On Cash–like Digital Payment Systems

Daniel A. Nagy, Department of Mathematics and Statistics,
Queen’s University, Kingston, Ontario, Canada
Overview of Cash

- **Peer-to-peer**
  - anyone can pay and receive payment
  - no distinction between buyers and sellers
- **Transactions are anonymous and irreversible**
  - strangers can deal with each other
  - no need for identification, no risk of identity theft
- **No special equipment for receiving or paying**
  - a wallet comes handy, but it’s not required
- **Minimal transaction costs – ideally zero**
  - the buyer pays as much as the seller receives
Digital Cash Challenge

- **Double Spending**
  - digital information is easy to reproduce
  - duplicates must not be accepted as payment

- **Privacy & Transparency**
  - *noone* should be able to find out
    - how much cash a given person holds
    - in what transactions a given person participates
  - *anyone* should be able to find out
    - how much cash has been issued by a given issuer
    - if an issuer fails to honor its obligations
Environment (assumptions)

• Low-bandwidth, instantaneous communication (messaging) is cheap and ubiquitous

• Asymmetric cryptography is not prohibitively expensive but not necessarily available at all times to all parties (especially to payers)

• Public records are cheap to access and search by content
Dramatis Personæ

- **Ivan**
  - the payment system’s operator, acting on behalf of the issuer
  - has a permanent network address and digital identity
  - is on–line at all times
  - is able to perform all sorts of cryptographic calculations in large quantities

- **Alice**
  - payer

- **Bob**
  - receiver of payment
Ivan

- Maintains public records of value
- Receives and verifies requests
- Updates public records of value
Ivan

- Maintains public records of value
- Receives and verifies requests
- Updates public records of value
Ivan

- Maintains public records of value
- Receives and verifies requests
- Updates public records of value
Payment Scenario

Ivan

Serial Number: 0000000004
Value: 20 units
Challenge:  (blank)
Issued for: Emission request for 20
Signature: Ivan

Alice

Bob
Micro-payment

Ivan

Alice

Bob

Serial Number: 0000000004
Value: 20 units
Challenge: 

Issued for:
Emission request for 20

Signature: Ivan
Micro-payment

Serial Number: 0000000004
Value: 20 units
Challenge:
Issued for:
Emission request for 20
Signature: Ivan

Exchange request:

Alice

Bob
Micro-payment

Ivan

Alice

Bob

Serial Number: 0000000005
Value: 20 units
Challenge: 

Issued for:

Exchange request:

Signature: Ivan
Payment with Receipt

Ivan

Serial Number: 0000000004
Value: 20 units
Challenge:

Issued for:
Emission request for 20

Signature: Ivan

Alice

Bob
Payment with Receipt

Serial Number: 0000000004
Value: 20 units
Challenge:

Issued for:
Emission request for 20

Signature: Ivan

Alice

Bob

Pay 20

Pay 20
Payment with Receipt

Exchange request:

Ivan

Serial Number: 0000000004
Value: 20 units
Challenge:
Issued for:
Emission request for 20
Signature: Ivan

Alice

Pay 20

Bob
Security

- depends on the nature of the cryptographic challenges
- scales with transaction value, as determined by the users
- can be adequate for users with low computational resources
- addresses insider fraud
Conclusions

- The proposed payment system matches paper cash more closely than existing digital solutions
- Adequate for the whole range of transaction values ranging from micro-payments to high-value transfers
- Provides for transparent issuer governance
- Open-source implementation: [http://sf.net/projects/epoint](http://sf.net/projects/epoint)