

# Bitcoin

Was ist Geld?

Was ist Bitcoin?

# Bitcoin: A Peer-to-Peer Electronic Cash System

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

**Abstract.** A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

## 1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. 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

unterliegt  
niemandem



- ✓ kein Gremium
- ✓ keine Schattenmänner
- ✓ keine Aufsichtsbehörde

Du bist die Bank



Wie schaut eine  
Bitcoin aus?

# Schlüsselpaar

Public

1p<sub>i</sub>ryJgCSNDrLkWZ9dUGqqbC3uuUU4kxH

5JerR4Ci1M1VTmRvjfLTdMcqTbB1cZEwxqEYc97JQXNq2T2v29W

Private

# Die Blockchain

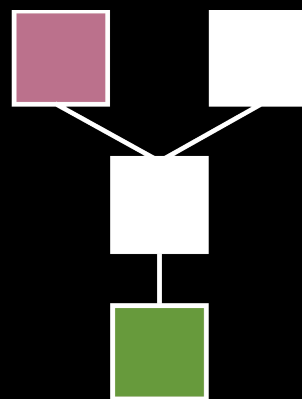
# Die Blockchain



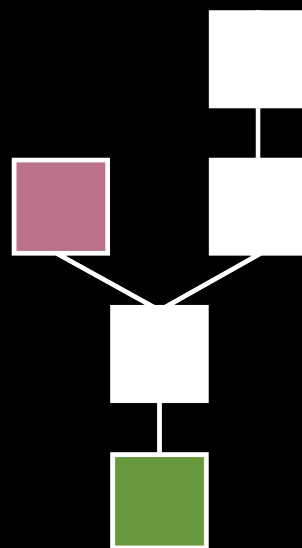
# Die Blockchain



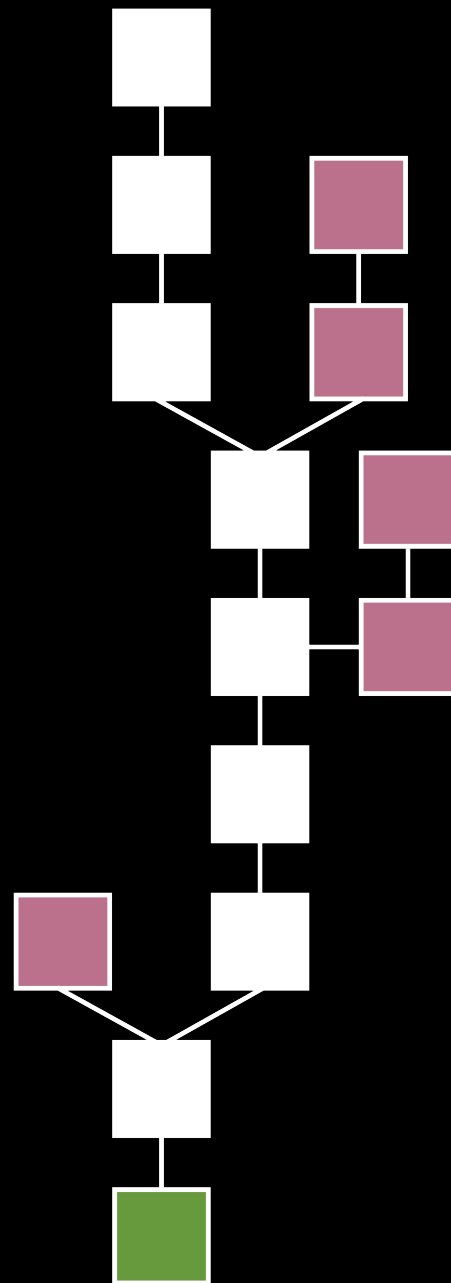
# Die Blockchain



# Die Blockchain



# Die Blockchain





Wie funktioniert's?

1piryJgCSNDrLkWZ9dUGqqbC3uuUU4kxH

# QR Codes



# Zum Thema Anonymität

# Vorteile von Bitcoin

geringe Gebühren

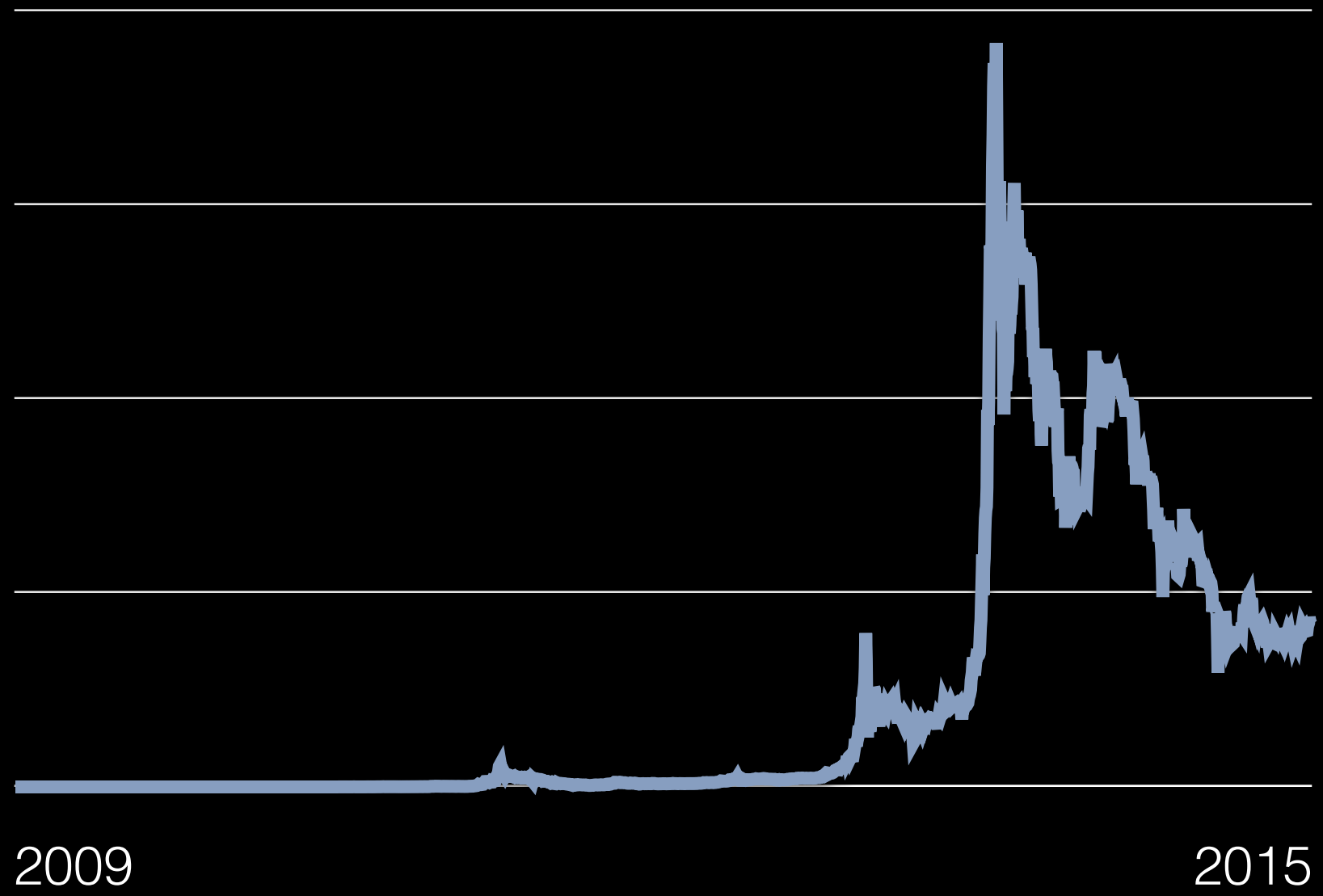
Global

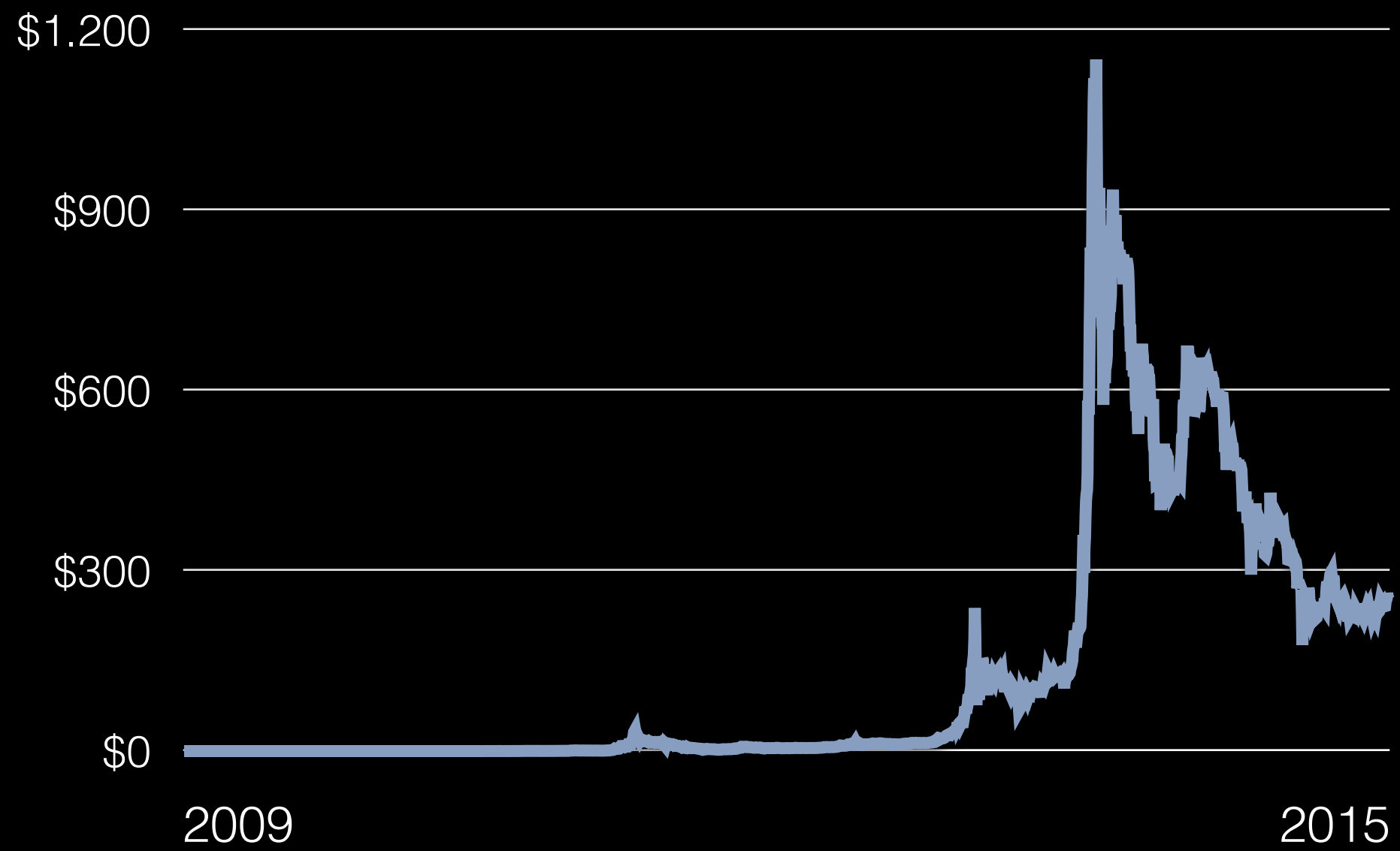
Sicher



Sichererer<sup>TM</sup>

dezentral





# Mythbusting

ABER...

Jeder kann beliebig  
Bitcoin erzeugen

ABER...

Jeder kann beliebig  
Bitcoin erzeugen

A large, thick red 'X' is drawn over the text, indicating that the statement is false or incorrect.

ABER...

Hinter Bitcoin  
steht doch gar nichts



ABER...

Hinte Bitcoin  
steht da immer nichts



ABER...

Nur 21 Millionen?!

ABER...

Nur 21 Millionen?!



ABER...

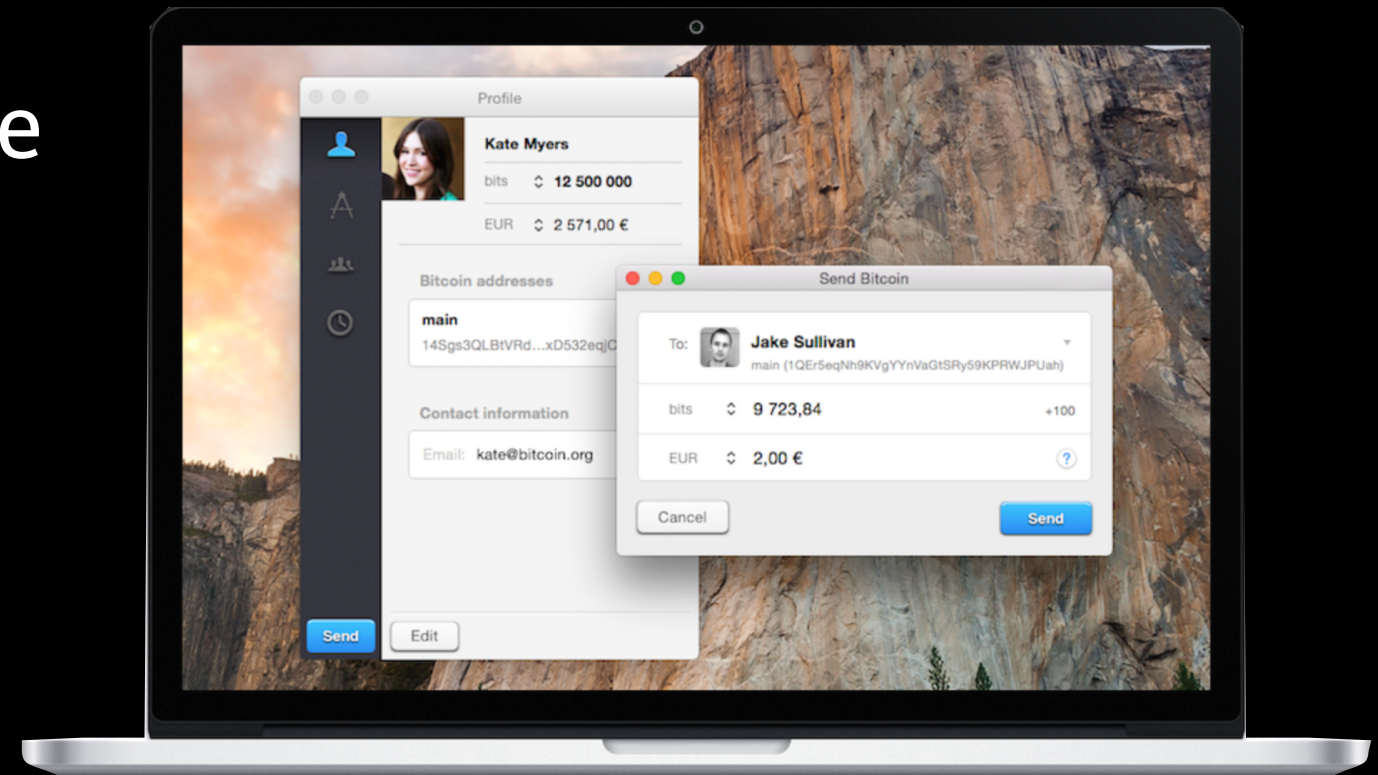
Jemand mit genug  
Rechenpower kann das  
Netzwerk übernehmen.

ABER...

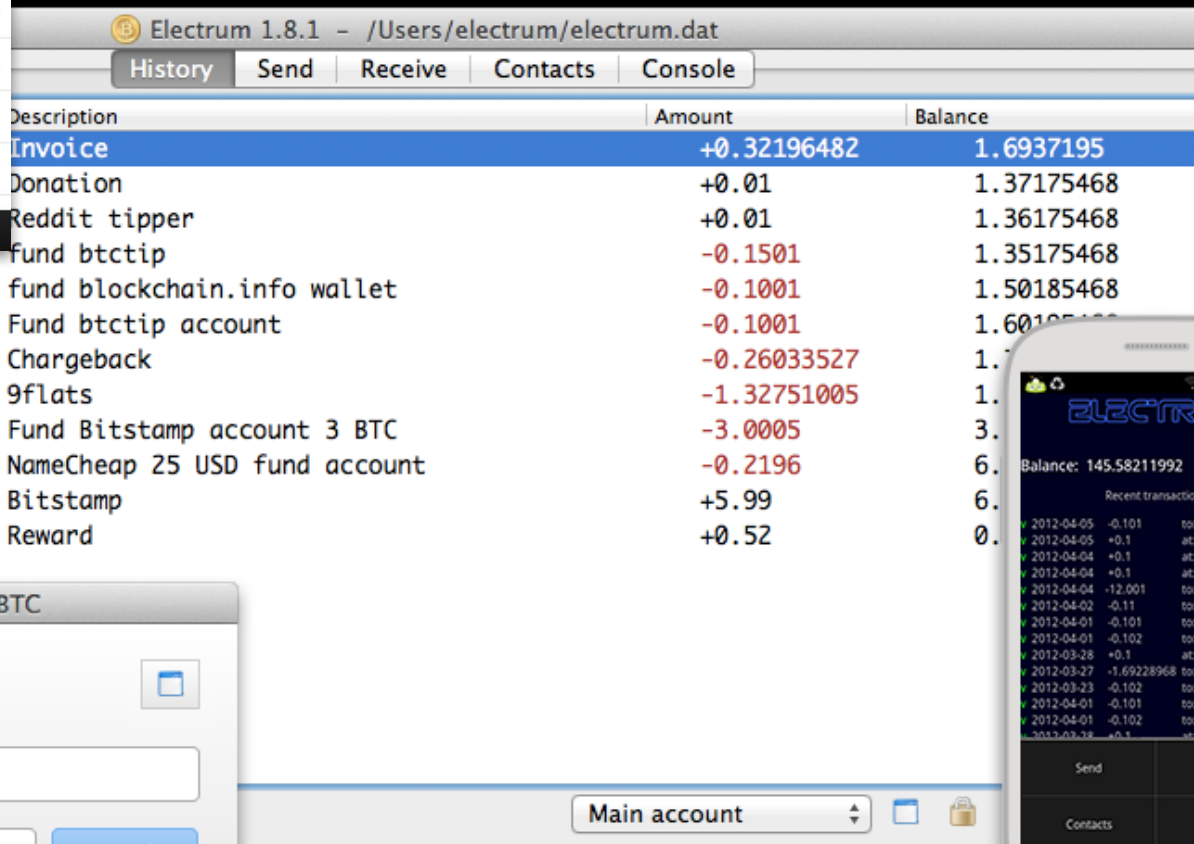
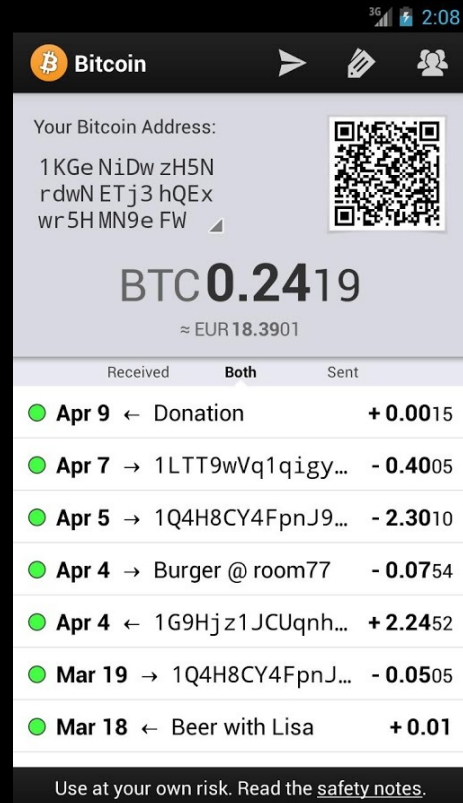
Jemand mit Zugang  
Rechenpower kann das  
Netzwerk übernehmen.



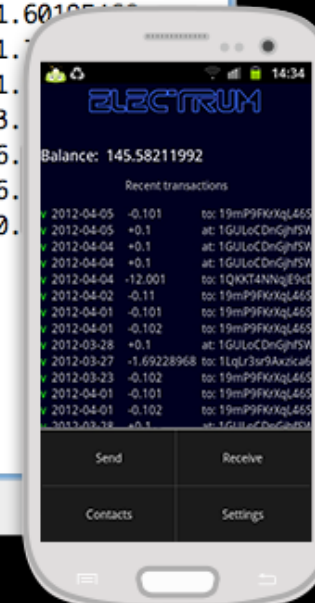
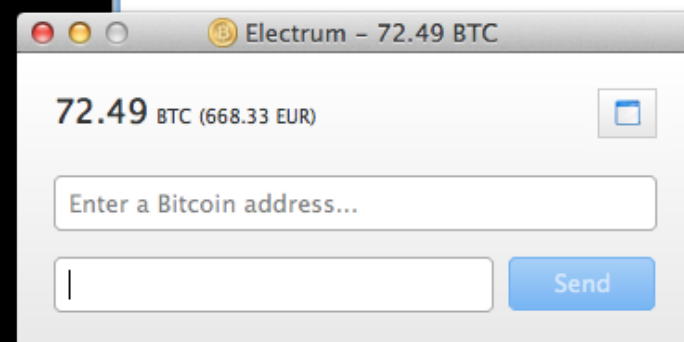
# Hive



# Bitcoin Wallet



# Electrum



Bitcoin Block Explorer - Blockchain.info

Home Charts Stats Markets Developers Wallet

## Home

Most recently mined blocks in the bitcoin block chain

Height	Age	Transactions	Total Sent	Relayed By	Size (kB)
<a href="#">281699</a>	19 minutes	492	4,484.61 BTC	<a href="#">GHash.IO</a>	242.95
<a href="#">281698</a>	30 minutes	546	3,985.58 BTC	<a href="#">GHash.IO</a>	242.87
<a href="#">281697</a>	39 minutes	668	3,132.32 BTC	<a href="#">GHash.IO</a>	243.36
<a href="#">281696</a>	50 minutes	218	3,858.97 BTC	<a href="#">GHash.IO</a>	175.94
<a href="#">281695</a>	51 minutes	790	5,009.31 BTC	<a href="#">BTC Guild</a>	487.44
<a href="#">281694</a>	1 hour 3 minutes	572	3,729.41 BTC	<a href="#">Slush</a>	340.24
<a href="#">281693</a>	1 hour 8 minutes	1501	13,080.42 BTC	<a href="#">BTC Guild</a>	487.26

### Latest Transactions

<a href="#">6507be425fa9ccaa37a594cea...</a>	< 1 minute	0.8461 BTC
<a href="#">a0b40e86dd8fc063e8abd542b...</a>	< 1 minute	0.0619 BTC
<a href="#">74491dfa2da9c3389dfa24a6...</a>	< 1 minute	0.13554694 BTC
<a href="#">87367c570f3be7a9f40997674...</a>	< 1 minute	0.0999 BTC

About & Contact: [About Us](#) - Status: [Ok \(673 Nodes Connected\)](#) - [Advanced](#)

Search

You may enter a block height, address, block hash, transaction hash, hash160, or ipv4 address..

Address / Firstbits / ip / SHA hash

blockchain.info

bitstamp.net

(\$821.61) Bitstamp - buy and sell bitcoins

https://www.bitstamp.net

# BITSTAMP

## Trade Bitcoins with style


You can send Bitcoins over the Internet directly to anyone with no middlemen. Like cash, Bitcoin transactions are irreversible. Bitcoins are traded worldwide. Here are some links to get you started:

[What is Bitcoin?](#) [How to buy Bitcoins?](#) [How to sell Bitcoins?](#)

[Open an account](#)

----- OR -----

[Login](#)




### Funding

SEPA deposits: **FREE**

SEPA withdrawals: **0.90 €**

International wire transfer: **€, \$, £**




### Market

Trading Fee as low as **0.20%**

Live Market Quotes

Instant Trades



### Service

We provide professional service and responsive support. Our site is actively developed and secured.

Simple **Advanced**

Currency Pair: **BTC/USD** Leverage: **None** 1 2 5 10 250

Order: **Buy** **Sell** Start: **Custom...**

Amount: **7** BTC  Amount of BTC to buy

Order Type: **Market** **Limit** Expires: **Good until cancelled**

Buy BTC at the best market price. When this order should be placed on the market. When this order should be cancelled (if not filled).

kraken.com

ZEROBLOCK | Bitcoin

New

# FOR BITCOIN

A new standard for s

- Secure platform on protected hardware
- Margin trading and advanced ordering
- Fast deposits and withdrawals

[Free Signup • Start Trading](#)

Danke :)