Research Opportunities in Cryptoeconomics

Nikos Bentenitis, PhD

Bitcoin Foundation, Mastercoin Foundation, CoinSimple

Bitcoin

Mastercoin

Research

CoinSimple

Bitcoin is *like* other currencies

- It can be divided and combined seamlessly
- It can be traded for national currencies
- It is scarce and useful as a means of exchange

Bitcoin is *unlike* other currencies

- It is scarce: There will never be more than 21 million bitcoins
- It is released over time with declining rate
- It can be subdivided into 100 million (0.00000001 bitcoin)
- It is impossible to be faked
- It has no central issuing authority and it is distributed
- It is based on a computer code that is open, transparent, tested and usable by anybody for any reason
- It provides financial privacy
- It carries no counter-party risk
- It allows complete ownership of money (storage

Bitcoin transactions are

- Secured by cryptography
- Verified using the largest distributed computation cluster in the world
  - The transaction verifiers are called *miners*
  - Miners get paid fees for each transaction they verify
- Transmitted through a distributed peer-to-peer network
- Published in a common ledger, the block chain
- Irreversible
- Have very low fees (about 0.0001 bitcoin)

Bitcoin transactions don’t need

- Banks
- SWIFT, SEPA and other inter-bank funding networks
- PayPal and other payment processors
- Western Union and other remitters

Bitcoin is a technology

- A database (a distributed asset ledger)
- A scripting language

(More on this a bit later)

Common questions

- Does Bitcoin have any value?
- Can you use a lot of money, or computers to “take over” the Bitcoin network?
- What can a government do to control Bitcoin?
  - Take down the central Bitcoin server?
  - Stop bitcoin transfers?
  - Take down the Bitcoin exchanges?
  - Ban its citizens from using Bitcoin?

Mastercoin

What is Mastercoin

- January 6, 2012: “The existing Bitcoin network could be used as a layer on top of which applications could be built” (J. R. Willett)
- Features
  - Distributed exchange
  - Smart property and user tokens
  - Contracts for difference
  - Betting and prediction markets

Mastercoin Funding

- The funding of Mastercoin is achieved its own tokens, Mastercoins (MSC)
- During one month (August 1-31, 2013,) for every bitcoin sent to a certain address
  - 100 MSC were debited to the sender
  - 10 MSC were put aside for development (Dev MSC)
- **4,740 BTC** were raised

Decentralized Applications are

1. Open-source computer programs
2. Autonomous, block chain-based
3. Self-sustaining
4. Consensus-based
5. Monetized with tokens

Growth of Decentralized Applications

1. White paper
2. Initial token distribution
3. Development-token distribution
4. Wider acceptance

Mastercoin is a Decentralized Application

- White paper
- Open-source
- Block chain-based (through Bitcoin)
- With a token: Mastercoin
- Token distribution Kickstarter-style
- Autonomous
- With incentives for stakeholders
- Consensus-based through proof of stake
- Wider acceptance

Bitcoin is a Decentralized Application

- White paper
- Open-source
- Block chain-based
- With a token: bitcoin
- Token distribution through mining
- Autonomous
- With incentives for stakeholders
- Consensus-based through proof of work
- Wider acceptance

Classification of DAs

- Type I: Bitcoin (has its own block chain)
- Type II: Mastercoin (needs Bitcoin for block chain)
- Type III: ComputeCoin (needs Mastercoin for tokens)

Advantages of DAs

- Stakeholders are given incentives
- Legal ground of open-source software
- No corporate "baggage"
- Great interest in the community (BitAngels, ETH)

Challenges

Challenges and Opportunities

- Cryptocurrency technology is currently using 30-year-old cryptography
- There are several problems in all existing cryptocurrency designs
- The discipline of “cryptoeconomics” is only just beginning.

Challenge 1: Scalability

- Bitcoin requires “full nodes” to store all transactions
- With 7 TPS block chain grows 1 MB per hour with 2000 TPS block chain will grow 1 MB per three seconds
- **Challenge**
  - Only large businesses will be able to run full nodes
  - Full nodes conspire to produce blocks giving themselves extra BTC
  - Light nodes have no ability to detect such fraud
- **Solutions**
  1. Empower light nodes via challenge-response protocol
  2. Block chain stored in the cloud on a distributed hash-table (DHT)

Challenge 2: Mining Decentralization

- Mining is no longer done by individuals on CPUs
- **Challenges**
  1. Mining pools that depend on centralized block validation
  2. Specialized hardware (ASICs)
- **Solutions**
  1. Mining algorithm involves interpreting a Turing-complete language (An ASIC in that algorithm is a CPU)
  2. Decentralization-friendly Proof of Work

Challenge 3: Useful Proof of Work

- **Challenge**
  - Mining algorithms use electricity to perform hard but useless computations
- **Solution**
  - Use algorithm that does something useful like finding prime numbers
- **Constraints**
  - Social benefit should not decrease over time
  - PoW functions must be easy to verify
  - Algorithm can be useless but motivate indirectly useful software/hardware research

Challenge 4: Price Stability

- **Challenge**
  - Volatile demand with predetermined supply makes price volatile
- **Solutions**
  1. Measuring price: Increase currency issuance if price goes up
     - Difficulty is related to price but confounded with technological advancement
  2. Measuring demand: Increase currency issuance if currency becomes more popular
     - Number of transactions, number of distinct miners, number of nodes (but beware of malicious actors)

Challenge 5: Proof of Stake

- **Challenge**
    - A distributed consensus algorithm that does not rely on wasting energy
- **Solution**
    - Proof of Stake algorithm
        - If there is a fork, everyone has the incentive to vote on all chains

Challenge 6: Issuance of N Coins per Person

- **Challenge**
  - Can we create a system where each person gets N coins/units for voting, basic income
- **Solutions**
  1. Trusted third party
  2. Human labor-based proof of work (a task that the average human can do competitively)
  3. Community reputation

Challenge 7: Proof of Excellence

- **Challenge**
  - Reward people working on research problems
- **Solutions**
  1. Computationally checked proofs of mathematical theorems
  2. Strategy games that promote artificial intelligence research
  3. Decentralized math challenges

Conclusion

- Cryptocurrency technology is currently using 30-year-old cryptography
- There are several problems in all existing cryptocurrency designs
- The discipline of “cryptoeconomics” is only just beginning.
- There exist “hard” problems in cryptoeconomics that require extensive modeling and research
- Cryptocurrencies may have applications as an economic layer in other cryptographic/computational projects (“folding@home-coin”, “Torokens”, GFS)

coinsimple

Market pain

Merchants want to accept Bitcoin but

- They need help with comparing, selecting and changing payment processors
- They need help with integrating payment processors
- They need more information about the transactions (analytics)
- They need to analyze large numbers of transactions (mega-analytics)

Customers

- Have an online store and wish to accept payments in bitcoins
- Face a complex and changing payment processing industry that is growing fast (BitPay, Coinbase, BIPS) and has new entrants (BitPagos, GoCoin, Circle)
- Do not have the technical skills to compare, select and integrate a payment processor
- Have to integrate the payment processors *separately*
- Do not have the technical skills the manage the information generated

Products and services

1. Bitcoin-to-local currency payment plugins that allow merchants to
    - integrate their favorite payment processor
    - switch from one payment processor to another
    - use them on Wordpress, Drupal and 21 more platforms
2. Software as a Service, SaaS, for merchants that give additional features like
    - big-data customer analytics
    - price optimizations

Team

- Nikos Bentenitis, CEO
- Gabriel Manricks, CTO
- Andreas M Antonopoulos, Advisor
- Jon Myers, Design and Branding
- Eddy Travia, Asia Business Development
- Jeff Root, Business Development

Funding

Incubated by SeedCoin, a virtual incubator for Bitcoin companies

Contact

- nikos@coinsimple.com
- coinsimple.com