



# What Happened to Digital Cash?



A. Michael Froomkin  
University of Miami  
<http://www.law.tm>

# Digital Cash—What is It?

- Store of value in digital form
- May require redemption or may be peer-to-peer
- May be ‘just a number’ (w/ digital signature backed by bank’s digital certificate)
- May require physical token for security
- May be fully traceable or payer-anonymous



# Common Issues

- Security
  - No forging cash
  - Don't want double-payment ... need to know when money is 'spent'
- Ease/Cheapness of use
  - End-users don't want to spend \$\$\$ on equipment; Want lower-than-VISA-margins
- Speed
  - Want quick transactions



# Solutions

- The Double-Spending Problem
  - Central registry (but it's slow)
  - Hardware solutions e.g. on-card monitor, but it's expensive and security is uncertain
- The Anonymity Issue
  - Fully anon cash or P2P can be used for money laundering
  - 'Blinded' coins



# Representative Implementations

- E-Cash by DigiCash (Chaum)
- Mondex
- Café Project (Conditional Access for Europe)
- Hashcash (and ilk)
- e-gold



# Making Money Makes Money

- Not just transactions fees at issuance and/or redemption
- Also the float
- Possible gain from unredeemed coins or balances (like old travelers checks)



# Why Nothing Took Off (1)

- Mondex
  - required infrastructure, Swindon test was a bust
  - (Rumor) Mondex had security issues at the ‘mint’



# Why Nothing Took Off (2)

- Chaumian cash
  - Chaum issues (Mark Twain Bank of St. Louis & 5 non-US banks)
  - Required finding a merchant who would accept it
  - Patent issues
    - Last major patent to expire in July 2005
  - FUD issues



# Why Nothing Took Off (3)

- Phil Agre said:
  - “With the bankruptcy of Digicash, it is time to assemble the definitive list of underperforming Internet technologies...The problem is that the Digicash people were living in the world of Alice and Bob -- a place where a mathematical proof can change the world in perfect defiance of the dynamics (if you can call them that) of large, highly integrated institutions”
- Did the customers really need it?
  - Unclear if we got a fair test for the software versions
  - Hardware had network effect, security issues
  - Or maybe it’s not what the market demanded



# A Solution In Search of a Problem?

- Mondex:
  - Savings didn't seem to justify expense for new hardware (network effect?);
  - customers didn't mind coins after all
- E-cash: Very little licensing made trials rare and peculiar
- Compare to air miles
  - “According to a new analysis by The Economist magazine, the global stock is worth more than \$700bn (£370bn), more than all the US dollar bills in circulation, and streets ahead of Britain's £42bn of notes and coins...”



# Or Just Biding its Time?

- Hashcash – maybe its time is coming?
- Chaumian cash patent expiry July 2005
- Interest in privacy is growing.
- But meanwhile...

