Bitcoin and Cryptocurrencies

Charalampos Papamanthou

University of Maryland

ENEE 459C

What is Bitcoin?

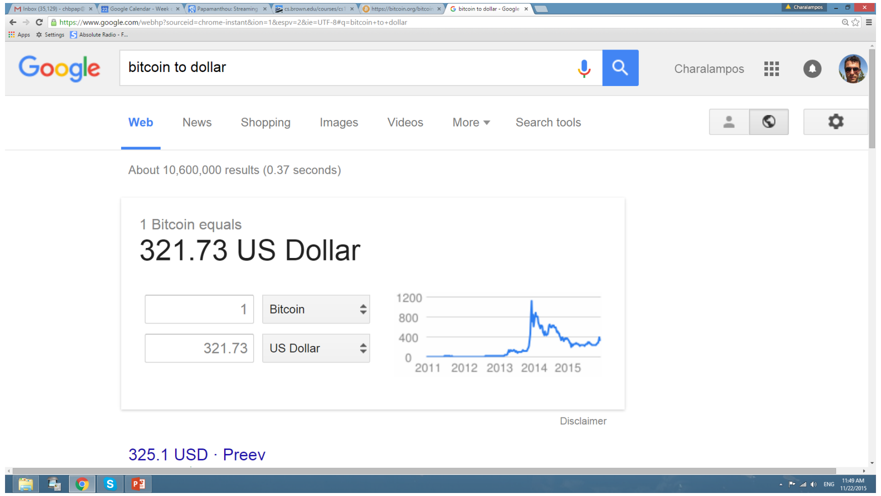
- Bitcoin is a e-cash system enabling as to move from currency (either paper or digital) based and regulated on centralized banks to fully-decentralized currency
- Bitcoin is not the first attempt to digitize cash
    - Lots of work on e-cash in the past (beginning with the work of David Chaum)
    - All e-cash works are using a centralized party to prevent double-spending
- Bitcoin works because it offers the right incentives
    - If you help maintain the correctness of the system, you will earn some Bitcoins
    - "Help" means offering some of your computational power to verify transactions (more on that later)
- Bitcoin was first described in a seminal paper by anonymous Satoshi Nakamoto

Interesting properties of Bitcoin

- Transparent
  - All the transaction made by Bitcoin users are recorded in a public ledger
  - See www.blockchain.info
  - Problem with privacy?
- Finite
  - There is an upper bound on the total amount of bitcoins that will ever be spent (there is no Federal Reserve here that can arbitrarily "print Bitcoins")
  - Simulates the gold standard
- Based on crypto and distributed algorithms
  - Owning money is equivalent to knowing a secret (in particular the secret key of digital signature)
  - Making sure that no double spending occurs is based on novel distributed algorithms (consensus)

Other properties of Bitcoin

- Global
  - Can be used to send money all across the world with very small fees (as opposed to fees charged by major banks)
- Also, you can trade Bitcoins for dollars and vice-versa
  - To buy and sell Bitcoins, go to https://www.coinbase.com/
  - What do you get and when you buy Bitcoins?
- Current price of Bitcoin



https://www.google.com/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=bitcoin+to+dollar

bitcoin to dollar

About 10,600,000 results (0.37 seconds)

1 Bitcoin equals

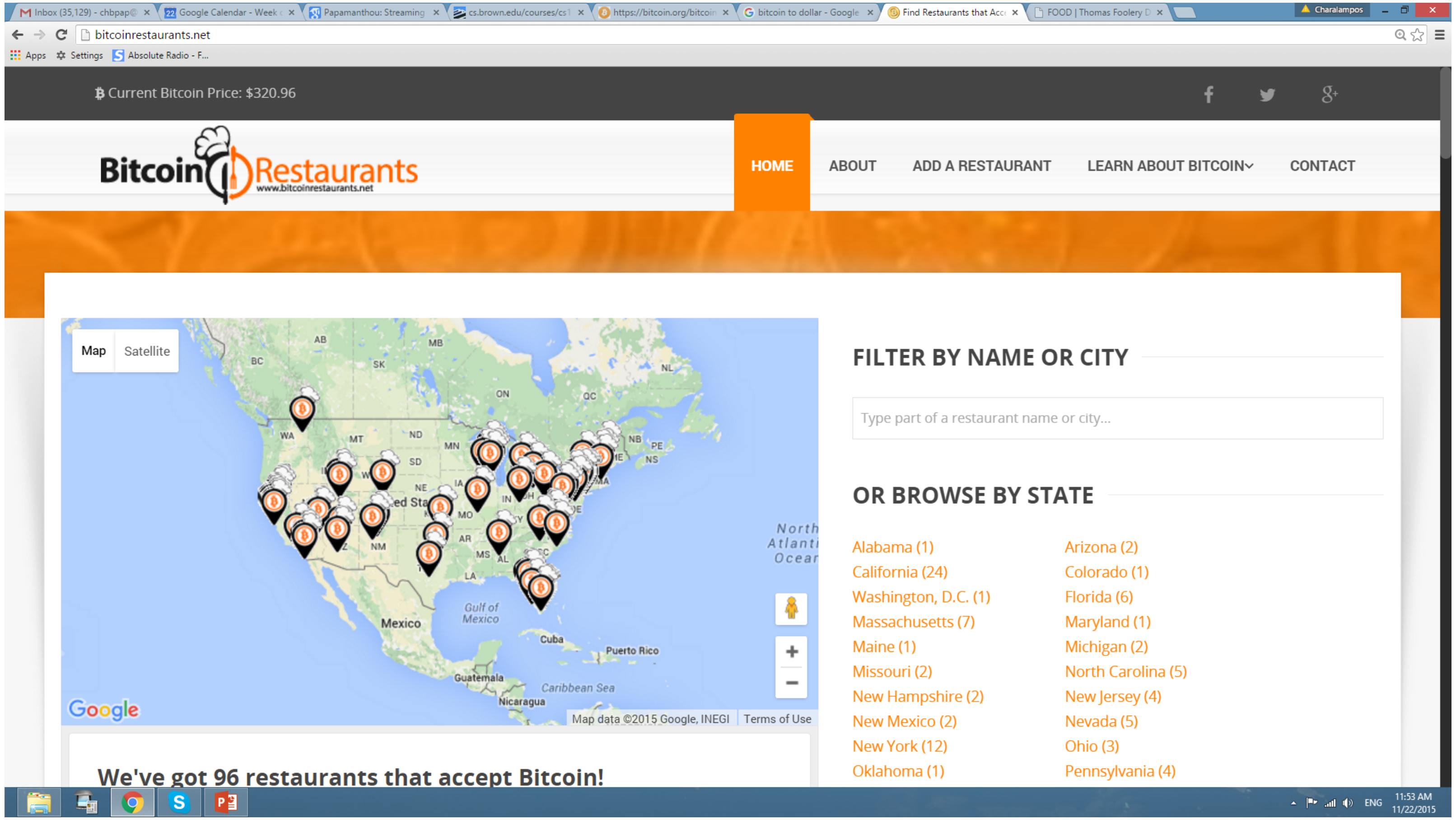
321.73 US Dollar

1	Bitcoin
321.73	US Dollar

Disclaimer

325.1 USD · Preev

Where can I pay with Bitcoin?



bitcoinrestaurants.net

฿ Current Bitcoin Price: $320.96

Bitcoin Restaurants www.bitcoinrestaurants.net

HOME ABOUT ADD A RESTAURANT LEARN ABOUT BITCOIN CONTACT

FILTER BY NAME OR CITY

Type part of a restaurant name or city...

OR BROWSE BY STATE

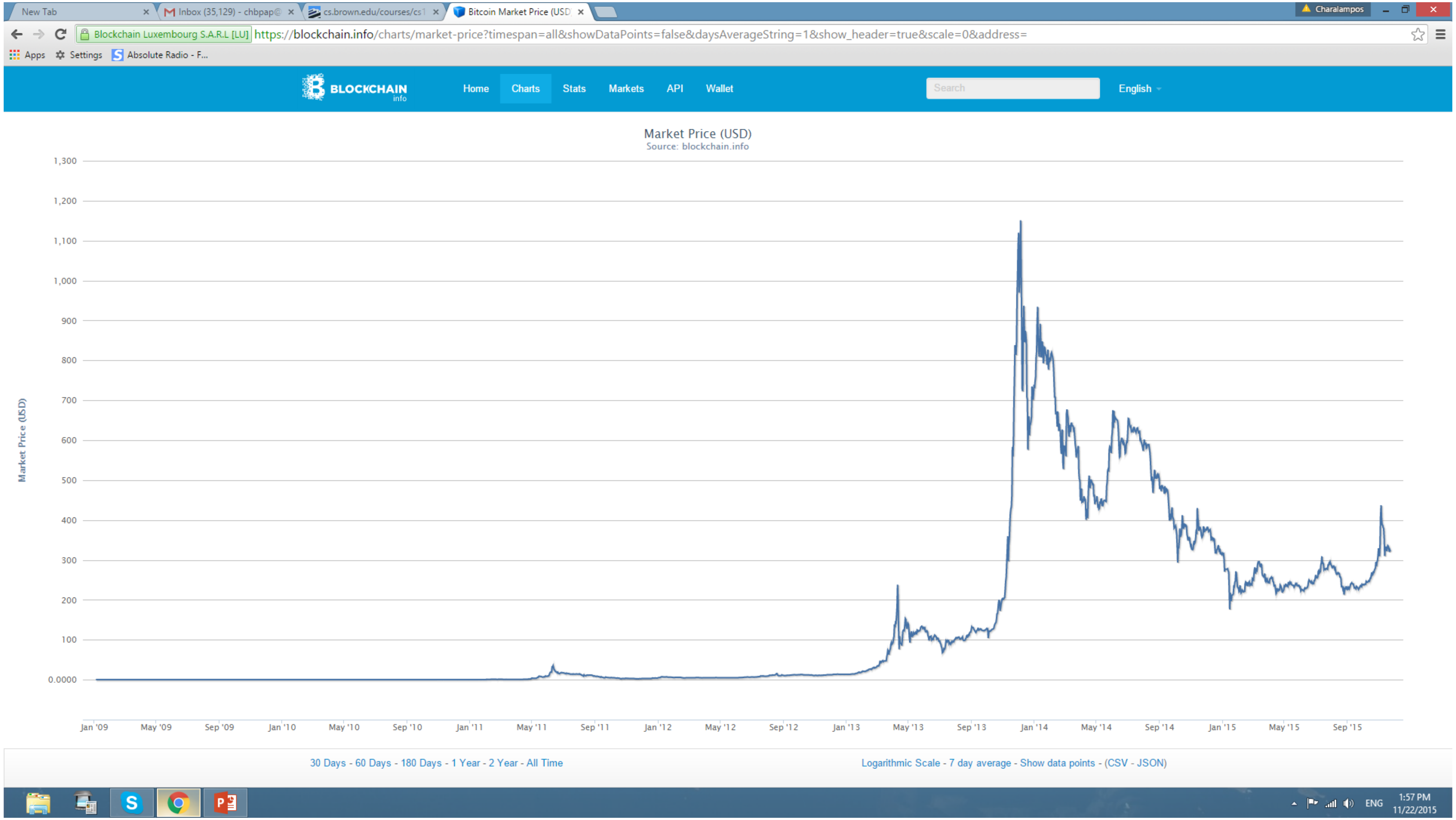
Alabama (1)	Arizona (2)
California (24)	Colorado (1)
Washington, D.C. (1)	Florida (6)
Massachusetts (7)	Maryland (1)
Maine (1)	Michigan (2)
Missouri (2)	North Carolina (5)
New Hampshire (2)	New Jersey (4)
New Mexico (2)	Nevada (5)
New York (12)	Ohio (3)
Oklahoma (1)	Pennsylvania (4)

We've got 96 restaurants that accept Bitcoin!

History of Bitcoin

- 2009: Satoshi Nakamoto’s paper
- 2009-2011:
  - Price less than 1 dollar
  - Community of enthusiasts
- 2013-today
  - Substantial growth
  - In December 2013, price reached 1000 dollars
  - Media coverage
  - Lots of startups facilitating Bitcoin adoption
  - Venture capitalists investment

Bitcoin price



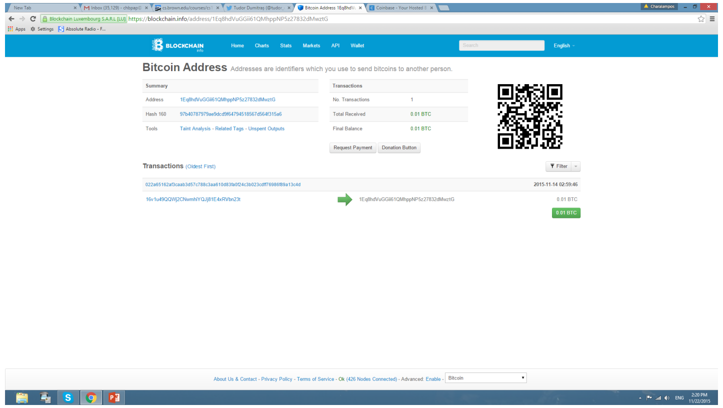
https://blockchain.info/charts/market-price?timespan=all&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&address=

How does it work?

- Main purpose of banks is to maintain balances correctly
- E.g., if I send you 10 dollars, the bank needs to subtract 10 dollars from my account and send 10 dollars to your account
- This is one of the most fundamental bank operations
- **The whole banking system works because we trust the banks to do so correctly**
- Partly for this service, we have to pay all these fees to the banks
- **Bitcoin main idea**
  - Do away with banks completely and maintain this file of balances in a distributed fashion
- But how do you pump money into this new economy?
  - **Pay people in Bitcoins to help maintain this file of balances, called "ledger"**

Bitcoin addresses

- Bitcoin addresses serve as the “account number” in your bank
- Every individual can have as many Bitcoin addresses as he wants
  - Very easy to create
  - No fees at all for having one
- My Bitcoin address
  - 1Eq8hdVuGGii61QMhppNP5z27832dMwztG
  - It now has 0.01 BTC associated with it
  - Let’s verify that



https://blockchain.info/address/1Eq8hdVuGGii61QMhppNP5z27832dMwztG

Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary	
Address	1Eq8hdVuGGii61QMhppNP5z27832dMwztG
Hash 160	97b40787979ae9dcd9f64794518567d564f315a6
Tools	Taint Analysis - Related Tags - Unspent Outputs

Transactions	
No. Transactions	1
Total Received	0.01 BTC
Final Balance	0.01 BTC

Transactions (Oldest First)

022a65162af3caab3d57c788c3aa610d83fa0f24c3b023cdff76986f89a13c4d 2015-11-14 02:59:46

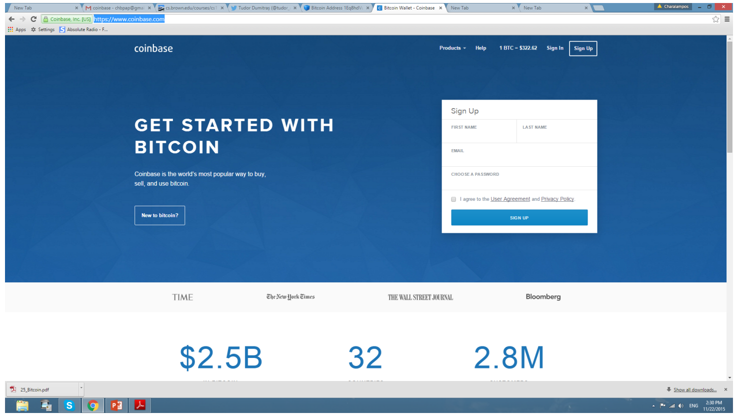
16v1u49QQWj2CNwmhiYQJj81E4xRVbn23t → 1Eq8hdVuGGii61QMhppNP5z27832dMwztG 0.01 BTC

0.01 BTC

About Us & Contact - Privacy Policy - Terms of Service - Ok (426 Nodes Connected) - Advanced: Enable - Bitcoin

What is this Bitcoin address?

- If you want to get into Bitcoin
  - You need to generate a (SK, PK) pair
- Of course, keep your SK secret
- The bitcoin address is an encoding of a hash of PK
  - bitcoin_address = enc(hash(PK))
- Make your PK available to everybody so that you can receive payments
- Downloading and installing coinbase app will take care of all these so that you are ready to send and accept Bitcoin payments



https://www.coinbase.com

GET STARTED WITH BITCOIN

Coinbase is the world's most popular way to buy, sell, and use bitcoin.

Sign Up

FIRST NAME

LAST NAME

EMAIL

CHOOSE A PASSWORD

□ I agree to the User Agreement and Privacy Policy.

1 BTC = $322.62

$2.5B

32

2.8M

A simple transaction

- Alice wants to pay 3 Bitcoins to Bob
- Alice owns 3 Bitcoins at address A
- Bob has address B
- To pay Bob, Alice creates a transaction and broadcasts it to the whole network
- The transaction contains
    - Addresses A and B
    - The public key associated with A
    - Amount 3 Bitcoins
    - A **digital signature** on the message of all the above, created with Alice’s secret key

Blockchain

- There are certain nodes on the network called **miners** that maintain the correct ledger of transactions
- Miners put transactions into blocks, and broadcast their blocks containing transactions that are consistent
    - E.g., a valid block cannot contain the following two transactions
    - A sent x Bitcoins to B (say B had 0 Bitcoins before)
    - B sent 2x Bitcoins to B
- Once a claimed correct block is broadcast, it needs to be verified by other miners before it gets added into the Blockchain
- Eventually, all miners will get to see the same blockchain
- This is the blockchain we see at blockchain.info
- On average, a new block is created every 10 minutes

How do miners reach consensus?

- Distributed computing consensus
- N players having inputs Boolean values x_1,x_2,…,x_N. They begin with some correct state **state**
- There is a well-defined function f(x_i,**state**) = **state’** deciding whether x_i can be added to the state or not
- Variable **state** contains only inputs that are true
- How can I compute a new state **state’**?
  - Easy! Send all x_i’s to a trusted bank! Then it can easily compute the function
  - We want distributed! Send all x_i’s to a player, and ask him to compute
  - Does not work: Some of them can be malicious, computing a wrong function (and you do not know this ahead of time)
- Goal: Maintain the correct state in the distributed system (i.e., if someone asks the system what its state is, he can get a reliable answer containing only true x_i’s)

Distributed algorithm to reach consensus

- All players store the initial **state** and their input x_i
- Pick a player j **uniformly at random**
- The player broadcasts its input x_j
- All players update their local **state** using **state'**=f(**state**,x_j)
- Theorem (informal): If you keep querying the system (namely, ask for every player to output their local state), you will be eventually be able to decide some correct new state **state'≠ state** of the system iff majority of players is honest.
- Honest means:
  - My x_i is true
  - I run the f algorithm correctly
- Why picking uniformly at random is important? (If I always pick the bad guys, the system will never move on to a new state **state'** (the good guys will always reject bad inputs!) and we will be stuck with the old **state**

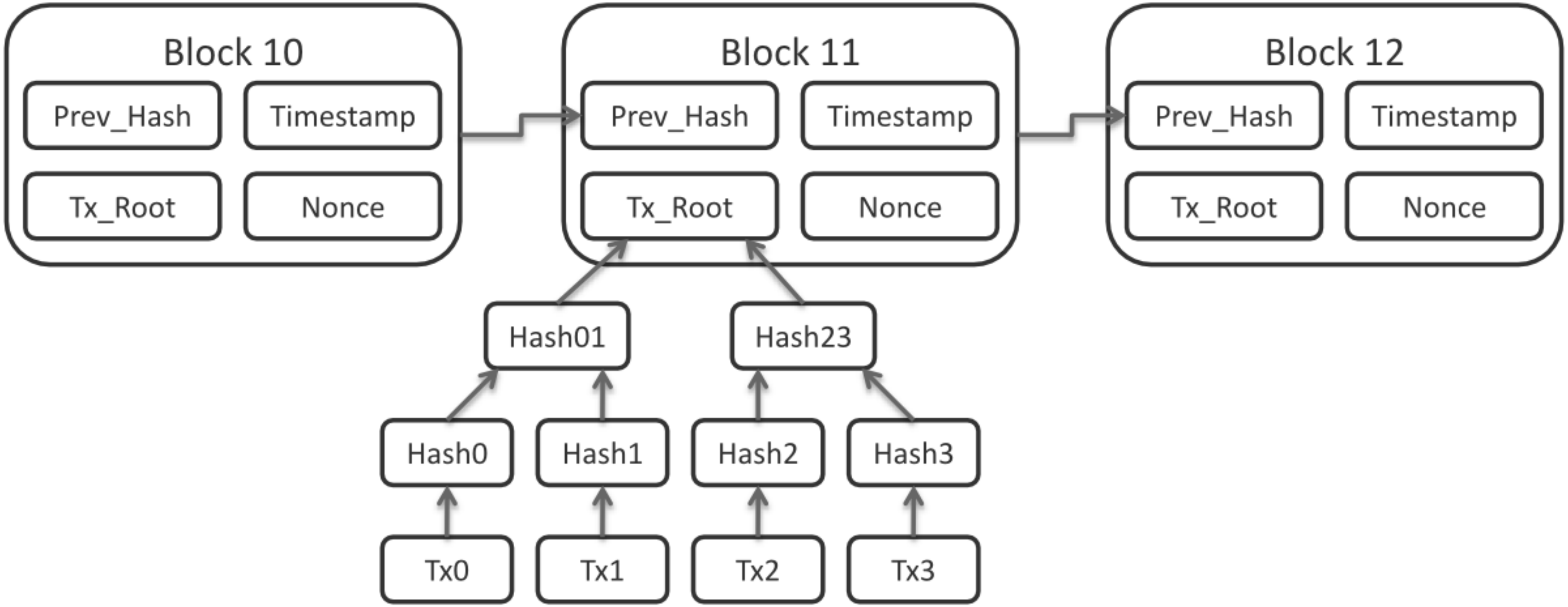
Bitcoin consensus

- It is an instantiation of what we described before
    - Players are miners
    - **state** is the blockchain, containing blocks that contain valid transactions
- So what is the difference?
- Remember an important requirement of the consensus protocol is that every time I should pick **someone uniformly at random**.
    - How do I pick someone uniformly at random in Bitcoin?
    - In particular, how do I pick someone uniformly at random in a distributed fashion?
    - Proofs of Work!!!

How does a miner prepare a block

- A miner receives a bunch of transactions from users
- He checks to see that the transactions he has are valid
- He organizes the transactions into a **block** b
- Now he is ready to broadcast his block and update the state of the system
- Wait, the theorem says he needs to be chosen at random
- Well, to be eligible for broadcasting, he needs to solve a computational puzzle and submit its solution
- Basically, the computational puzzle requires him to invert a hash

Bitcoin Blocks and Transactions



What is the nonce in each block?

- Each block submitted by a miner has a nonce
- This nonce is the solution to the following puzzle
  - H(nonce||previous_block_hash||hash_current_transactions) < target_value
- The block will be accepted after the above is checked
- The smaller target_value is, the higher the difficulty
- The above mechanism serves for choosing some miner at random, making sure the ledger is maintained correct
- The smaller target_value is, the higher the difficulty of the puzzle
- Adjusted by the Bitcoin foundation to make sure one block is mined approximately every 10 minutes
- Questions
  - Why would you invest your computational power to prepare blocks?
  - What are the incentives?

Incentives for miners

- Miners help maintaining the correct ledger, but there is an incentive
  - Every time the mine a block successfully, they collect transaction fees from the transactions they mine
  - E.g., I might have a transaction saying with Inputs address A and 20 bitcoins and outputs address B and 19 bitcoins
  - 1 bitcoin will be the transaction fee for the miner
- You are not required to add transaction fees in your transactions
- But if you do, you are more likely to have your transaction verified
- Is this the only revenue for miners?

How do you put money into the system?

- For every block mined, there is a special transaction called coinbase
- This transaction “creates” money
- E.g., creating a successful block can reward you ~35 Bitcoins
- That is around $9,000 USD
- Concerning the Coinbase transaction
  - Starts at 50 BTC
  - Halves every 210,000 blocks (around 4 years)
  - When it would go to 0, it would not be possible to mine Bitcoins and around that time almost 21 million Bitcoins will have been produces
  - THIS IS HARDCODED INTO THE BITCOIN SOURCE

Forking on the Blockchain

- It might be the case that two nodes get to mine a different block around the same time
- So two nodes can get solutions of different puzzles at the same time
- So the blockchain can degenerate into a tree
  - Two miners can store different paths of this tree
- Bitcoin consensus algorithm ensures the longest blockchain will prevail
- The longest chain will always win (it contains the most cumulative hash power)

Recap

- How do you join Bitcoin?
- What happens when you want to send 4 Bitcoins to Alice?
- How is the ledger maintained?
- What is the purpose of the miners?
- How do the miners get paid?
- What happens when two different blocks are mined around the same time?
- Why does Bitcoin is similar to the way people used to do business in the past (i.e., using gold)

Bitcoin and privacy

- Is Bitcoin private?
- Not really. It provides pseudonimity, since no real names appear on the blockchain
- But you can launch linking attacks by analyzing the transaction graph
- Proposed alternatives
  - Zerocoin, Zerocash
  - These are new cryptocurrencies with privacy
- Intuitive difference between Bitcoin and Zerocash
  - A miner in Bitcoin proves that a sender A has the money to pay a sender B
  - A miner in Zerocash proves that there is an input transaction from the past that can be sent to B (breaks linkage)
- Complicated crypto construction called SNARKs are required

Building applications with Bitcoin

- Implementing a commitment over Bitcoin
- I claim I know the solution x to a problem b but I do not want to reveal it to you; I commit to c(x) and I send c=c(x) to you
- You solve the problem
- Then I reveal x to you. How do you know I knew x back then. You check if c(x) = c and that x is a correct solution (I could not have found a different input)
- But if I lied to you, I could just run away and never reveal x to you
- So I would have betrayed you

Implement timed commitment with bitcoin

- Initially, the party A that knows the secret x, posts a transaction containing c(x) and carrying a large amount of money.
- The body of the transaction is more complicated
  - Informally, it says that if the party does not post another transaction within time t revealing the correct x, then all deposit goes to the other party, otherwise he gets the money back
- So the party knowing x must reveal it otherwise he looses the whole deposit!
- In general, Bitcoin has a scripting language allowing you to specify more complicated conditions for a transaction to be verified

One step further: Smart contracts

- Bitcoin scripting language is not Turing-complete
- How about if more complicated conditions should be responsible for the flow of cash in the system?
- E.g.,
  - Play rock-paper-scissors on Bitcoin and make sure money goes to the winner, without having a trusted third party overseeing the process
- Smart contracts: You can write programs in a Turing-complete language and have miners verify transactions by executing these contracts
- Example: Ethereum
- Research: Privacy-preserving smart contracts (talk to me if you are interested)