BitCoin Issues

Charanjit Jutla
BitCoin’s Rise

• A perception that BitCoin is a potential non-fiat currency, rivaling GOLD.
• A decentralized implementation ingeniously based on proof of computational work
  – Tries to democratize monetary policy
    • As more people get involved in the authentication process, the less the “cartel” controls money policy…including money creation.
Decentralization Breakdown

• Risks of Hard Forks?
  – Two competing hash chains persist
    • Either by software problems or cartel control
      – Hopefully, software problems can be amicably resolved
    • How big is cartel risk?

• Claim
  • Cartels (or big players) need only control (say) 10% of mining to control hash chain direction.
    – Small miners will gravitate towards these big players.
    – Unlimited supply of new small miners (who jump in)
Why would Cartels Fork?

– Political or Nationalistic Reasons
  • Not interesting

– Mining cartels would ultimately become the savior of last resort in a credit based economy.
  • People need to invest their bitcoin savings
  • Most money is invested in “safe” bonds.
    – But with no governmental control, require insurance on investments
    – Insurance companies need re-insurance (e.g. AIG)
  • Mining Cartels are the best re-insurance companies in a world where bitcoin is the only currency.
    – They can insert arbitrary new money in the hash chain in a crisis…just like the FED.
Why would Cartels dilute BitCoin?

• Same reason as FED devalues fiat
  – Risk of complete breakdown of economy, if insurance companies go bankrupt
  – Assets of mining cartels to be seized by government… if reinsurance not honored.

• What about all the small miners?
  – Wither democratization of BitCoin?
    • They can try an alternate fork, but that would cause dramatic loss in valuation of BitCoin anyway.
Lack of Instant Credit in BitCoin

• Since BitCoin transactions require proof of work by miners, a tiny transaction can take an hour to be finalized (or proven secure).
  – However, proof of work is there only to allow democratization
  – We saw how democratization may not be possible after all in extreme crisis situations.

• Best to let Government or Powerful Banks control the transaction validation.
  – This would allow instant international transactions as well (with say, 5 minute credit).