Bitcoin: digital cryptocurrency for the masses

Colin Dean -> @colindean

#ytaets

August 28, 2013 - YourTalentAgents Emerging Technology Series

Introduction

Agenda

- ✓ Meta
- ✓ Technology overview
- ✓ Real world usage
- ✓ Q&A
- ✓ Thoughts (time permitting)

Knowledge Assumptions

- ✓ Public key cryptography
- ✓ Hashing
- ✓ Basic networking fundamentals
- ✓ Mobile phone or computer

Introduction

Digital cryptocurrency.

- ✓ Digital - not a physical object
- ✓ Crypto - secured by cryptography
- ✓ Currency - can be used as a medium of exchange, i.e. money.

Pedantics of Terminology

- ✓ Bitcoin = protocol
- ✓ bitcoin = money
- ✓ BTC = abbr
- ✓ XBT = proposed ISO 4217 code

Beginnings

- ✓ Satoshi Nakamoto
  - ✓ Anonymous author, absent
- ✓ Began in 2008 or earlier
  - ✓ bitcoin.org registered Aug 2008
- ✓ Genesis block: 3 Jan 2009

Who runs it?

We do.

- ✓ Not a company.
- ✓ Not a security.
- ✓ Not a product.

Beware of misrepresentation.

Who develops it?

- ✓ Team of ~12 developers
- ✓ Gavin Andresen
  - ✓ Lead developer

Two Key Aspects to Technology

- ✓ **Mining** - Generation of Bitcoin, proof of work
- ✓ **Transacting** - Exchange of Bitcoin, proof of authorization

Mining Overview

Two purposes:

- ✓ Inflate supply, gradually decreasing
- ✓ Verify transaction validity

Concerns

- ✓ End user not expected to care
- ✓ End user expected to **be able to care**
- ✓ All can be peers

Basic objects

- ✓ Block: a collection of hashes and values
- ✓ Transaction: transfer of value
- ✓ Blockchain: a series blocks and transactions forming a public ledger

Mining Algorithm

- ✓ in = previous block information plus nonce
- ✓ Block found when **sha256(sha256(in)).to_int** > difficulty
- ✓ Difficulty changes every 2016 blocks

Receive transactions

- ✓ Check mempool
- ✓ Validate transactions
- ✓ Include with block broadcast

Inflating Supply

- ✓ Block = claim block reward
- ✓ Block reward = BTC to miner

Continue inflating

- ✓ Block found every ~10 minutes
- ✓ Sometimes more
- ✓ Sometimes less

Gradually decreasing

January 2009

50 BTC per block - 7200/day

November 2012

25 BTC per block - 3600/day

August 2016?

12.5 BTC per block - 1800/day

Adjusting biweekly for advances

- ✓ Difficulty aids consistency
  - ✓ Up to quarters in a bust
    - ✓ 16 decreases so far
  - ✓ Up to quadruples in a boom
    - ✓ +3,000% since 2012
- ✓ Compared against hash output

Until it stops

- ✓ Continues 32 halvings
- ✓ Stop at **21,000,000 BTC**

When?

- ✓ circa 2140

Or not

Much sooner?

Total Bitcoin to Exist

21,000,000.00000000 BTC

Actually

- ✓ 2,100,000,000,000,000 units
- ✓ 2.1 quadrillion
- ✓ 1 unit = **satoshi**

Comparison

- 10.5 trillion USD in M2: Federal Reserve
  - M2 = money markets + savings + CDs < $100k PLUS
  - M1 = checking accounts PLUS
  - M0 = currency in circulation
  - M3 = larger deposits, institutional money

Mapped to USD

- ✓ $200,000 = 1 BTC
- ✓ Worldwide M3 in circulation = ~ $75 trillion (2010)

Coins in circulation

11.5 million

(as of 8 August 2013)

Also, fees

Block reward + transaction fees

- ✓ 2013: 25 BTC + < .5 BTC
- ✓ 2140: 0 BTC + ??? BTC
- ✓ Fees > reward in 2070s or sooner

Mining programs

- ✓ Automation
- ✓ Work distribution, via pooled mining
- ✓ Alternative processors (GPU, FPGA, ASIC)

Questions about mining?

- ✓ Unprofitable without investment now

Transacting Overview

- ✓ Generating addresses
- ✓ Interconnecting
- ✓ Receiving
- ✓ Sending

Generating addresses

- ✓ Public key cryptography
  - ✓ Private key
  - ✓ Public key
- ✓ HASH160

Address composition

- ✓ 34 characters
- ✓ First character
  - ✓ 1 = Bitcoin public key string or **address**
  - ✓ 5 = Bitcoin private key string
- ✓ Base58 ensures readability
- ✓ Checksum

Interconnecting

- ✓ Lookups
  - ✓ DNS
  - ✓ IRC (going away)
- ✓ P2P
- ✓ Negotiation

Receiving

- ✓ Inputs -> Outputs
- ✓ Ledger vs reality
- ✓ Verification

Sending

- ✓ Transaction creation
- ✓ Spending outputs
- ✓ Fees
- ✓ Broadcast

Real World Usage

- ✓ Official client: bitcoin.org
- ✓ Several other popular clients (SPV! Electrum!)

Getting Bitcoin (hard way)

- ✓ Exchange (Mt.Gox, CampBX)
- ✓ Seller (Coinbase)
- ✓ OTC (LocalBitcoins)

Getting Bitcoin (easy way)

- ✓ Earn!
  - ✓ Work
  - ✓ Comment - /r/bitcointip
- ✓ Beg
  - ✓ Faucets

Spending Bitcoin

- ✓ Type an address
- ✓ Scan a QRcode

Where to spend

- ✓ Wiki/Trade - huge list
- ✓ BitcoinStore - online CE store
- ✓ In Pittsburgh
  - ✓ Oh Yeah! - Highland Ave, Shadyside
  - ✓ Waffalonia - Murray Ave, Squirrel Hill

Demo

Multibit to Android

Advantages versus others

- ✓ Quick transfer for asynchronous payments
- ✓ Theoretically anonymous
- ✓ No external control

Disadvantages against others

- ✓ Long transfer for synchronous payments
- ✓ Balances public (but difficult to trace)
- ✓ Requires electronics and Internet
  - ✓ Innovations diminishing this

Warning

This is beta technology.

It can break.

You can lose money.

No one can save you from yourself.

Backup frequently and **securely**.

Q&A

Questions? Demandoj?

Resources

- ✓ Bitcoin Wiki
- ✓ Bitcoin StackExchange
- ✓ Bitcoin Foundation
- ✓ BitcoinTalk

Altcoins

- ✓ Clones that change components and variables
- ✓ Litecoin - scrypt, 2.5 min conf
- ✓ Feathercoin - scrypt, 2.5 min conf, checkpointing
- ✓ DevCoin, Primecoin, PPCoin, Ripple
- ✓ Garzik's Law

Branch projects

- ✓ NameCoin - distributed domain name system
- ✓ BitMessage - expiring messaging

Prior Art

- ✓ Hashcash - Adam Back (1997)
  - ✓ Spam countermeasure
- ✓ bmoney - Wei Dei (1998)
- ✓ bitgold - Nick Szabo (1998)
- ✓ “Proofs of Work and Bread Pudding Protocols” - Jakobsson & Juels (1999)
- ✓ RPOW - Hal Finney (2004)

Challenges

- ✓ Reliance on connectivity
- ✓ Software learning curve
- ✓ Regulatory burden

Under the banyan tree

- ✓ Offline transactions added to Android client
- ✓ Physical bitcoin
- ✓ Brainwallet

New wallet for new paradigm

- ✓ Hard to teach security
- ✓ Hard to earn trust, seconds to lose it forever
- ✓ Storage requirements for first-class node
- ✓ Mobility

Fiat <-> Bitcoin is hard

- ✓ Government regulations
- ✓ Bank interference
- ✓ Emerging businesses
  - ✓ Intent
  - ✓ Security
  - ✓ Trust

References

- ✓ Federal Reserve Money Stock Measures
- ✓ Quantative Easing is Nothing New by Mike Hewitt
- ✓ Difficulty Adjustment History
- ✓ Bitcoin is Worse is Better

Thanks!

Colin Dean
@colindean