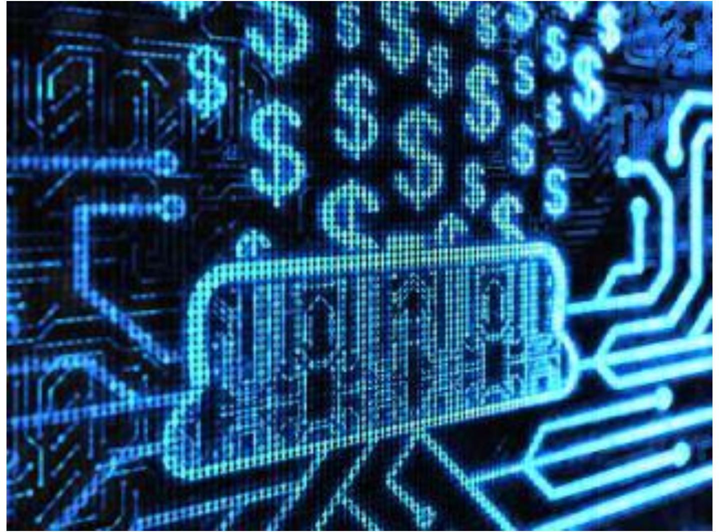
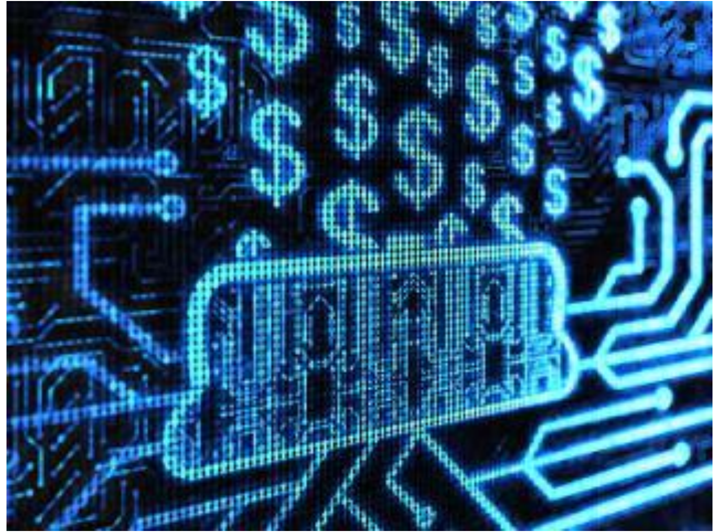


Digital Cash

Siu Sing Yu

Advised by

Prof. Cunsheng Ding



Introduction

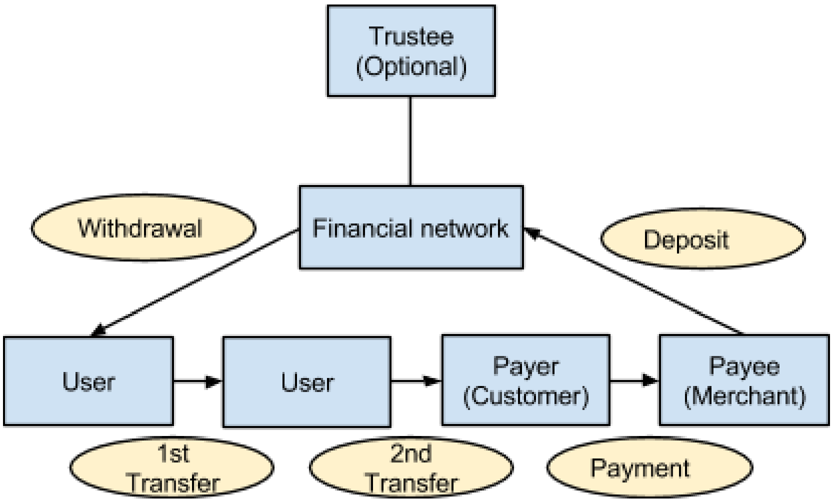
Using money is the most common economic behaviors of humans but what exactly is money? With the advancement of cryptography and massive coverage of internet, could digital cash be the next dominant form of money? What are the problems researchers striving to solve in order to make digital cash practical? What will be the benefit and problems of using digital cash? What is ideal money? This is a topic across both Cryptography and Economics.

Digital Cash in Cryptography

How to achieve,

1. **Anonymity**
2. **Offline capability**
3. **Divisibility**
4. **Transferability**
5. **Anonymity revocation**

Authoritative cash

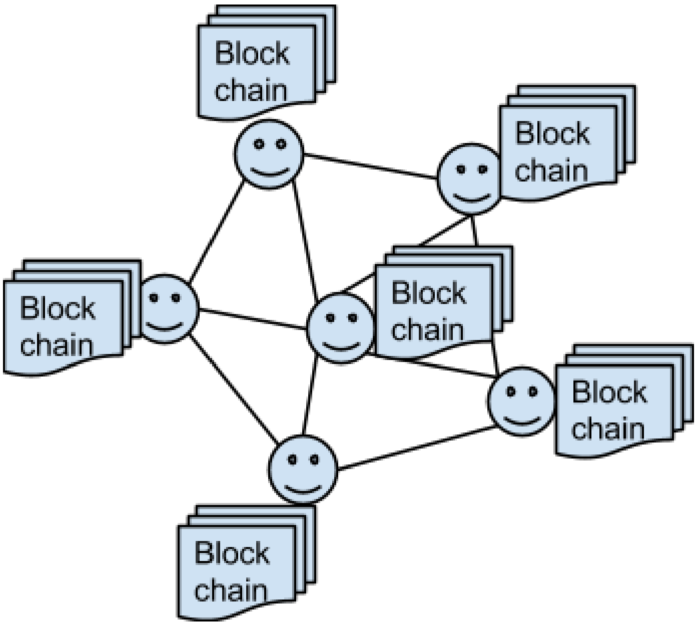


Common techniques

1. **Blind signature**
2. **Cut-and-Choose protocol**
3. **Restrictive Blind signature**
4. **Wallet with Observers**

5. **Division tree**
6. **Attaching payment history to cash**
7. **Attaching encrypted withdrawal and deposit information by trustee**

Anarchic Cash

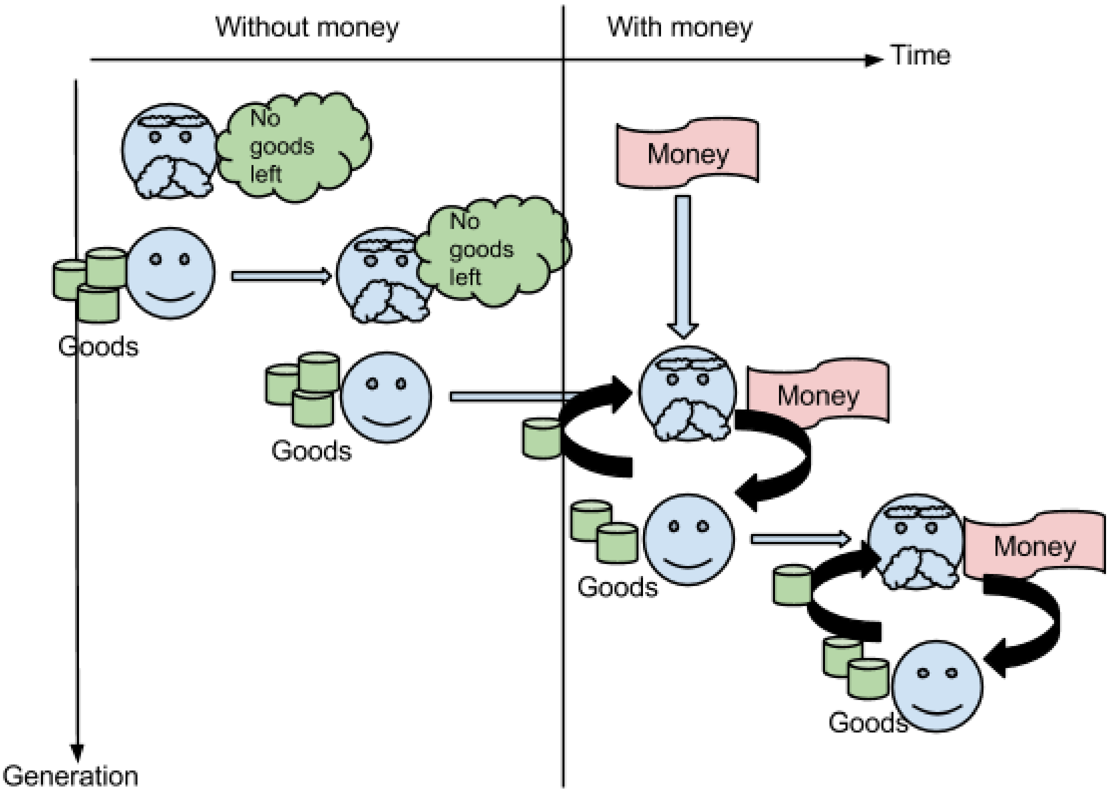


Common techniques

1. **Digital signature**
2. **Public block chain record**
3. **Proof of Work**
4. **Incentives to encourage honest transaction**

Money in Economics

Why do we use money? Explained by Overlapping generation model:



What is ideal money?

1) Storage of consumption, 2)Costless to produce, 3)Costless to store, 4)Costless to trade(use), 5)Issuer benefit free, 6)Flexible supply

Conclusion

Authoritative cash achieve features of ideal money. Some problems still remain

1. **Double spending problem limits transaction size**
2. **Key compromising is disastrous**
3. **Taxation ambiguity**
4. **Intensified exchange rate fluctuation**
5. **A new place for financial crisis**

Anarchic cash violates some features of ideal money, cannot dominate unless

1. **Backed up by valuable asset**
2. **Justified mining mechanism**
3. **Flexible money supply mechanism**