FAMU-FSU
College of Engineering

NDCoin

A Cryptocurrency-Based Distributed Computing Market

ECE Graduate Seminar
Tuesday, September 9th, 2014

Dr. Michael Frank
Associate in Engineering
FAMU-FSU College of Engineering

v1.1

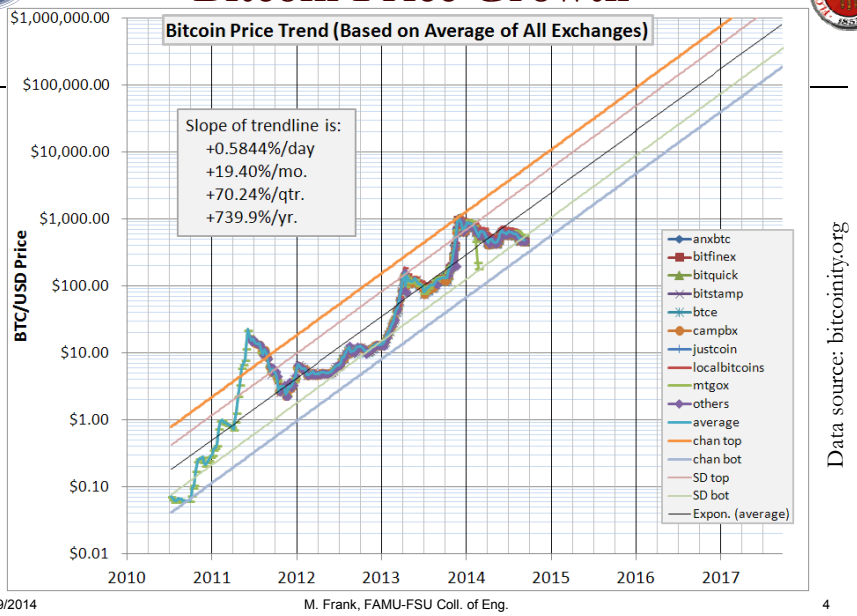
Outline of Talk

- Bitcoin's blockchain tech. → a general approach for solving the Byzantine Agreement problem
  - Can use it to achieve distributed consensus in any database application!
- Use in distributed high-performance computing
  - Enable rapid growth with low barriers-to-entry
- Outline of NDCoin protocol
  - Basic features & structure
- Generalization to general-purpose computations
  - A target for future development effort

What is Bitcoin?

- The world's first decentralized digital cash system!
  - Introduced in 2009 by "Satoshi Nakamoto"
  - Now worth over $6 billion (market cap.)
  - Could become a major world currency?
- For more details, please refer back to the talk that I gave in this seminar series last January:
  - http://www.eng.fsu.edu/~mpf/bitcoin-talk.pdf

Bitcoin Price Growth



Data source: bitcoinity.org

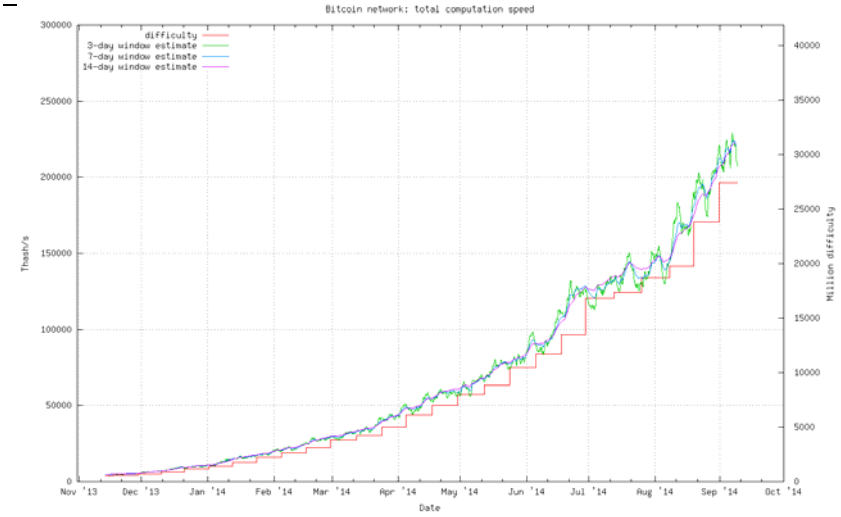
"Byzantine Generals" problem

- Generals must coordinate armies for attack
- Messages may be intercepted/forged
- Some generals could be turncoats!

Bitcoin's Solution for Byzantine Agreement

- Needed to establish consensus re: order of transactions
  - Prevents double-spending / negative balances
- Bitcoin's solution:
  - Nodes race to commit sets of transactions to the public ledger ("blockchain") by solving a difficult mathematical problem ("proof of work")
  - Computational power → decision-making authority
    - Advantage: Can't be faked; takes real resources
- **Note:** The *same* technique could be used to register transaction commits in *any database application*.
  - Can do any information-processing task whatsoever!
  - No need for centralized control → "incorruptible"

Bitcoin Network – Aggregate Speed And Mining Difficulty – Last 10 mo.



One Interesting Application: A Market for Distributed Computing

- Problem:
  - Underutilized computing resources
  - Users w. sporadic need for massive processing
- Cloud computing systems exist (*e.g.* EC2),
  - But existing services are expensive & limited in capacity
  - And you have to trust a central provider (e.g. Amazon)
- Idea:
  - Build a distributed computing marketplace to harness underutilized machines;
  - Use a cryptocurrency for fraud-proof settlement
    - very low barriers-to-entry → rapid network growth

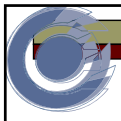
http://www.cise.ufl.edu/research/ocean

The O.C.E.A.N. Project

- A major research project that I ran in the University of Florida's dept. of Computer & Information Science & Engineering from 2000-2004. (~8 faculty; ~14 students)
  - Open Computation Exchange & Auction Network
  - Goal: Create a distributed computing market
  - Pre-Bitcoin, so was missing the cryptocurrency-based payment system
    - Thus, project fizzled out… Time to resurrect?

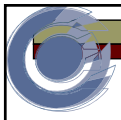
NDCoin – A Step on the Road to a Cryptocurrency-Based OCEAN

- Focus: *nondeterministic* computational tasks
  - Involves brute-force search for a solution
  - Solutions, once found, are relatively easy to verify
    - No question about whether problem was solved
- I outlined a simple cryptocoin-based protocol for this in Feb. 2014 (http://ta.gd/NDcoin)
  - Fraud-proof; no trust in participants required



Examples of Nondeterministic Computations

- Many classically difficult (NP-hard, NP-complete) computational problems:
  - Various problems in search / optimization / planning / scheduling / *etc.*
  - http://en.wikipedia.org/wiki/List_of_NP-complete_problems
- Many practical problems of significance:
  - Protein folding, genetic analysis, data mining, automated diagnostic systems, process control, engineering design optimization, *etc.*



Basic Outline of NDCoin Operation

- Clients post job requests including program code in a nondeterministic, Turing-complete language
  - And a "bounty" which is set aside until deadline
- Nodes that find solutions post fingerprints (hashes) of the solutions to the blockchain
  - Stakes a claim to the bounty
- After solution fingerprint is committed, solver posts the actual solution
  - Client can optionally verify that solution is accepted
- If solution(s) is/are accepted or verified correct before deadline, bounty transfers to the solver(s);
  - No valid solutions → bounty reverts to client

Fields of Solve-Request Transaction

#	Description
1.	Maximum length of witness bit-strings for this problem instance
2.	Virtual machine code for nondeterministic algorithm for this problem class
3.	Maximum limit on number of operations allowed in verifying solution candidates
4.	Maximum limit on memory allocation allowed in verifying solution candidates
5.	Transaction fee amount (to be split between miner & coin smelting pool)
6.	Number *N* of distinct solutions for which bounty will be payable.
7.	Bounty amount per solution.
8.	Deadline date/time or block number.
9.	Public key of client account from which bounty is to be posted & fees paid.
10.	Digital signature of transaction (signed by above key).

Fields of Solution-Claim Transaction

#	Description
1.	Fingerprint (cryptographic hash) of: <reference to solve-request transaction, plus solution witness string, plus public address of solver's account to receive the bounty payment, plus random data padding to a minimum length>
2.	Transaction fee amount (to be split between miner & coin smelting pool)
3.	Public key of solver's account from which transaction fees are to be paid.
4.	Digital signature of transaction (signed by solver's fee-payment account)

Fields of Solution-Reveal Transaction

#	Description
1.	Reference to the solution-claim transaction to be validated.
2.	Reference to the original solve-request transaction for the problem being solved.
3.	Actual solution witness string.
4.	Public address of solver's account to receive the bounty payment.
5.	Random pad data.
6.	Transaction fee amount (to be split between miner & coin smelting pool).
7.	Public key of solver's account from which transaction fees are to be paid.
8.	Digital signature of transaction (signed by solver's fee-payment account).

Fields of Solution-Accept Transaction

#	Description
1.	Reference to the solution-reveal transaction to be accepted.
2.	Transaction fee amount (to be split between miner & coin smelting pool).
3.	Public key of client account from which bounty is to be posted & fees paid.
4.	Digital signature of transaction (signed by above key).

- Funds are released to the solver if a valid solution-accept transaction has been posted, or if a certain time limit has expired and the posted solution is verified.

Potential Weaknesses in Protocol

- Attack Scenario #1 (DOS attack):
  - Client posts wasteful jobs that:
    - Take significant resources to test candidate solutions
    - Have few or no solutions
  - OR: Client fails to accept valid solutions posted
  - Nodes waste resources attempting to solve problem, or independently verifying solutions
- Mitigation strategy:
  - Transaction fee ensures this attack is not free
  - Nodes can refuse to attempt high-resource jobs
  - Nodes can refuse to award payment for high-resource jobs for which no solution is accepted

Taking NDCoin farther…

- What's the next step?
  - We'd prefer our system to work for any general-purpose computations, not just nondeterministic search problems.
- Unfortunately, verifying correctness of results then becomes more difficult.
  - One approach: Use a SNARK (Succinct Non-interactive Argument of Knowledge) to prove that computation was performed correctly
    - Requires some substantial compute-time overheads
  - Alternatively: Rely on client to validate solutions
    - No longer 100% trustless; may need a reputation system

Conclusion

- A secure, scalable, open marketplace for distributed computation (at least of the nondeterministic variety) can be built using known techniques & technologies.
  - Harnesses underutilized computing resources.
- This system has the potential to be extremely fast-growing, due to its low barriers-to-entry.
  - Perhaps, it could quickly (within a few years, like Bitcoin) grow to become the world's largest supercomputer!
- The associated coin (NDC) could become extremely valuable very quickly.
  - Has inherent real value, unlike most cryptocurrencies.
  - Speculators would snap it up…

R PLAN "4" $UCCE$$!!!11!1!

1. Help develop NDCoin proof-of-concept/prototype as a volunteer
2. Get hired to help complete OCEAN development out of ICO seed funding
3. Be an early NDC/OCN miner
4. …?
5. $$ PROFIT $$