Modelling Collective Commons Problems: Future Scenarios for P2P "Money"

David Hales, University of Szeged, Hungary
www.davidhales.com

Diversity in Macro Conf. Feb 24-25th 2014
University of Essex

Who am I?

- Computer scientist
- PhD in agent-based modelling (Essex)
- Artificial societies focus (MAS)
- Moved into P2P
- Coming full circle
- Disclosure: no substantial position in any of systems mentioned or association with them

Summary

- Will distinguish two classes of Peer-to-Peer (P2P) systems that have emerged
- Will focus on new fully decentralised class (such as bitcoin and bittorrent)
- Outline their interesting properties
- Discuss how might be captured in Agent-based models
- State future research challenges / open issues related to Bitcoin and emerging variants

Two classes of P2P

- First wave P2P:
  - Centralised systems architecture
  - Conventional company structure
  - Provides “person-to-person” platform
  - Zopa.com (p2p lending), Napster (file-sharing)
- Second wave P2P:
  - Distributed systems architecture
  - No conventional ownership (open source)
  - Self-organised software provides services
  - Bitcoin (p2p “money”), bittorrent (file-sharing)

2nd wave - P2P Terminology

- Software running on user devices are called *Clients*
- The way the software behaves and communicates is called the *Protocol*
- The dynamic connections clients make between each other forms what is termed an *Overlay Network*
- Clients communicate by passing *messages* over the overlay network

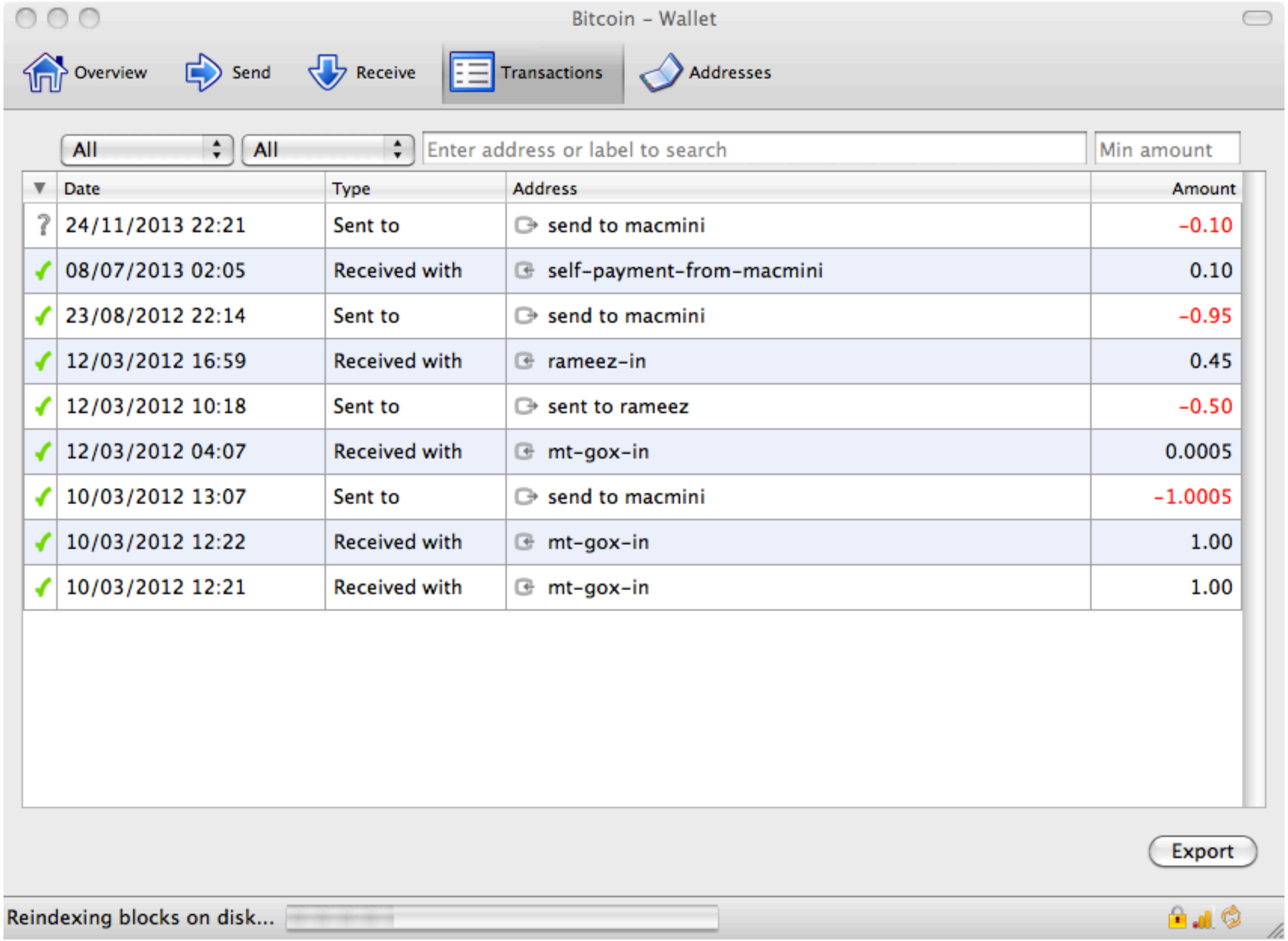
What is Bitcoin?

- Decentralised information system
- Supports distributed public ledger (blockchain)
- Ledger updated in and stored in *all* clients
- Clients will not accept updates that violate the ledger (to stop double spending)
- Ledger stores bitcoin transactions
- Bitcoins are endogenously created (mined) within the system - awarded to those who provide substantial CPU power maintaining the ledger
- Bitcoins are released to a schedule with an upper limit set at 21m by 2140.

What is Bitcoin?

- I am not going to spend time on the technical detail of Bitcoin. See:
  - Satoshi, N. (2009) "Bitcoin: A Peer-to-Peer Electronic Cash System". https://bitcoin.org/bitcoin.pdf.
- Suffice to say it uses public key crypto and an incentive system to provide quite robust distributed ledger services.

Bitcoin client



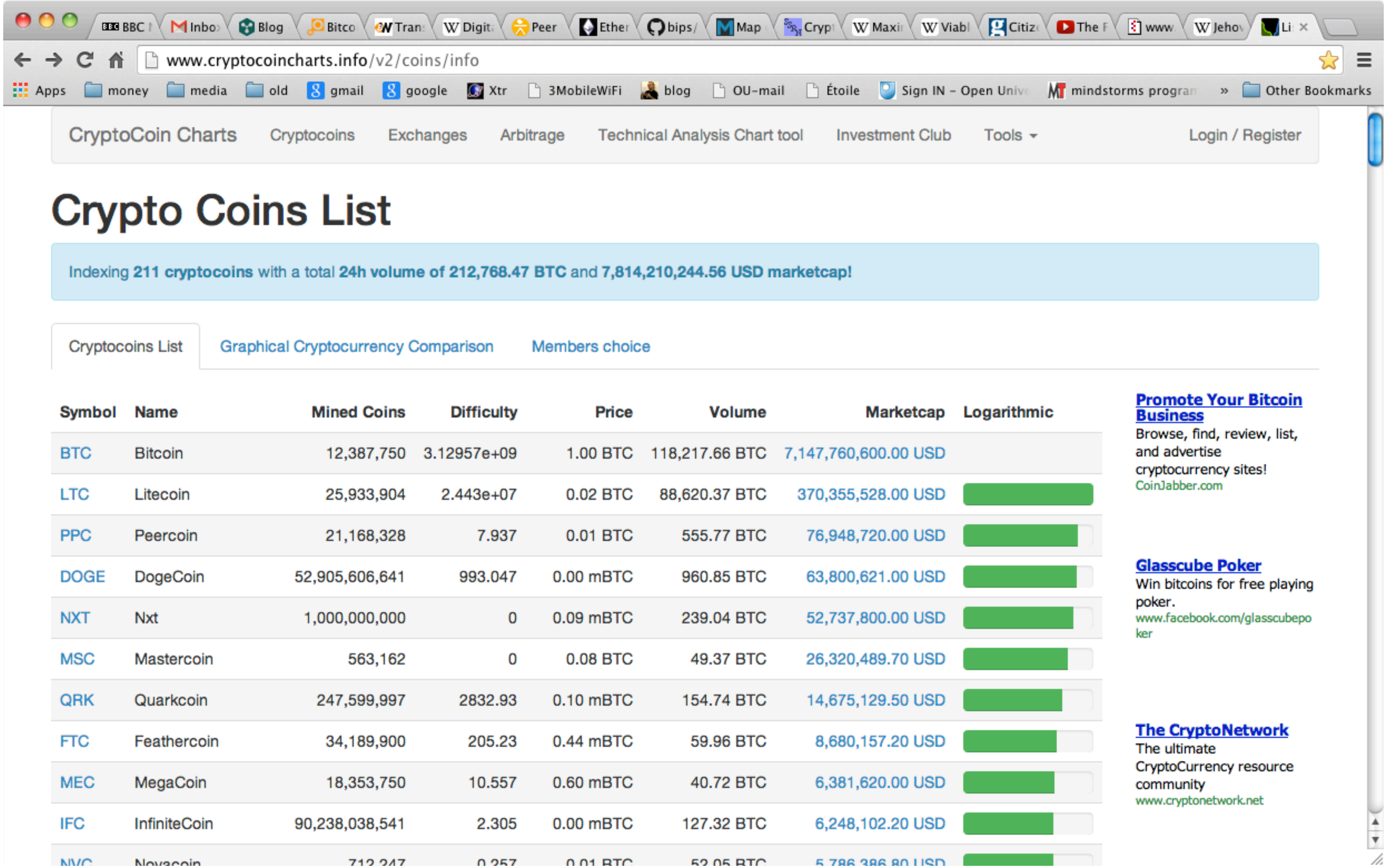
	Date	Type	Address	Amount
?	24/11/2013 22:21	Sent to	send to macmini	-0.10
✓	08/07/2013 02:05	Received with	self-payment-from-macmini	0.10
✓	23/08/2012 22:14	Sent to	send to macmini	-0.95
✓	12/03/2012 16:59	Received with	rameez-in	0.45
✓	12/03/2012 10:18	Sent to	sent to rameez	-0.50
✓	12/03/2012 04:07	Received with	mt-gox-in	0.0005
✓	10/03/2012 13:07	Sent to	send to macmini	-1.0005
✓	10/03/2012 12:22	Received with	mt-gox-in	1.00
✓	10/03/2012 12:21	Received with	mt-gox-in	1.00

Reindexing blocks on disk...

Many Bitcoin variants

- Bitcoin has spawned many variants (altcoins)
- As of Feb 2014 over 100 (but small no. active)
- Each supports subtlety different properties
- Some “pre-mine” coins or place different limits on total number of coins that can be produced.
- Some attempt to allocate coins to national communities
- In general however, they all rely on the distributed ledger concept (the blockchain)

From: www.cryptocoincharts.info



CryptoCoin Charts | Cryptocoins | Exchanges | Arbitrage | Technical Analysis Chart tool | Investment Club | Tools ▾ | Login / Register

Crypto Coins List

Indexing **211 cryptocoins** with a total **24h volume of 212,768.47 BTC** and **7,814,210,244.56 USD marketcap!**

Cryptocoins List | Graphical Cryptocurrency Comparison | Members choice

Symbol	Name	Mined Coins	Difficulty	Price	Volume	Marketcap	Logarithmic
BTC	Bitcoin	12,387,750	3.12957e+09	1.00 BTC	118,217.66 BTC	7,147,760,600.00 USD	
LTC	Litecoin	25,933,904	2.443e+07	0.02 BTC	88,620.37 BTC	370,355,528.00 USD	🟩
PPC	Peercoin	21,168,328	7.937	0.01 BTC	555.77 BTC	76,948,720.00 USD	🟩
DOGE	DogeCoin	52,905,606,641	993.047	0.00 mBTC	960.85 BTC	63,800,621.00 USD	🟩
NXT	Nxt	1,000,000,000	0	0.09 mBTC	239.04 BTC	52,737,800.00 USD	🟩
MSC	Mastercoin	563,162	0	0.08 BTC	49.37 BTC	26,320,489.70 USD	🟩
QRK	Quarkcoin	247,599,997	2832.93	0.10 mBTC	154.74 BTC	14,675,129.50 USD	🟩
FTC	Feathercoin	34,189,900	205.23	0.44 mBTC	59.96 BTC	8,680,157.20 USD	🟩
MEC	MegaCoin	18,353,750	10.557	0.60 mBTC	40.72 BTC	6,381,620.00 USD	🟩
IFC	InfiniteCoin	90,238,038,541	2.305	0.00 mBTC	127.32 BTC	6,248,102.20 USD	🟩
NVC	Novacoin	712,247	0.257	0.01 BTC	53.05 BTC	5,786,386.80 USD	🟩

Promote Your Bitcoin Business
Browse, find, review, list, and advertise cryptocurrency sites!
CoinJabber.com

Glasscube Poker
Win bitcoins for free playing poker.
www.facebook.com/glasscubepoker

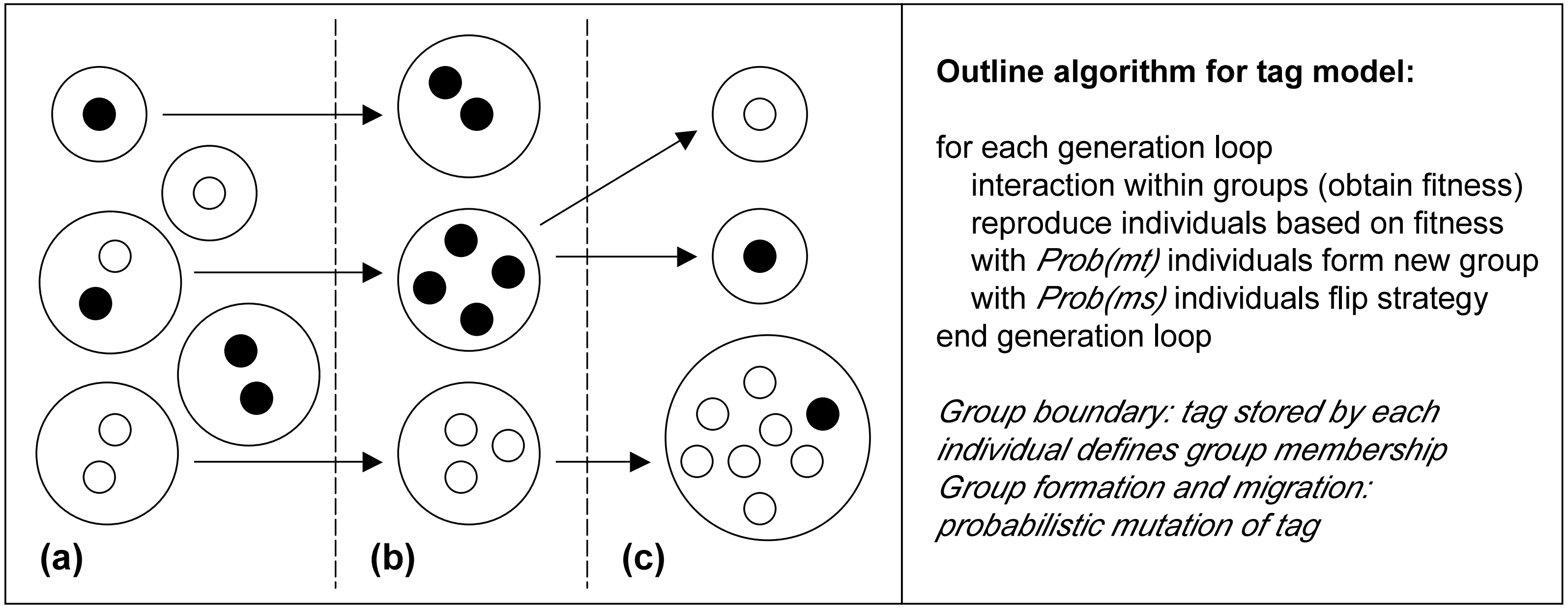
The CryptoNetwork
The ultimate CryptoCurrency resource community
www.cryptonetwork.net

Group selection of variants?

- Could we model this ecology of variants using previously proposed cultural group selection models?
- There are several, summary of some given in:
  - Hales, D., (2010) **Rationality meets the Tribe: Recent Models of Cultural Group Selection**. In Mollona, E., (ed) Computational Analysis of Firms' Organization and Strategic Behaviour. Routledge. http://cfpm.org/~david/papers/tribe-proof-v1.pdf

Tag Models

- Tags may be bit strings signifying some observable cultural cues
- Tags may be a single real number
- Any distinguishing detectable cue
- Most show cooperation / altruism between selfish, greedy (boundedly rational) agents



Outline algorithm for tag model:

```
for each generation loop
    interaction within groups (obtain fitness)
    reproduce individuals based on fitness
    with Prob(mt) individuals form new group
    with Prob(ms) individuals flip strategy
end generation loop
```

Group boundary: tag stored by each individual defines group membership
Group formation and migration: probabilistic mutation of tag

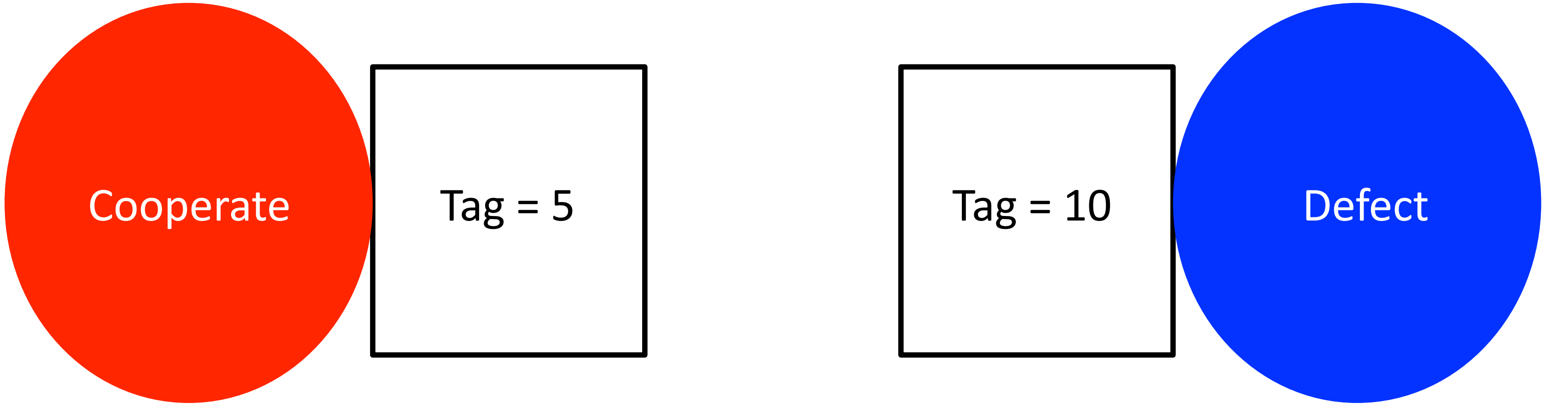
Schematic of the evolution of groups in the tag model.
Three generations (a-c) are shown. White individuals are pro-social, black are selfish. Individuals sharing the same tag are shown clustered and bounded by large circles. Arrows indicate group linage. Migration between groups is not shown. When b is the benefit a pro-social agent can confer on another and c is the cost to that agent then the condition for group selection of pro-social groups is: b > c and mt >> ms

Riolo, Axelrod, Cohen, Holland, Hales, Edmonds…

Simulation algorithm

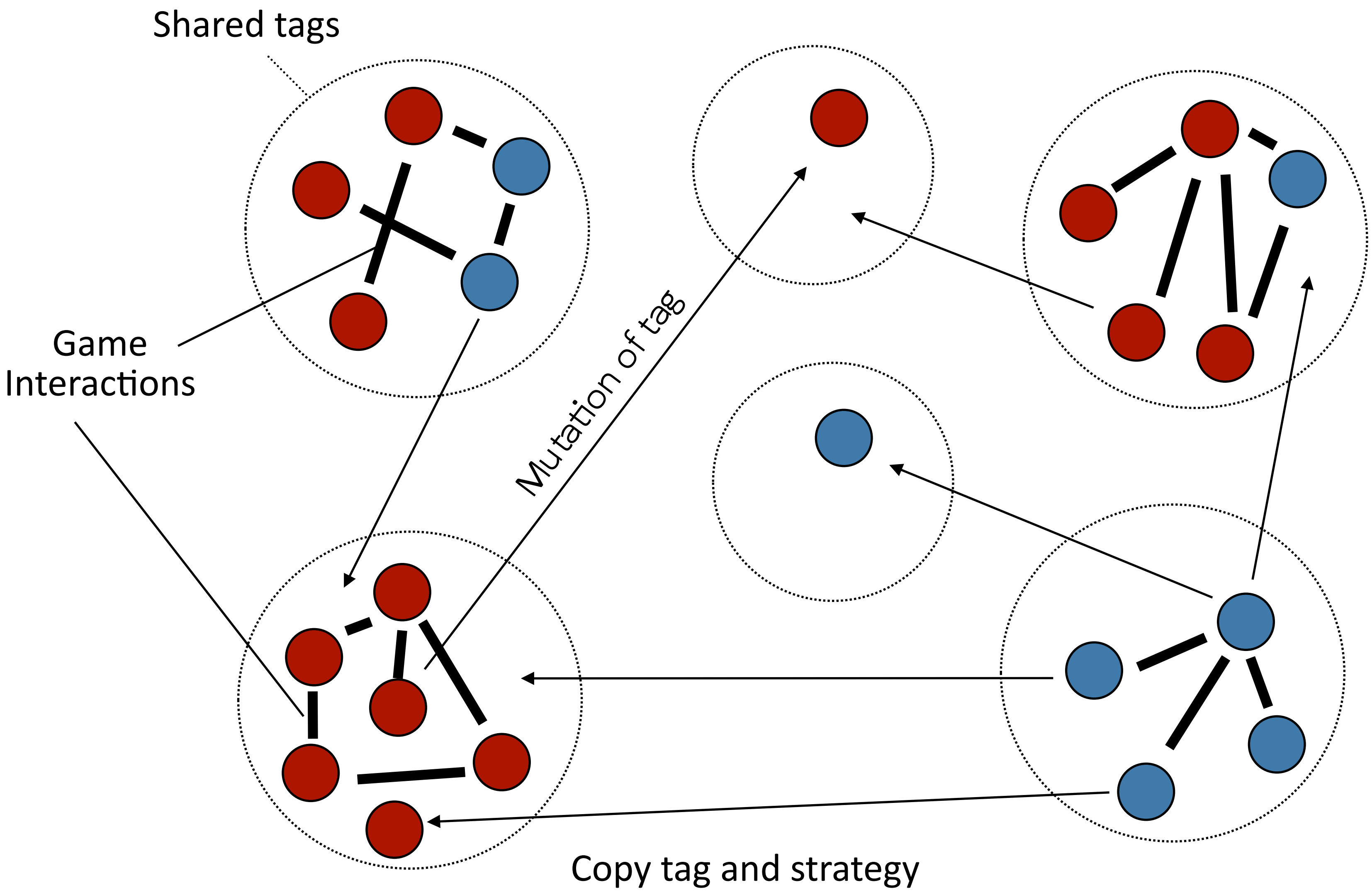
```
Initialise all agents with randomly selected strategies
LOOP some number of generations
    LOOP for each agent (a) in the population
        Select a game partner (b) from the population
        select a random partner with matching tag
        Agent (a) and (b) invoke their strategies
                                        receiving the appropriate payoff
    END LOOP
    Reproduce agents in proportion to their average payoff
                    with some small probability of mutation (M)
END LOOP
```

Agents – a tag and a PD Strategy

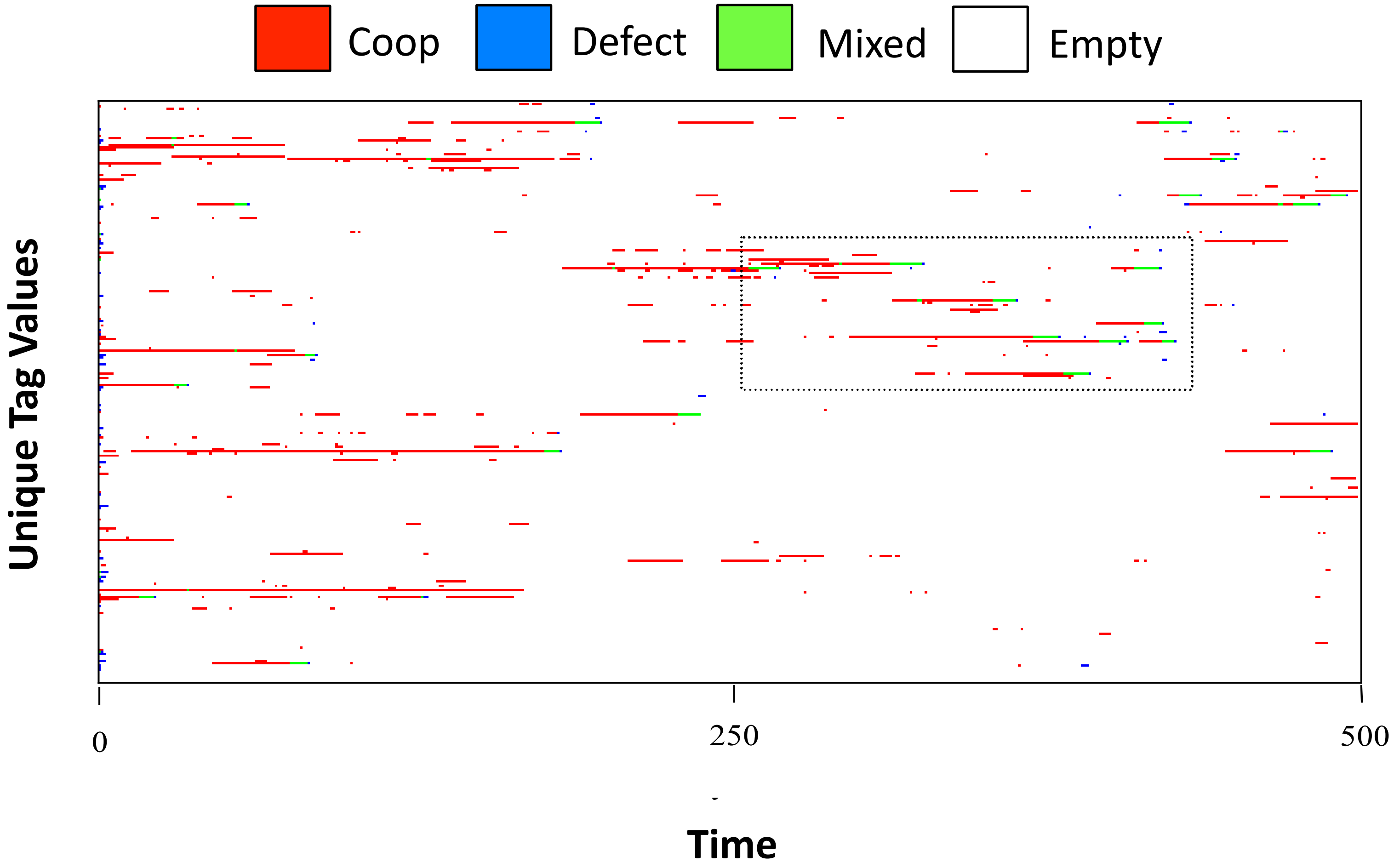


Tag = (Say) some integer
Game Interaction between those with same tag (if possible)

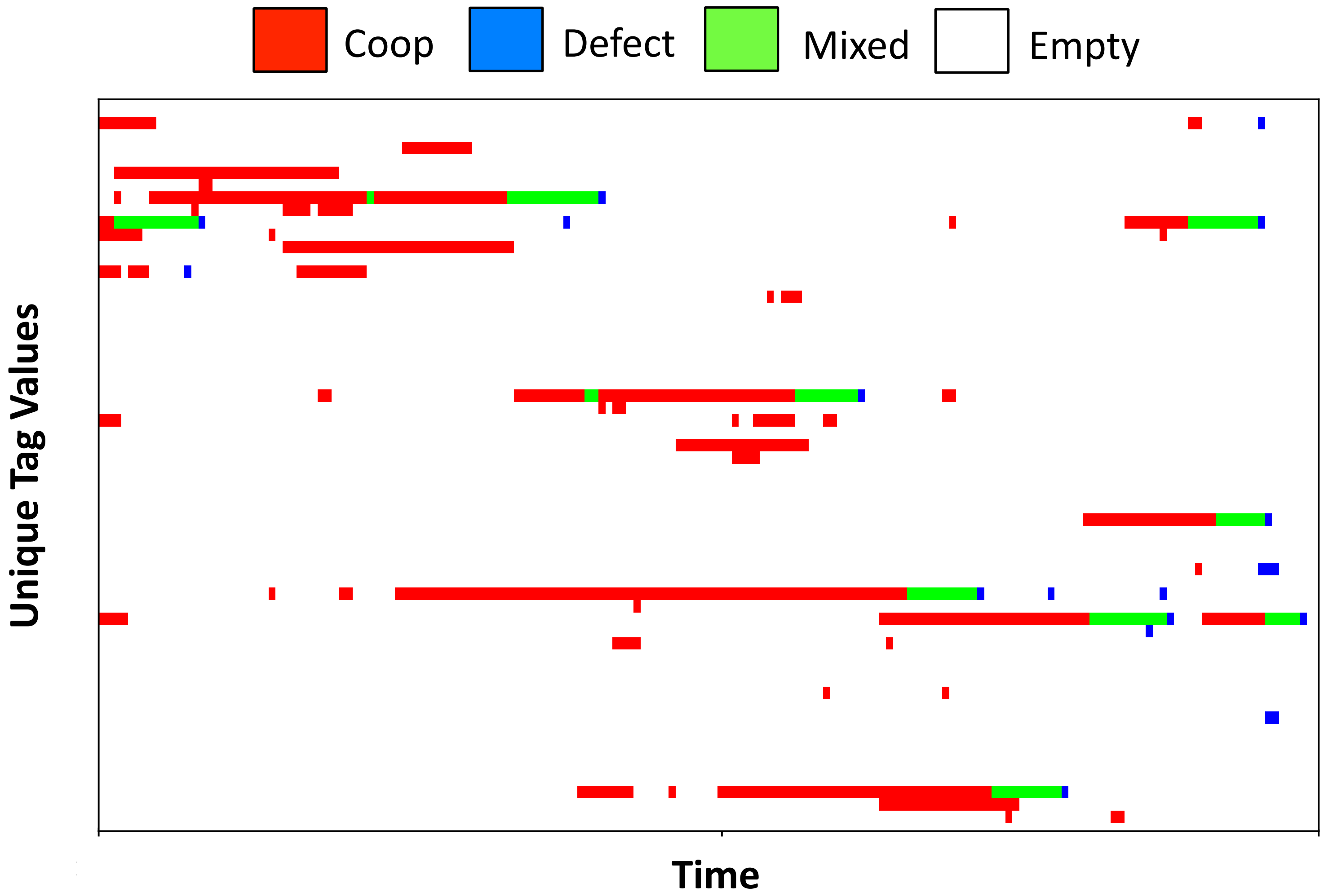
How tags work



Visualising the process



Visualising the process



Network rewire model

Each node *p* periodically performs a game interaction with a randomly chosen neighbor

Each node *p* periodically executes the following:

```
$q$ = SelectRandomPeer()
If $\text{utility}_q > \text{utility}_p$
    drop all current links
    link to node $q$ and copy its strategy and links
    mutate (with low probability) strategy and links
```

Network rewiring movie

Tags applied to altcoin ecology?

- Groups have to be formed more quickly than invaded and killed (new altcoins created rapidly)
- New groups are formed by mutation on the tag (new altcoin variants?)
- Old groups are killed by mutation on the strategy (hacking or speculation?)
- So if tag mutation > strategy mutation this should promote cooperation (following the protocol, avoid speculative runs?)
- Compare Tiebout (1956). Although here we have simple bounded imitators we still assume zero cost for moving, creating a new tag, network effects etc.

Further emerging research areas?

- Recentralisation
- Dynamic money supply
- Price stability
- Distributed institutions

Recentralisation

- Wallet services, central exchanges, mining pools, developer groups
- *Is recentralisation of Bitcoin (and variants) inevitable?*

Dynamic money supply

- Existing coins do not allow dynamic expansion and contraction of money supply
- This is considered a feature not a bug
- Attempts (such as Ripple.com)
- *Is it possible to create a P2P system supporting fractional reserve type functions?*

Price stability

- Bitcoin evidences high volatitly on exchange markets against fiat
- *Would it be possible to create a P2P system that could proactively attempt to stabalise such coins using some form of distributed algorithmic “open market operations”?*

Distributed institutions

- Speculated that next wave of P2P could be termed “Distributed Autonomous Organisations”
  - Based on computationally specified contracts
  - Many possible services other than coins
  - Governance: Voting, joint control of accounts, etc.
  - See www.ethereum.org
- *Can productive aspects of existing institutions be used as “templates” for new algorithmically enabled distributed institutions*

Conclusion

- On-going computational experiments “in the wild” with “skin in the game”
- Challenge to modellers – but look inherently amenable for agent-based approaches
- Could this all be a passing fad…
- Or as significant as the invention of double entry bookkeeping and the joint stock company?

Questions?

- Thank you for your attention