Lars Schimmer

GLT 2013

20.April , 2013

Übersicht

- 1. Technik
- 2. Nutzung
- 3. Gefahren
- 4. Fragen?

Bitcoin Ökosystem

- Bitcoin ist eine offene, verteilte, mit Hashsummen gesicherte P2P Datenbank
- Bitcoin ist Synonym für das System, die Nutzung desselben und als Geldsystem
- Keine exklusive Nutzung als Währungssystem

Blockchain

- Datenbank als Blockchain: Daten werden in Blöcken geschrieben, jeder neue Block signiert den vorherhgehenden
- Jeder Client braucht die aktuelle Blockchain
- Die Daten sind frei und öffentlich lesbar
- Geschrieben wird ein Block vom siegreichen Client nach Verifizierung anderer Clients
- Gültig ist eine Blockchain, wenn >1/2 der Rechenleistung im Netzwerk diese nutzt

Transaktionen

- Transaktionen sind Bewegungen von Bitcoins von einem Client zu einem anderen
- Transaktionen werden in die Blöcke geschrieben und jeweils signiert mit dem Key des sendenden Clients
- Jeder Client hat die ganze Toolchain und somit auch die gesamte Liste an Transaktionen des Netzwerks
- Transaktionen brauchen 6 Verifikationen = 6 neue Blöcke nach Aufnahme der Transaktion in einem Block, ca. 1 Stunde

Transaktionen

- Jeder Client hat seinen private Key in einer „Wallet“ – Geldbörse
- Jeder private Key kann viele öffentliche Keys haben – jeder Sender kann eine eigene Adresse des Empfängers bekommen
- Transaktionsgebühren fallen bei geringen Transaktionswerten an (0.0005 BTC)
- Freiwillige Transaktionsgebühren erhöhen Chance auf schnellere Aufnahme in einem Block
- Max. 500 Transaktionen pro Block, mehr warten auf nächste Blöcke

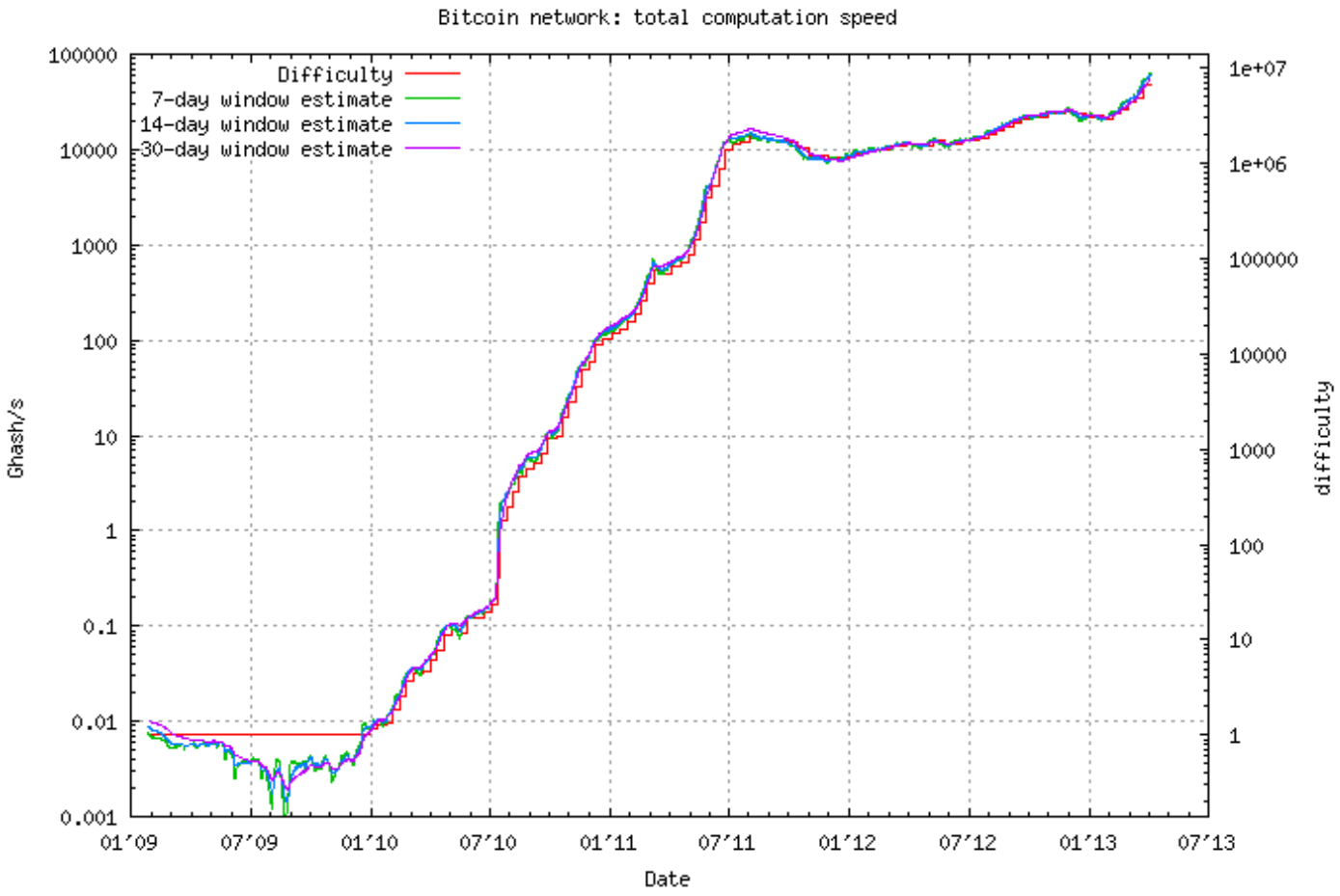
BTC erzeugen

- 2-fache SHA256 Hashsummenberechnung mit Zielwertvorgabe (Difficulty) mit Einrechnung der Transaktionen (merkle Tree)
- Der erste Client mit korrektem Ergebnis darf einen neuen Block schreiben und wartet auf Verifizierung durch andere Clients
- Der Client, der einen Block schreiben darf und verifiziert wurde, erhält eine Belohnung von derzeit 25 BTC und die Transaktionsgebühren für den Block
- Difficulty wird nach 2016 Blöcken neu berechnet

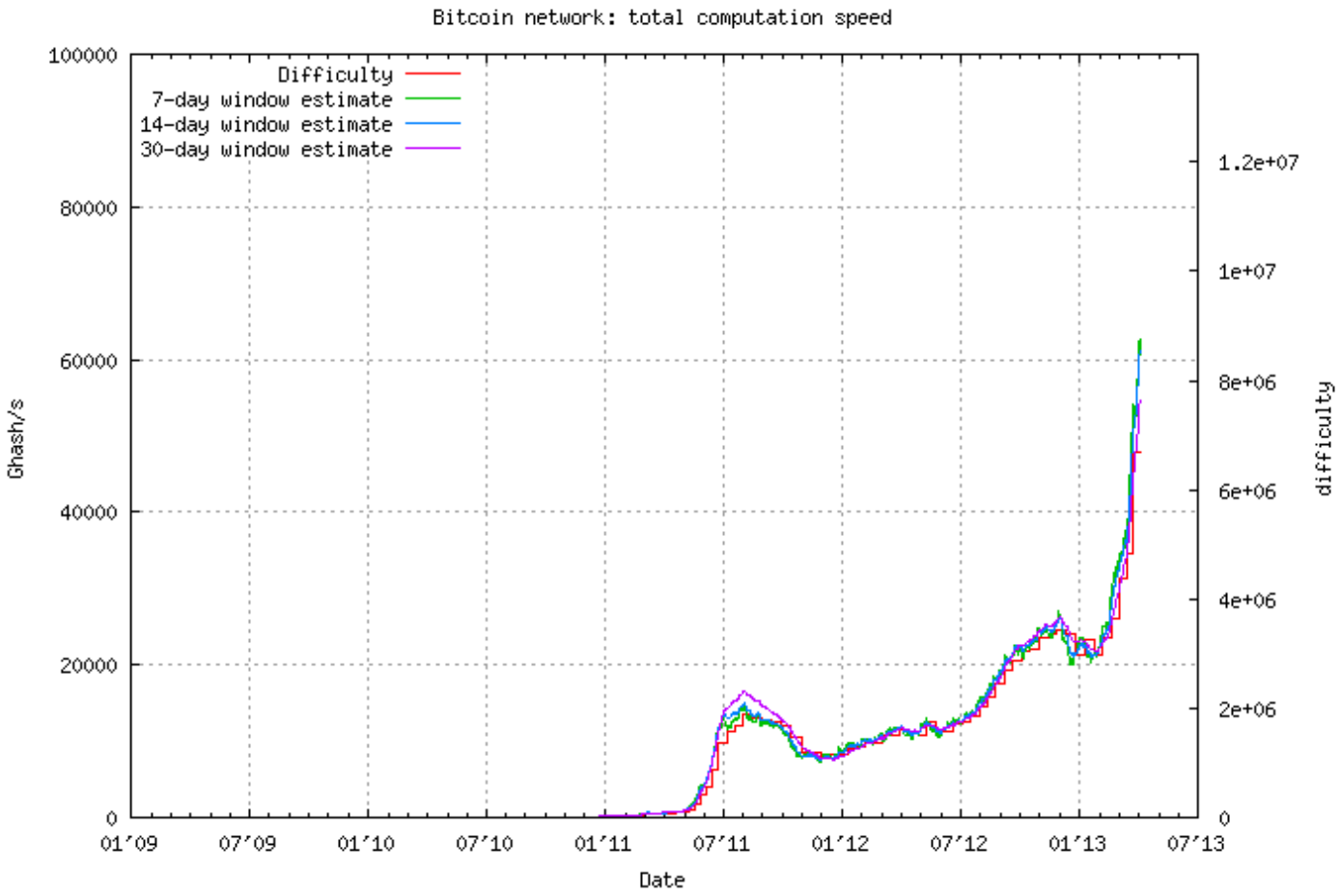
BTC erzeugen

- Vorgabe: 6 Blöcke/Stunde
- Alle 210.000 Blöcke wird die Belohnung halbiert (Anfang 2013 von 50 auf 25 BTC)
- Maximal 21 Millionen BTC werden erzeugt (End ca. 2140)
- Danach nur Transaktionsgebühren als Belohnung des Blockschreibers
- Anfangs mining mit CPU only, dann GPU, später FPGA, ganz neu: ASIC
- Mining Pools als Konzentratoren

Bitcoin Compute Speed



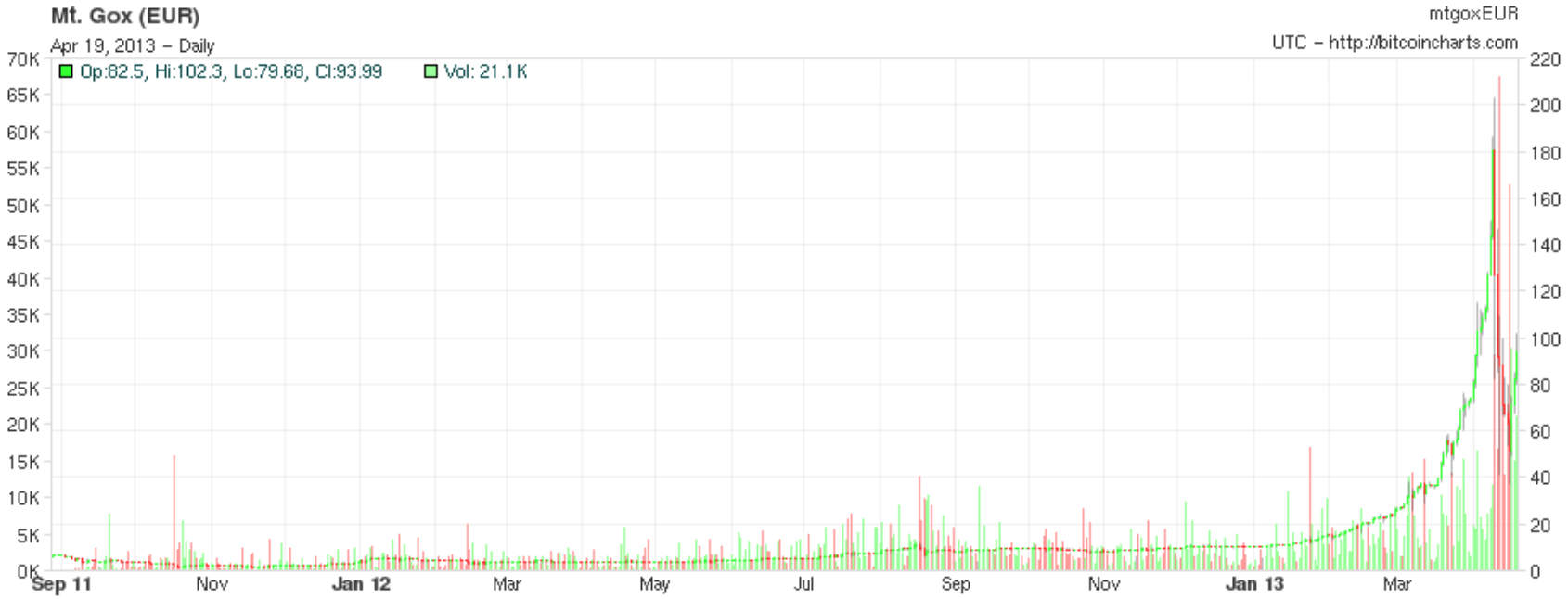
Difficulty Werte



Bitcoin als Geld

- Bitcoins wurden von Anfang an als unabhängiges Währungssystem designed
- Begrenzte Menge an BTC, wenn Wallet weg, dann BTC weg
- Wert ist abhängig vom Vertrauen alleine
- Von Anfang an Waren/Service für BTC (z.B. eine Pizza vom Lieferdienst für 20.000 BTC)
- Später Wechselstuben im Internet (MtGox z.B.)
- Derzeitiger Wert (20.4.2013: 1BTC=91 Euro)
- Kleinste Einheit: 0.00000001 BTC

Bitcoin als Geld



Andere Nutzungen

- Die Technik wird nicht nur für Bitcoins genutzt
- Andere Blockchain, anderer Nutzen
- Z.B. LiteCoin (auch Geld)
- NameCoin – DNS mit Bitcoin
- BitMail – Emails in den Blöcken speichen

Probleme

- Keine Sicherheit auf den Wert eines BTC!
- Mining braucht viel Power (Stromverbrauch)
- Keine offizielle FIAT Währung, keine Anerkennung
- Kann jederzeit verboten werden
- Steuerrechtliche Grauzone (Gewi nne versteuern aber Verluste nicht absetzbar)
- Mit Verlust der Wallet sind die BTC endgültig weg
- Wer 50% der Netzwerkrechenleistung hat, kontrolliert die Blockchain (Mining Pools)
- Viele Online Dienste (hacker, viren, scammer)

Links

- http://www.bitcoin.org
- https://mtgox.com
- https://bitc.oin-24.com
- https://bitcointalk.org
- http://bitcoincharts.com/
- http://bitcoin.sipa.be/
- Uvm.