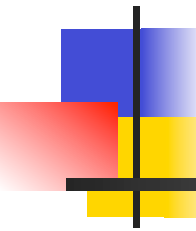


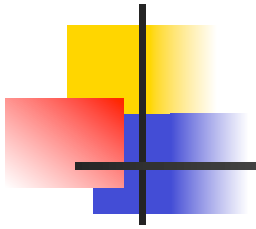
DO$H – Decentralized Object Storage Help (need better name☺)

Jon Crowcroft,

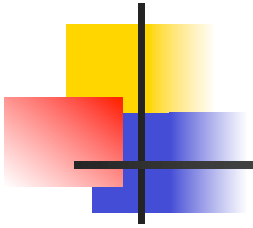
http://www.cl.cam.ac.uk/~jac22

http://hubofallthings.com/

Background to P2P and Virtual Currencies

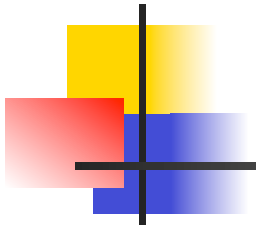


- Peer-to-peer systems avoid infrastructure
  - Eschew centralised ownership/management
  - Examples:
  - Internet (originally), Usenet
  - Mesh wireless nets
  - Mobile Ad Hoc Nets (MANETs)
  - Oppportunistic/mule nets are examples



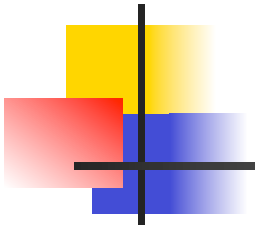
P2P #2

- Mutual exchange of resources
  - Layered on another (infra or p2p) net
  - Structured v. Unstructured, DHT, Key,Value stores, in Cloud (Cassandra etc)
- Storage
  - BitTorrent, Freenet, Eternity
- Computation
  - SETI@Home, ClimatePrediction.com
- Service (e.g. Presence)
  - Skype (originally)



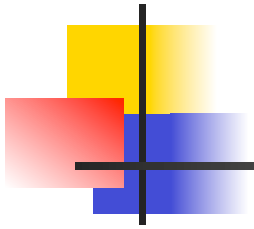
Virtual Currencies

- No currency - direct barter
  - Air Miles
  - Subway tokens
  - Exchanges – credit cards, paypal
- New:: BitCoin, Ripple, Properties
  - Decentralised Mint
    - no Owning/coercion
  - Decentralised Verification
    - mutual benefit in verifying == p2p store/check
  - Non-inflationary (BitCoin)



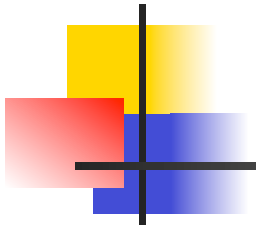
Mint/Verify BitCoin - crypto

- Basic trick is "proof of work"
  - Mitigates both forgery&double spending
- P2P verification entails keeping history
  - Transaction chain->not strictly anonymous
- Various possible problems like hoarding
  - Plus finite total (eventual) number of BitCoins -> possible loss impact
- "Alien Technology"



P2p incentives and currencies

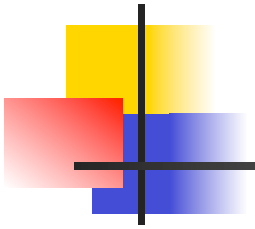
- We've been trying to get incentive alignment in p2p
  - Bittorrent uses tit-for-tat tokens
  - Did same in our work on mesh wifi
  - With deflationary currency to deal with
    - People leaving with money in their pocket
    - People joining/starters…
- Then along comes bitcoin (and ripple)
  - But….



Objections to BitCoin

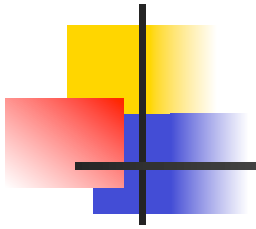
1. Proof of work is a waste of energy
2. Not anonymous (at least not as much as some people think)

- We don't like 1, but we don't mind 2.
- So……



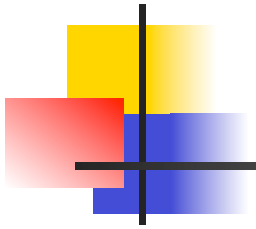
DO$H: an anonymous idea (by me)

- To fix some elements of bitcoin
  - And p2p storage systems
- Specifically,
  - Want to fund the Personal Cloud vision
  - with backup/resilience
  - other goodness properties



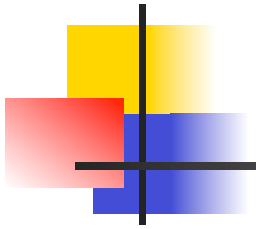
Personal cloud

- Everyone keeps their personal data
  - In their pocket
  - In their home hub, or car or bike
- But want backup (or nearby copies)
  - Could crypt and put in cloud
  - Or crypt and put in friends/family
  - Or even (many) arbitrary other users stores
- How to pay for cloud storage/cpu?



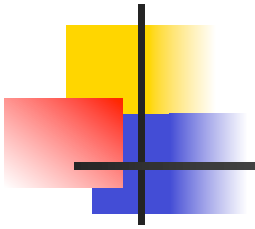
Monetizing Personal Data

- Don't "***put all our eggs in one basket***"
- s/facebook/personal cloud/
- Monetize data ***case by case*** basis
  - Idea also from HAT project
  - Have relationship with many vendors of goods and services – loyalty cards etc
  - They don't have usage data – we do
    - in personal cloud – home power, fridge, fitbit, scales, washing machines etc



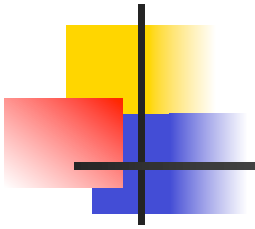
Model is they pay us

- Supermarket/pharmacy pay us for data
- In DOSH
- Generate DOSH coins by crypting our data – i.e. useful
- So we get adverts, but they don't leak data
- we also get DOSH, and could give BACK in exchange for no ads (just storage)



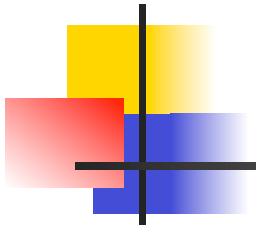
DOSH is quite like BitCoin

- But not deflationary – but bounded by people and goods used
  - so can't hyperinflate due to sustainability of world
- Keep BitCoin model of auditable verification chains
  - so can discourage use for Silk Road #3



Two more ideas

- Could source randomness for hashes DOSH protocol from non-co-ercable places
  1. Sustainable energy sources (solar/wind) contain natural randomness, which can be observed/recorded but aint easy to fake/ force
  2. Could also use 3D printers DRM random source (and so mark real world goods 3D printed with BitCoin verification hash



Have some pieces

- http://perscon.net/
- http://nymote.org/software/irminsule/
- Need to do open source DOSH
- And find some seed users…

- You didn't hear this from me

Who Am I?