td>
<td>Donation Button</td>
</tr>
<tr>
<td>Unspent Outputs</td>
<td></td>
</tr>
</tbody>
</table>

#### Transactions (Newest First)

- **Transaction: 87510a42b474967a01abf9ea3a16bb0b094aa71d4f97e3651b504c984deaf80**
  - 2014-02-25 14:27:52
- **Transaction: 1AsLCVaf3NN6XMs3vBmjhbWXxX9p7w9d9j**
  - 2014-02-25 13:56:58
- **Transaction: 23fb62bd75238073e672e072e998be96365cbcb22ec811618f7a6b0eb66b5ead8cf**
  - 2014-02-25 14:27:52
- **Transaction: 1JIK5LPsXqTulU8zuFwtrt6GRWWzcs6RRe**
  - 0.01001592 BTC
- **Transaction: 1Mv3vzn0Q8Wv83THvSkFumvILb5W9R4vi**
  - 1 BTC

**About & Contact:** About Us - Status: Ok (601 Nodes Connected) - Advanced: Enable - Currency: Bitcoin
The 51% Cartel Attack?
(Or: the "Goldfinger Attack")
"Frisbee-on-the-roof": Unrealistic, but an interesting thought experiment
Transaction Malleability

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

I am sweating as I write this.

Christmas brought grave news. I cannot adequately express how deeply honored I was by your unconditional support of my staff.

I do not expect the same reaction to today's revelations. This movement is built on integrity, and I feel obligated to be forthright with you.

I held myself to a high standard as your leader, yet now I must utter words all too familiar to this scarred community:

We have been hacked.

Nobody is in danger, no information has been leaked, and server access was never obtained by the attacker.

Our initial investigations indicate that a vendor exploited a recently discovered vulnerability in the Bitcoin protocol known as "transaction malleability" to repeatedly withdraw coins from our system until it was completely empty.

Despite our hardening and pentesting procedures, this attack vector was outside of penetration testing scope due to being rooted in the Bitcoin protocol itself.

This attack hit us at the worst possible time. We were planning on re-launching the new auto-finalize and Dispute Center this past weekend, and our projections of order finalization volume indicated that we would need the community's full balance in hot storage.

-----END PGP SIGNED MESSAGE-----
Re: IMPORTANT: Humbled and Furious

Everyone who is capable please assist us in following these transactions - this is a large amount of money and the individual responsible can and will be located.

If you’re reading this - I hope you grow a pair of balls and return this money before you lose the chance to spend it - if I find you before your moral compass turns back true north you are going to wish you had never been born.

“Government exists to protect us from each other. Where government has gone beyond its limits is in deciding to protect us from ourselves.”

– Ronald Reagan

Re: IMPORTANT: Humbled and Furious

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

I feel I must too apologize. Our security has always been held in high esteem and yet an attack was successful that has cost you all your hard money. I am grateful that no user data was compromised. The market will soldier on. We will prevail in this. The site will return for you all to use safely, only without the escrow feature.

Just as Defcon, I have been furious since discovering this attack on our market. We took our time gathering this data on the perpetrators so as not to compromise their buyers. They are innocent in all of this. That being said, if anyone bought from these vendors and has intel of value, provide it to a member of staff such as myself. You will be rewarded accordingly.

Once again, I am sorry for this devastating loss to you all and hope that you retain your faith in Silk Road.

Cheers
DoctorClu
1. Money and cash
2. Three threat models
3. Bitcoin in practice
4. A crypto-cash future?
Many interesting (non-mining, non-drug) business possibilities: a system worth securing and regulating
Othercoins!

Litecoin
Auroracoin
Dogecoin
Allahcoin
Solarcoin
Primecoin
Freicoin ...

and 125+ more ...
More interesting than mere knockoffs:

*Bitcloud* Proof of stake with bandwidth

*Ethereum* Software development with contracts and transactions!

*Zerocoin* Actually anonymous

*Namecoin* A DNS system!

&:
The Distributed Autonomous Corporation?

Or: after crypto-currency comes crypto-equity!
THANKS!

fb42@nyu.edu
finn@pressmail.ch
(key: finnb.net/public.asc)