Bitcoin

The World's First Person-to-Person digital currency

Gavin Andresen
gavin@acm.org

Monday, June 20, 2011

The Bitcoin Project is an experiment-- a very ambitious experiment. The goal of the project is to create a better international currency and payment network-- one that is stable and secure, and one that gives people more direct control over their finances.

I'm going to tell you what it is, how it is different from the currencies we're all using today, get into some technical details about how it works, and give a few example of innovative projects that are using it. I'll finish by giving a brief summary of the progress of the project so far, and speculate a little bit on what is likely to happen in the future.

Bitcoin is Pure Money

Monday, June 20, 2011

What is a bitcoin? Bitcoins are very close to a “pure money” -- they are digital transactions that function as money. They are a unit of account, a means of exchange, and a store of value, but unlike previous digital currencies, they are not backed by precious metals or the full faith and credit of any government. They are almost the Platonic ideal of money, and are valuable only because they are useful as a money. That is a concept that most people have trouble accepting; that a money “backed by nothing” can be valuable. But if you think about why we value things it makes sense. I value a hammer because it is good at banging on nails. Bitcoins are valuable because they are good to use as money.

Also unlike previous digital currencies, bitcoin is completely decentralized. There is no central bank issuing bitcoins and there is no payment processing company validating transactions. Before credit card companies and national currencies, people used decentralized non-digital currencies like gold and silver. Some people have suggested that bitcoin might be Gold 2.0 -- a digital version of one of the most ancient forms of money.

Bitcoin is Payment Network

Decentralized

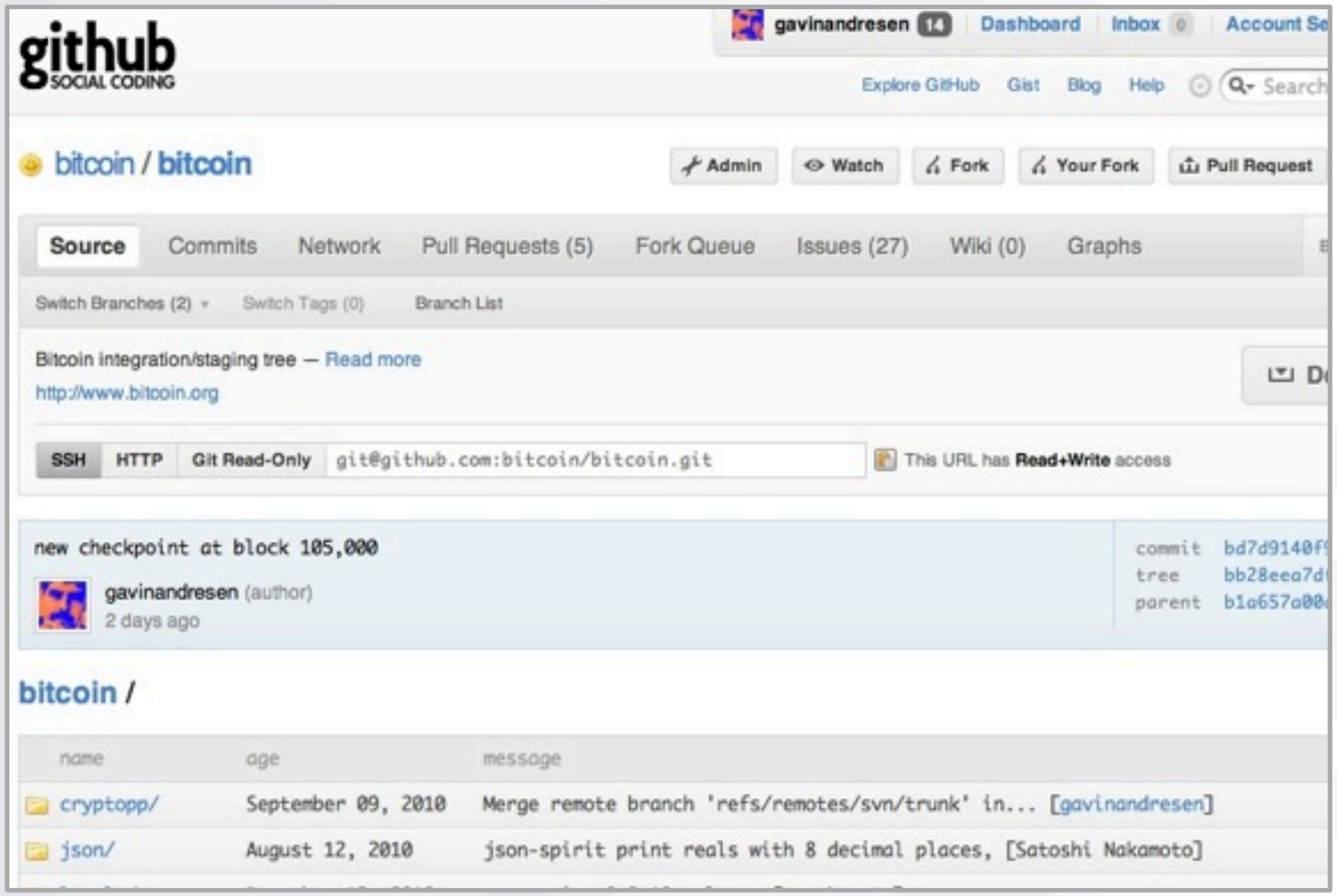
Node-to-node

Monday, June 20, 2011

Bitcoin is also a global peer-to-peer network, across which transactions are broadcast. Your computer must be connected to the Internet to send or receive transactions, but there are no sign-up requirements or fees to pay; anybody can join and participate in the payment network. There is no central organization with a list of approved Bitcoin Payment Processors.

There are somewhere between 20 and 30 thousand nodes connected at any given time; any given node is connected to between 8 and 150 mostly-randomly-selected neighbors.

Bitcoin is Open Source



Monday, June 20, 2011

Bitcoin is open source, released under the MIT software license, which allows anybody to anything they wish with it. It was first released in January, 2009, and has been downloaded by hundreds of thousands of people. I'm one of five core developers who has direct write access to the reference implementation's source code, but we have accepted patches from a programmers from all over the world. The five core developers are from four different countries.

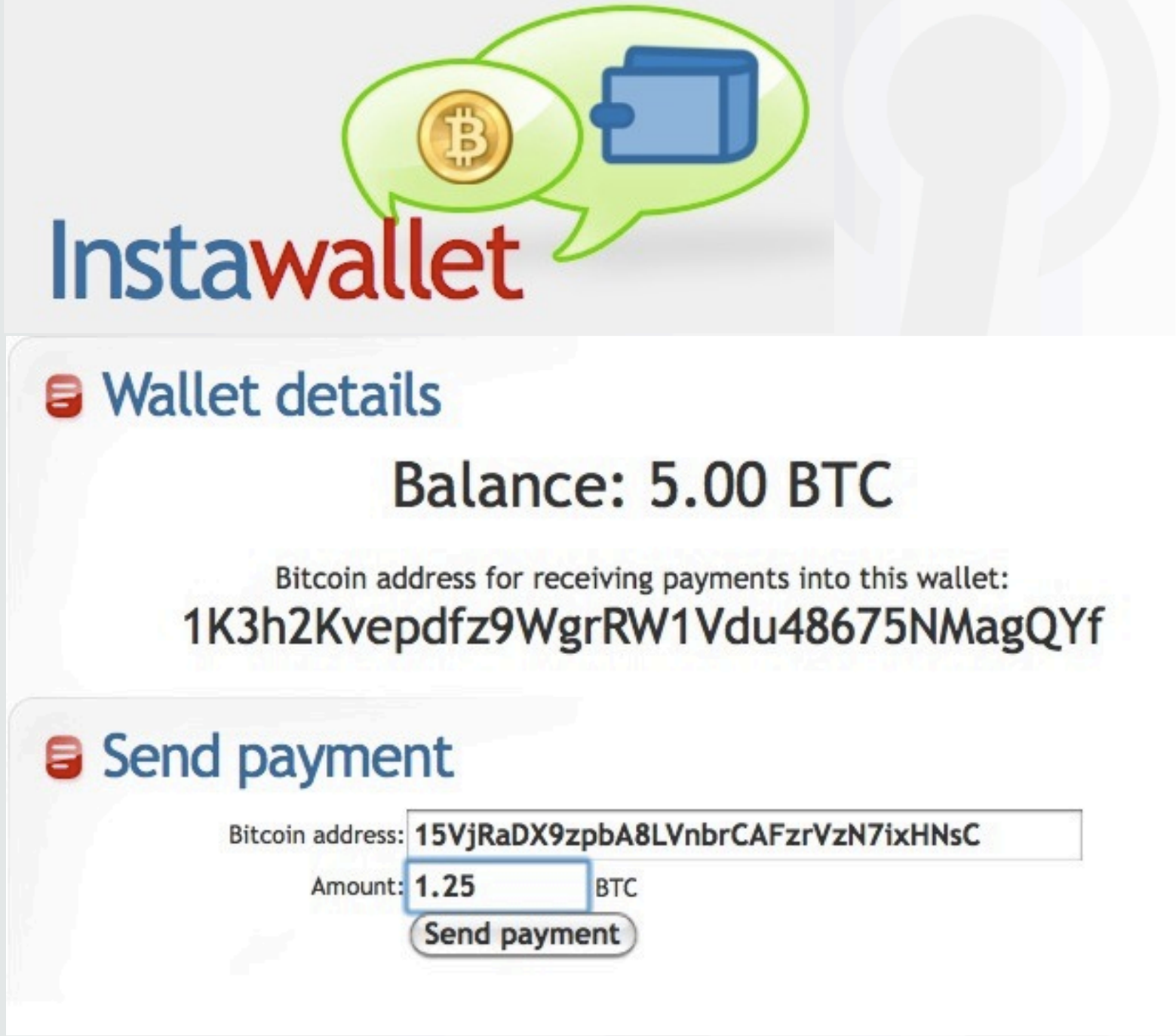
Everybody is a volunteer; there is no official Bitcoin Incorporated to pay anybody a salary. Bitcoin is the first major open source project that I've been involved with, and the loose organizational structure is both refreshing and frustrating. Refreshing because it really is a meritocracy-- help the project move forward and you'll earn the respect of "the community." Frustrating because I can't just fire the real idiots.

What's the big deal?

- "Open money"
- Best available technology
- Designed for Innovation

Monday, June 20, 2011

So what's the big deal? Why all the hype, and why do I think bitcoin has the potential to have a huge impact on the world?
Many of the early adopters are excited by the idea of "open money" -- a trust-no-one currency that isn't subject to manipulation by central bankers who are supposed to be wise enough to know what the right monetary policy aught to be at any given moment. Many are also excited by the idea of a payment system that is written from scratch and based on the very best cryptography and designed to work securely over the existing, public Internet.
I am optimistic about bitcoin's future because it is designed for innovation, and I believe that innovation is the key to our long-term economic prosperity.



https://www.instawallet.org/

Monday, June 20, 2011

Innovation example #1: This is a screen shot of my "instawallet". Instawallet.org is an online bitcoin wallet service created by a person in Germany; it is a website that will hold bitcoins for you. The first time you visit, it creates an empty wallet and gives you a bitcoin address for receiving payments-- no sign-up or registration is required. I've got 5 bitcoins in my instawallet. If I want to send them to somebody else, I just paste their bitcoin address into the Send Payment form, enter the amount I want to send, and press the Send payment button. Software running on the Instawallet web server is connected to the bitcoin network to send and receive payments.
For poor people around the world who don't have access to banking services but might soon have Internet access on their mobile phones, a solution like Instawallet could have a huge impact, giving them a safe place to store small amounts of wealth and a very low-cost way to pay anybody, anywhere in the world.

Ways to get bitcoin

- Buy from exchange
- Sell something for them
- Generate them

Monday, June 20, 2011

Once you have a wallet, there are three ways to get bitcoins. You can trade another currency that you happen to have (maybe the dollars that you're sitting on right now) either directly with somebody who already has bitcoin or through a bitcoin-dollar currency exchange. The biggest bitcoin exchange today is a website called "MtGox", and on a typical day it is handling over $1million in transactions. One bitcoin currently costs roughly $20.

You can also get bitcoins by trading something other than currency for them-- you can sell something or provide a service and earn them, assuming you can find somebody willing to pay for your product or service in bitcoin.

The last way you can get bitcoins is the way all bitcoins are initially created-- you can (try) to generate them. Remember that bitcoin is completely decentralized, so even the task of creating the currency is done by the nodes on the network. Figuring out a secure way of doing that was the technical breakthrough that makes the entire system possible.

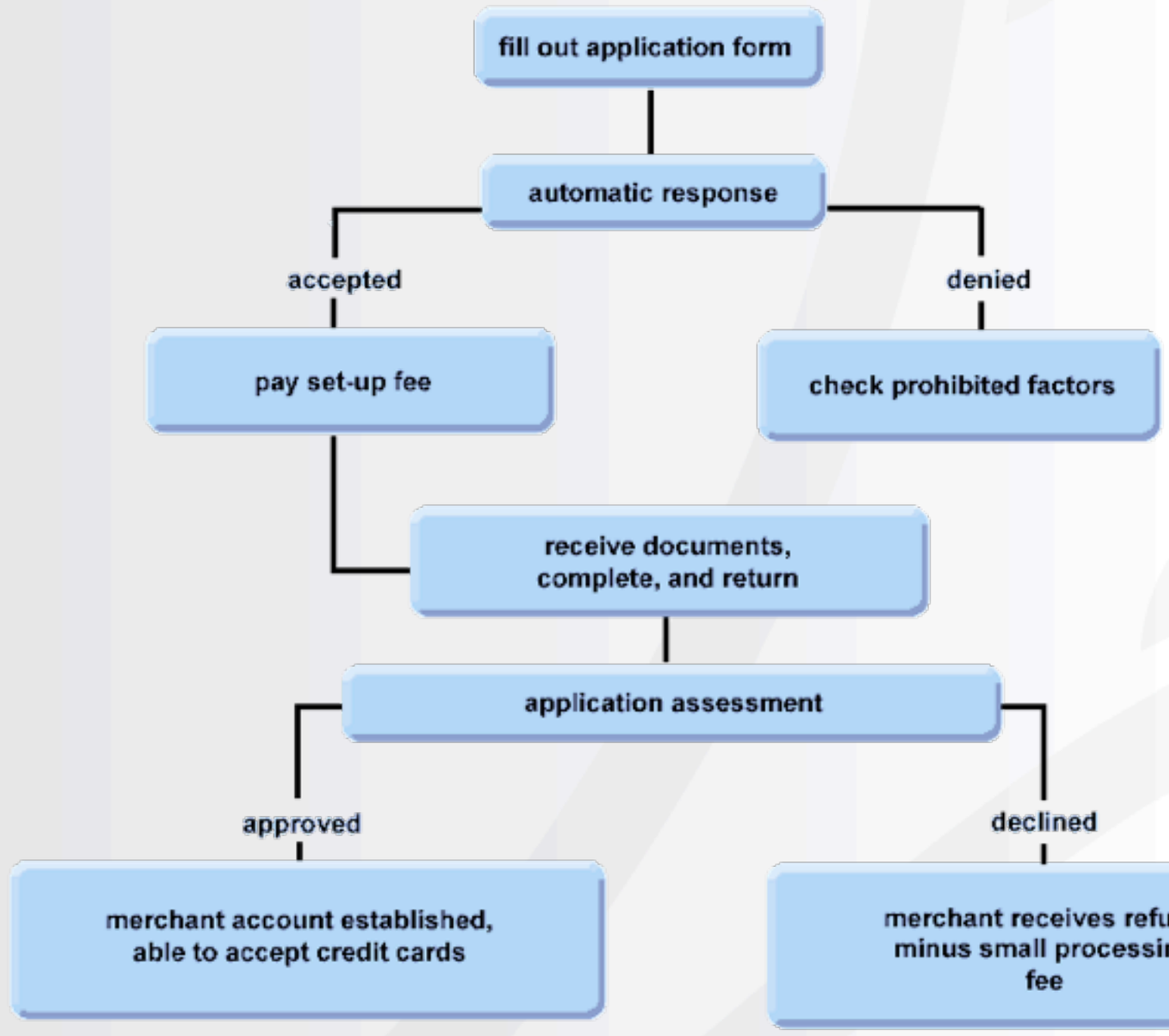
Who accepts Bitcoins?

Image credit: weusecoins.com

Monday, June 20, 2011

The bitcoin economy is tiny but growing; more and more merchants are accepting bitcoin as payment. Bitcoin is attractive to merchants because bitcoins are like cash-- there are no forms to fill out or membership fee, transaction fees are very, very low, and there are no chargebacks (all sales are final-- once a bitcoin transaction is sent to the network, it cannot be reversed). Early adopters were mostly online services-- web hosting, phone-over-the-internet, web developers offering their services for bitcoin. The biggest barrier to the adoption of bitcoin by merchants selling physical goods is bitcoin's huge hour-to-hour price volatility. Daily swings in the bitcoin-to-dollar exchange rate of plus or minus 40% are common. That is one of many chicken-and-egg problems that bitcoin will have to overcome if it is ever going to be more than a novelty currency that only geeks like me use.

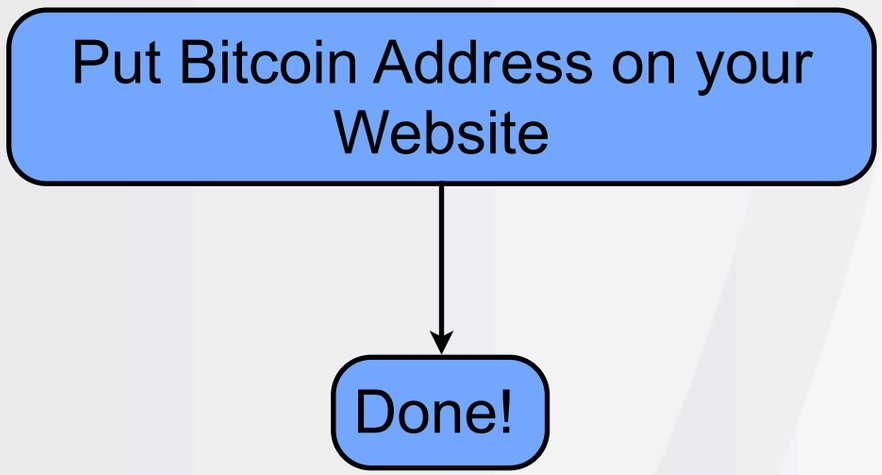
Accepting credit cards



Monday, June 20, 2011

In spite of the huge price swings, there are some brave merchants selling tangible goods for bitcoins. Part of the reason is because compared to accepting credit cards, accepting bitcoin is trivial. This is a flow chart I got from the website of a company providing merchant services, explaining the process for getting an account with them. Compare that to the process for accepting bitcoins:

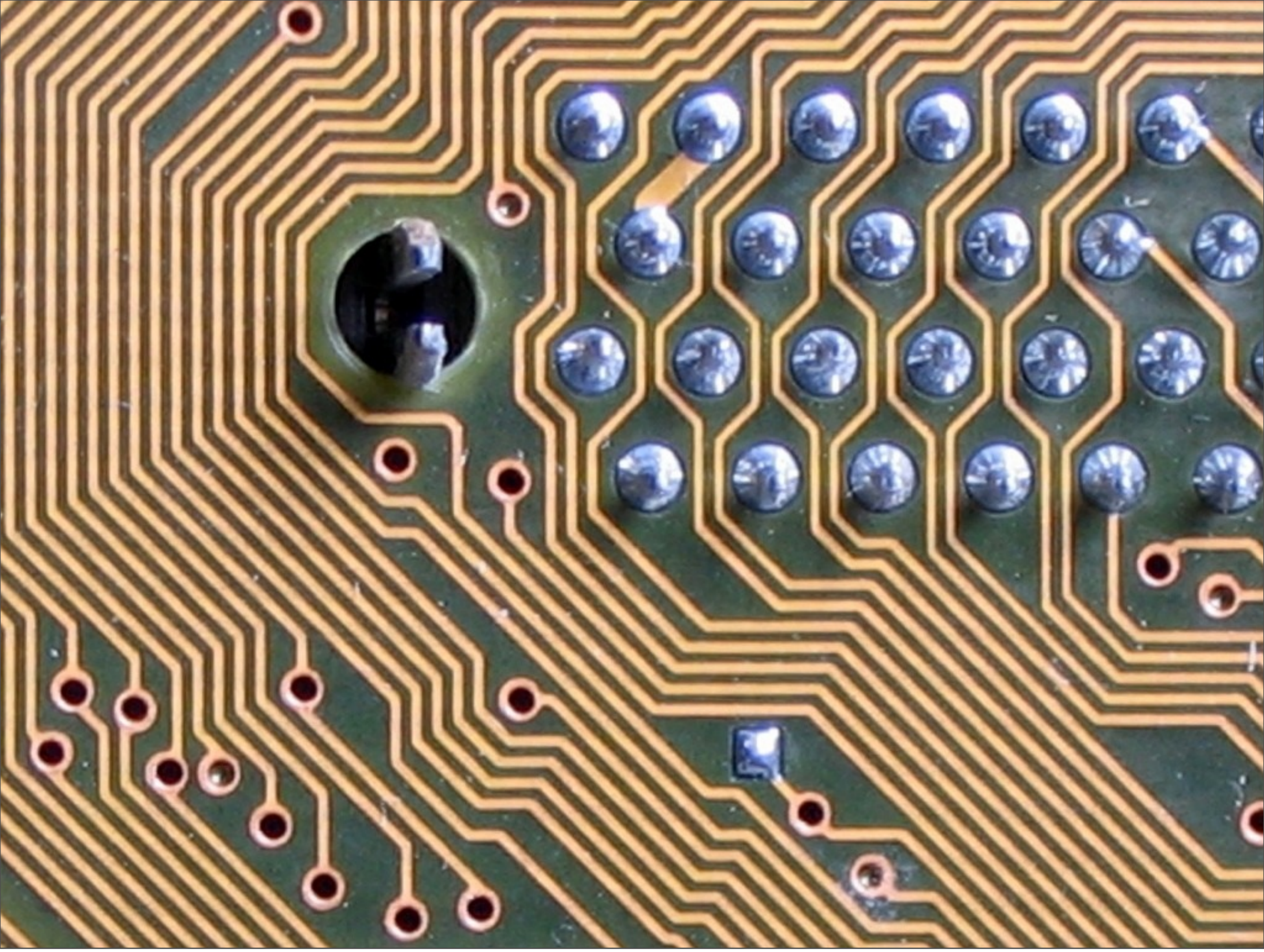
Accepting Bitcoin



Monday, June 20, 2011

One step: ask your customers to pay to one of your bitcoin addresses. That is it. It would be two steps if you want to count setting up a bitcoin wallet as a separate step-- visit instawallet.org, then somehow tell your customers your new bitcoin receiving address.

There is still a lot of infrastructure yet to be adapted or built for merchants that accept bitcoin; merchants that process a high volume of transactions will want a solution that plugs into their existing back end order management systems, for example. Bitcoin is still just a toddler; it has a lot of growing up to do.



Monday, June 20, 2011

Image credit: http://www.flickr.com/photos/hinkelstone/2435823037/

So: what is a bitcoin REALLY? I'm going to get technical for a bit and dive deep into its guts, describing the novel algorithm that securely creates a predictable supply of bitcoins and describing what bitcoins really are-- cryptographically signed transactions.

Proof-of-work block chain

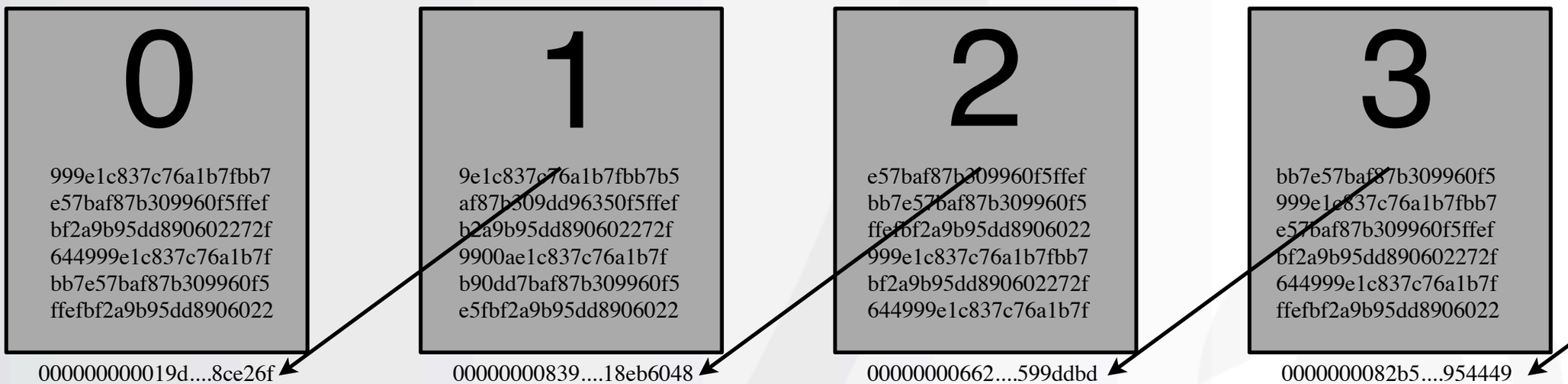
- **Key breakthrough**
- Two ideas:
  1. Hash chain
  2. Proof-of-work
- Distributed time-stamping algorithm, solves “double-spend” problem

Monday, June 20, 2011

The key technical breakthrough that makes a decentralized digital currency possible is the combination of two existing ideas: a hash chain, and proof-of-work. Together they solve the general ‘distributed time-stamping’ problem.

For a digital currency, the problem is if some digital coins are spent twice, which “spend” is valid? That is easy with a central server-- whichever one reaches the server first is the valid one. Decentralized is much harder.

Hash chain

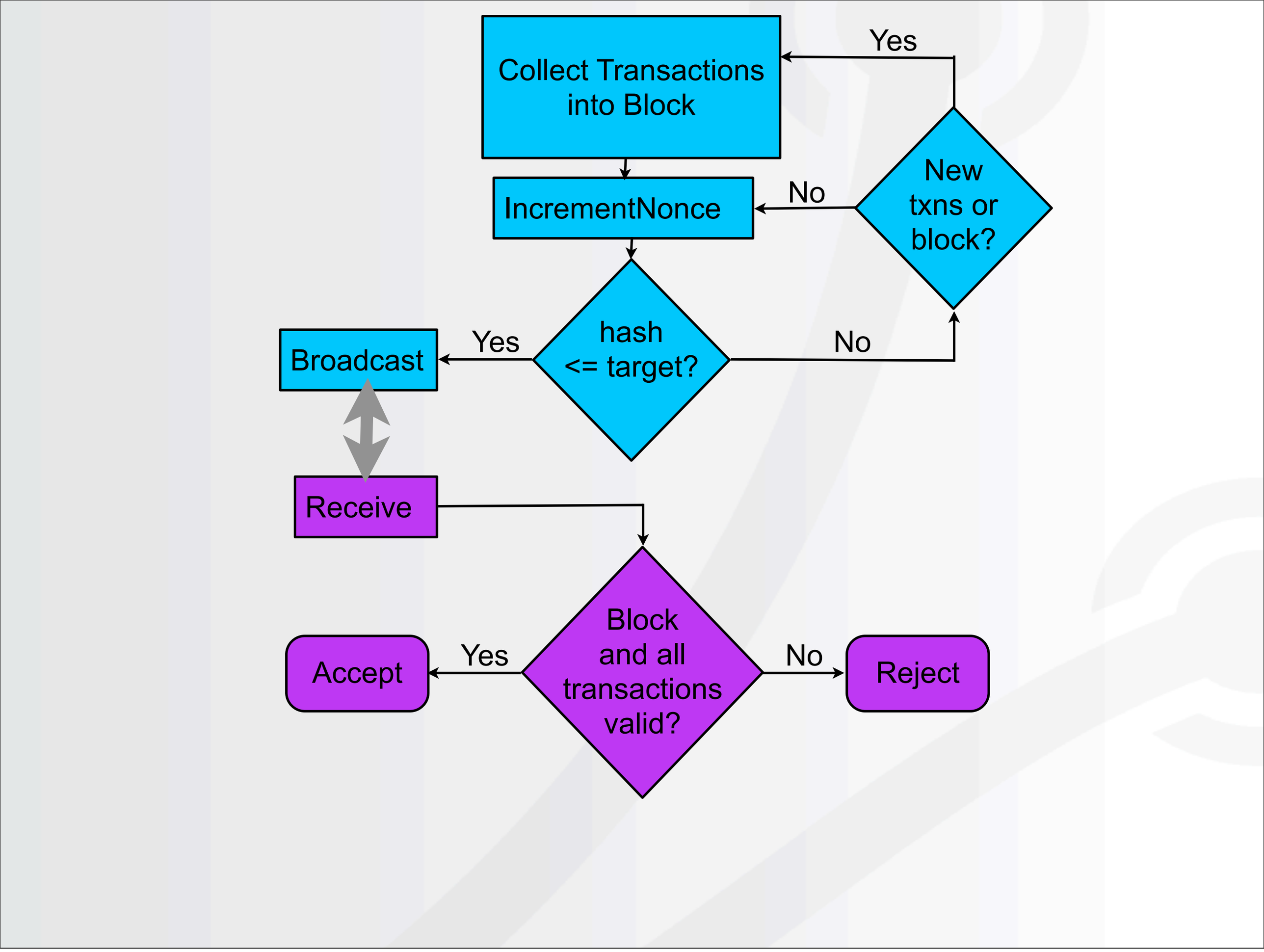


Monday, June 20, 2011

First part of solution: the hash chain.

Starts w. Genesis block (hard-coded). Blocks contain: hash of prev block, valid txns, timestamp. First txn: block reward (50 BTC). All nodes in network verify all blocks.

Changing any piece of data in any block changes the hash for that block and all subsequent blocks. The block chain is the canonical record of all bitcoin transactions.



Monday, June 20, 2011

Second piece is proof-of-work. All generating nodes (aka “bitcoin miners”, like mining for gold) are running the algorithm in blue, trying to find a block hash smaller than the current hash target. Serves two purposes: limits the number of bitcoins created over time. And is a fair way of selecting which transactions will be considered valid.
All nodes on the network check their work (algorithm in purple), and will not accept invalid blocks.
Incentive for bitcoin miners to find blocks: first transaction in every block creates new bitcoins, miners create a transaction that pays themselves newly-minted coins.

Hash Target

Block 1:
`0x00000000fff0000000000000000000000000000000000000000000000000`

Block 126,430:
`0x00000000000044b9f200000000000000000000000000000000000000000`

Monday, June 20, 2011

The hash target is adjusted every 2016 blocks so that no matter how many computers are computing block hashes, only 6 blocks are generated per hour (2016 blocks divided by 6 blocks per hour is two weeks). All nodes compute it using the timestamps that are in the blocks in the block chain, so all nodes compute exactly the same target value. Hashes are 256-bit numbers, which are inconceivably large. The current target is over 800,000 times more difficult to hit than the original target, and is growing rapidly as more people join the bitcoin network and try to generate coins.

Block Race

Monday, June 20, 2011

Two (or more) nodes might find the next block at about the same time. Both will broadcast to the network, and the result is a “block race.” The **next** block found will almost always resolve the race, by building on one of the blocks (repeated races are possible but become increasingly unlikely).

Centralized is simpler

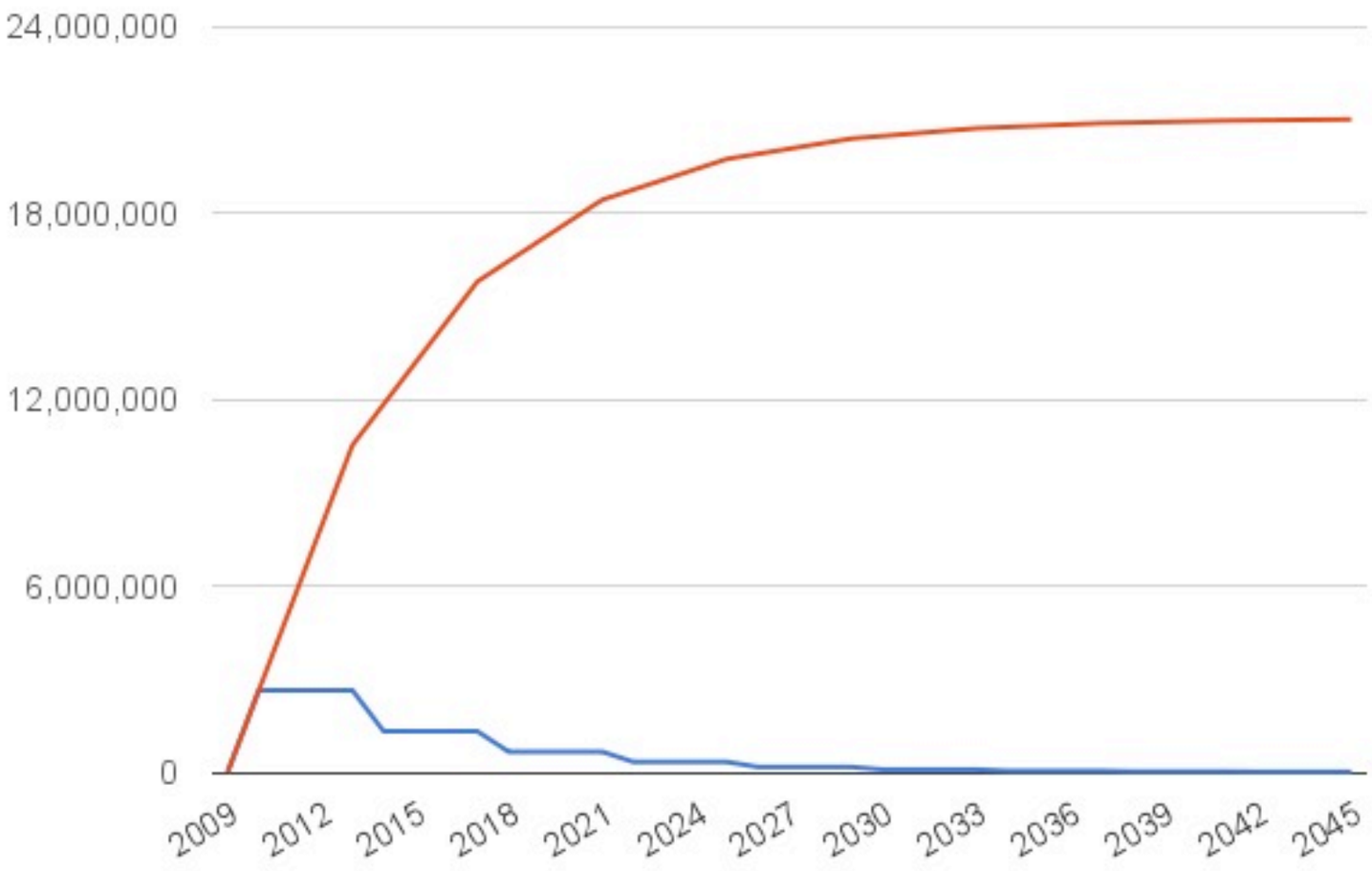
Bitcoin is Trust No One

Monday, June 20, 2011

Why bother being decentralized?
Centralized solutions are much simpler: use a central server to issue money, process/verify transactions. BUT: you must trust the central authority, and if the central authority fails or is compromised the results can be catastrophic.
Bitcoin is a Trust No One System; majority makes the rules, and as it becomes more diverse catastrophic failure of the entire system should become less and less likely.

Artificially limited supply

Bitcoin generation will slow...



... over the next 50 years

Monday, June 20, 2011

Block reward cut in half every 4 years, to artificially limit supply.
Designed to be like extracting a natural resource.
Divisible to 8 decimal places, so ultimate supply is 2.1 quadrillion of smallest possible unit.

What is a transaction?

- Payment to one or more addresses
- Block reward transactions create bitcoins (no previous transactions)
- Other transactions spend payments received from previous transactions
- Payment flow forms directed graph that anybody can verify using the block chain

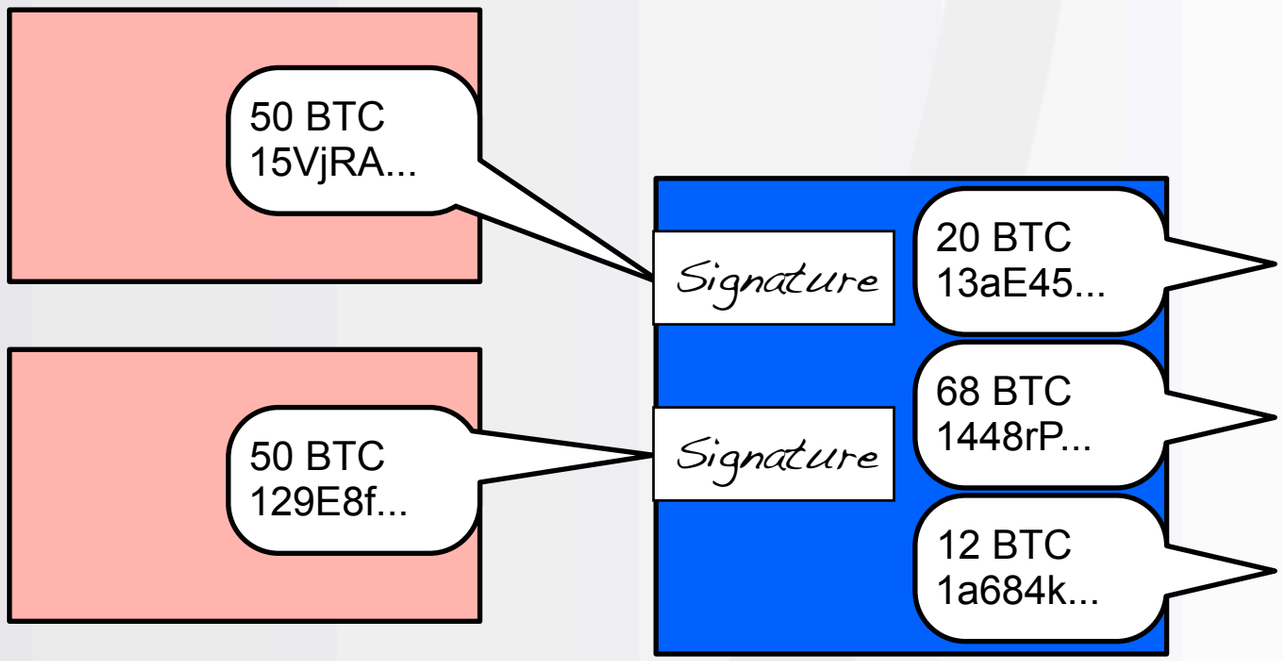
Monday, June 20, 2011

Under the covers, there are no bitcoins. There are only transactions, which are payments to one or more bitcoin addresses, from zero or more previous transactions.

Transactions for a directed graph, always starting at generation transactions (the first transaction in every block, which rewards the miner for finding the block).

Average transaction size is about 300 bytes-- very small.

Transaction example



- 100 BTC transaction
- 2 inputs, 3 outputs

Monday, June 20, 2011

Here's a 2-input, 3-output transaction. Two create-50-BTC transactions are combined, with payments going to three different bitcoin addresses -- 20 BTC to one address, 68 to another, and the other 12 to a third.

Input transactions are always completely spent, so usually a transaction includes a "change" output with any leftover coins.

Addresses : Public Keys

- Payments go TO a public key...
- ... FROM a private key
- Security depends on private key

Monday, June 20, 2011

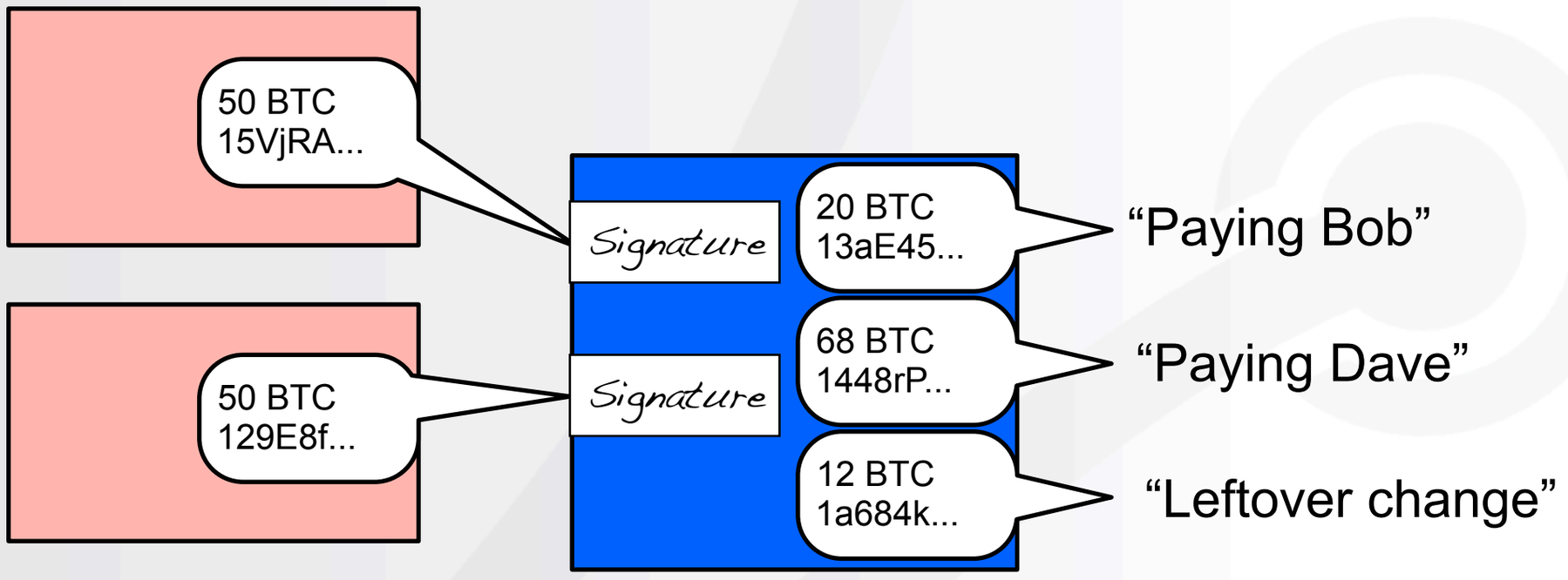
Besides hashing to try to find blocks, bitcoin software spends most of its checking 256-bit Elliptic Curve Digital Signatures (ECDSA) to make sure transactions are valid...

...security depends on private key AND secure communication of payee's public key (otherwise MITM could replace...)

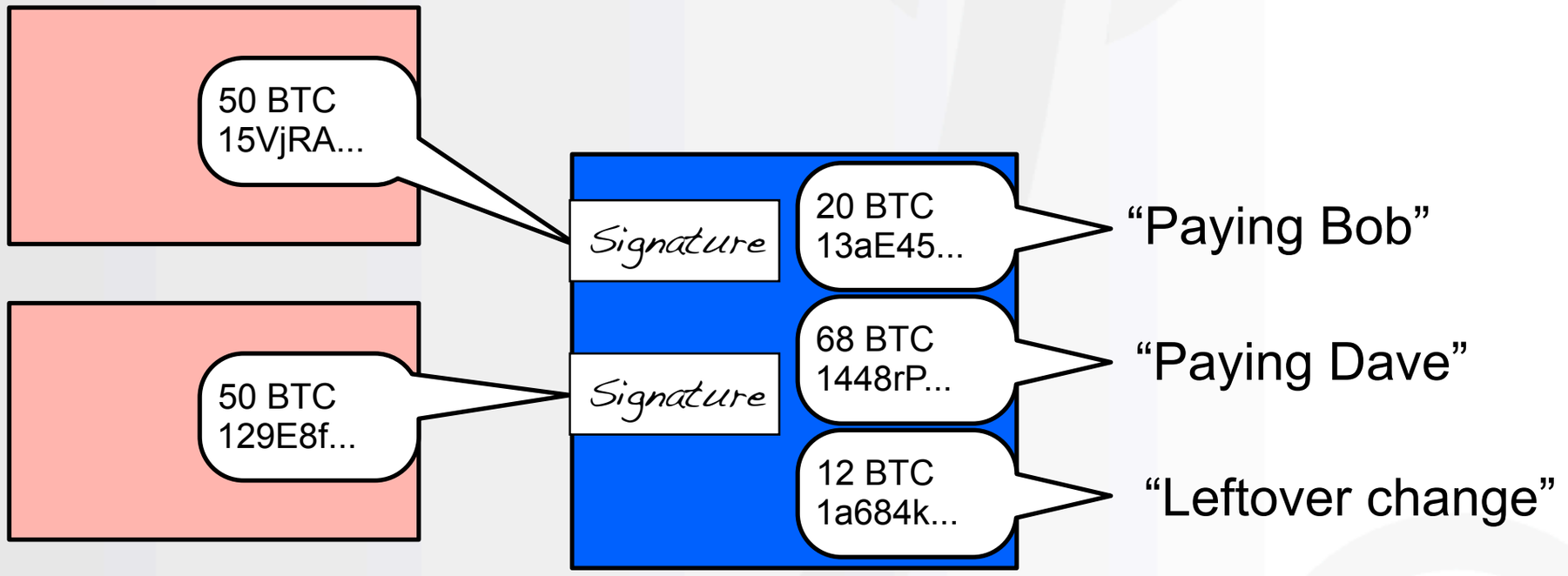
Compare to credit card transactions: I have to trust the merchant with my card or number. I have to trust the credit card company with my personal info.
Or bank account: I have to trust bank will keep my $$$ safe (or that FDIC insurance will be there when I need it). Aside: I DO trust my bank and the FDIC, but not everybody does.

Implications for Privacy

- Entire transaction graph is **public**
- But ownership of keys is private...
- ... until you trade with somebody and reveal one or more of your public keys.



Who knows what?



- I know: one of Bob’s and one of Dave’s public keys
- Bob and Dave know two of my public keys (15VjRA... and 129E8f...)

Monday, June 20, 2011

Here’s the sample transaction again, this time labelled with information that the sender and receivers know. I’m paying Bob 20 bitcoins, Dave 68, and I get 12 bitcoins back in my wallet as change. I know one of Bob’s and one of Dave’s public keys (but they will each have lots of different public keys).
Bob and Dave each know two of my public keys (the previous transation’s outputs).
I can know when Bob spends the coins I sent him by watching for a transaction involving his public key. I might even be able to tell WHAT he is spending them on, if he sends them to a well-known address (like a charity’s donation address).

Transaction graph analysis

- Trades leak information

- Shared (online) wallet services:
  Privacy+ : keys are mixed
  Privacy- : vulnerable to subpoena

Monday, June 20, 2011

Information is leaked as transactions are made. I might be able to tell that Bob is paying Dave, since I know a little bit about the public keys in their wallets.

Using a shared online wallet service can be both good and bad for privacy. It might be good, because you are sharing coins with lots of other users. However, if the shared wallet service is hacked or served with a subpoena, it likely contains a huge amount of information on your transactions.

Future Transactions

- Now:
  `pay public_key amount`
- Future:
  `pay any_of(public_keys) amount`

Monday, June 20, 2011

Bitcoin transactions today are simple-- “pay that public_key this amount of bitcoins.” But in the future, more complex transactions are possible; for example, transactions that can pay any one of several people, or that can only be spent if 3 of 5 people sign the transaction with their private keys. The transaction validation system in bitcoin is designed to be very flexible, although we don’t expose that flexibility and are very conservative with the types of transactions that are allowed on the network today. But I expect that in the future more flexible transactions will be fully supported, and we’ll see transactions that contain extra data and complex multi-party transactions using the same basic infrastructure that we’re using today.

Privacy and the Network

- Bitcoin traffic: unencrypted
  - Transactions are public
  - Security depends on private keys
- Eavesdropping at ISP:
  - send-payment transactions
  - “I found a block” announcements
- Ultra-nerds: bitcoin + TOR proxy

Monday, June 20, 2011

Bitcoin network traffic is unencrypted. Encryption isn’t necessary, because it is a public network that anybody can join and all transactions are public-- there is nothing to hide. Security depends entirely on the strength of the 256-bit ECDSA algorithm and on keeping your private keys safe.

State of the Project

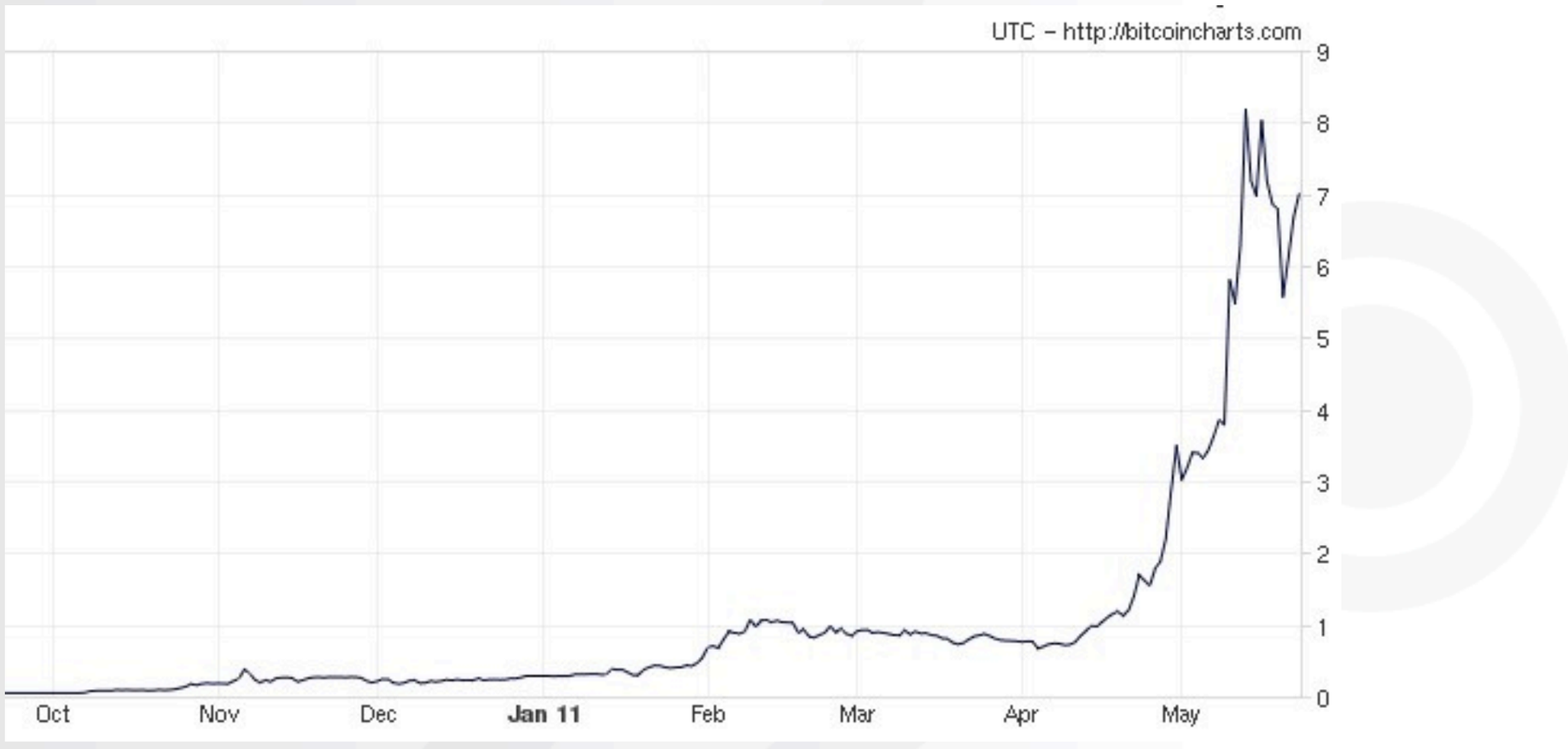
Monday, June 20, 2011

Two words: growing pains
Good problems to have: huge influx of users, lots of press coverage.
System is, so far, handling the extra transaction/user load very well. Issues we've run into: bootstrapping mechanisms (how do new nodes find each other initially).
Transaction fees to prevent "transaction spam" -- sudden price rise not dealt with well at all.

Stats: 20-30,000 connected nodes in the network. Total CPU power dedicated to finding bitcoin blocks: 81 PetaFLOPS/second (world's fastest supercomputer: 2.6 petaFLOPS)

$0 to $40 million so far...

Bitcoin value February 2010: Zero
Value May 2011: $7



Monday, June 20, 2011

WRONG: about $130 million (bitcoins selling at $20 each)
Over $1 million in bitcoin transactions cross the payment network each day; trading inside the exchanges is several times that (so lots of speculation/trading).

At least 16 currency exchanges (this chart from the largest: Mt. Gox)
Exchange bitcoins for dollars, euros, pounds, yen -- even the Second Life virtual world's Linden Dollars.

Physical Bitcoins

Image credit: http://bitbills.com/

Monday, June 20, 2011

Rapid innovation and change.

Bitcoin innovation #2: bitbills. Bitcoins you can hold.

The folks at bitbills.com generate a keypair and print out the public and private keys; private key is hidden inside the card. They then send N bitcoins to that public key, and pinkie-swear-promise that they destroy the electronic copy.

They're meant to be traded like cash, but if you want you can cut the card apart, reveal the private key, scan it in with any device that can read QR codes, and spend them online.

Challenges

- Organization
- Technical challenges scaling up
- Price stability scaling up
- Legal uncertainty
- Criminals and security

Monday, June 20, 2011

Bitcoin has come a long way in 2-and-a-half years, but still, hopefully, has a long way to go. I predict stormy seas ahead, because there are a lot of serious challenges.

First, there is an organizational challenge. Right now, there is no official bitcoin organization; there is just a loose affiliation of volunteers who are interested in the project either because the technology appeals to them or the idea of a non-governmental international currency for the Internet appeals to them or because they think they might make a lot of money using bitcoin. As multiple implementations of bitcoin appear, there might need to be a more formal organizational structure to work out interoperability problems.

There will certainly be technical challenges as transaction volume grows, although I am least worried about those issues-- they have been solved before, and if the bitcoin network scales up to handling thousands of transactions per second there will be plenty of money to pay engineers to solve those issues.

Price stability is a huge problem for merchants right now...

Will the Bitcoin Experiment Succeed?

Monday, June 20, 2011

Bitcoin is getting a lot of hype right now, both positive and negative, and it is easy to forget that it is really still an experiment. There has been nothing like it before, so nobody knows how the experiment will turn out.
Maybe the world doesn't need or won't want a decentralized Internet-based currency. Maybe it will be overrun with criminals and people will lose trust in it. Maybe it will be a niche currency used only by crypto-geeks to buy geeky T-shirts from each other.

Now that it has been demonstrated that a decentralized digital currency is possible, maybe a competitor will arise and IT will take over the world. That would be OK with me; competition is good. We enjoy the highest standard of living in the world because U.S. companies have been freely competing with each other and with countries all over the world for a couple of hundred years. I believe that a currency designed specifically for the Internet could be as important as the Internet itself; I'll find out over the next few years if I'm right or not.