Stochastic Models for blockchain analysis

Decentralized and cryptopricing

Pierre-O. Goffard

Institut de Science Financières et d'Assurances
pierre-olivier.goffard@univ-lyon1.fr

6 septembre 2021

Decentralized and cryptopricing

1 Decentralized finance

2 Cryptopricing

Types of Crypto Assets

- Cryptocurrencies
- Utility Token
- Security Token
- Non Fungible token

Cryptocurrency

Decentralized finance

Digital currency as a medium of exchange with three key characteristics

- Anonymity
- No central authority
- Protected against double spending attack

J. Lansky, "Possible state approaches to cryptocurrencies," *Journal of Systems Integration*, vol. 9, pp. 19–31, jan 2018.

How does it work ?

Decentralized finance

1. No central authority (Decentralized network)
2. Ledger to record all the transactions and coin ownership (blockchain)
3. A coin generation process (block finding reward)
   ↪ Incentive to the full nodes
4. Ownership can be proved cryptographically (wallet associated to a public/private key)
5. Transactions can be issued by an entity proving ownership of the cryptographic unit (through the private key)
6. The system cannot process more than one transaction associated to the same cryptographic unit (double spending)

More on anonymity

- Transparent account : The owner has revealed her identity in a credible manner
- Semi-transparent account : The owner identity is traceable by state authority
    - Exchange to fiat currency with an exchange office that abids by KYC rules
- Pseudo anonymous account : Owner identity is known by the owner's business partners (like a merchant who would remember the customer's face in the case of an extraordinary purchase).
- Anonymous account : Nobody knows the owner's identity, newly created account.

Purposes of cryptocurrencies

- Micropayments : If the transaction fee is significantly lower than the amounts conveyed
  - ↪ $0.03 for DogeCoin
- Foreign payments : International payment without delay and bank fees
- Payments in countries with unstable local currencies : In some African and South American countries with high inflation rate
- Information retention : OP_RETURN transactions to add informations without transferring any amount of cryptographic unit.

Risk associated to cryptocurrencies

- Low market capitalisation : If the number of users is limited and the market cap is low then one user's trade may have disproportionate consequences of the coin value
- Private key = ownership : Personal computers or server of wallet management services may be hacked. One solution is to resort to hardware to store the private key.
- Transaction irreversibility : If some funds are transfered by misstake, they are not recoverables
- Account anonymity : Whenever an account issue transactions, it becomes pseudo-anonymous. It is difficult to for the authority to find the identity of a pseudo anonymous account when funds are used for criminal activities (financial theft, tax evasions, extortions or bribery).

Cryptocurrency implementation

Blockchain parameters

- Consensus protocol (PoW or PoS)
  - ↪ Hash function (SHA-256 for Bitcoin and scrypt for LiteCoin)
    - ↪ Hybrid PoW/PoS (PeerCoin)
- Block generation time
  - ↪ every 10 minutes for Bitcoin
    - ↪ every 12 sec for Ethereum
- Block finding reward
  - ↪ Halved every 210,000 blocks in Bitcoin. It started at 50 BTC, is now 6.25 BTC `https://www.bitcoinblockhalf.com/`
- Total coin supply
  - ↪ 21,000,000 in total for Bitcoin
- Transaction fees
  - ↪ GAS in Ethereum

These choices lead to the creation of multiple cryptocurrencies

Examples

Bitcoin and AltCoins (Ethereum, LiteCoin, DogeCoin, Ripple...), see `https://en.wikipedia.org/wiki/List_of_cryptocurrencies`

Utility token

Digital asset that grant access to goods and services provided by the network.

- Digital coupon or digital casino chip
- Mainly powered by the Ethereum blockchain through smart contracts
- Crowdfunding means for blockchain based start up projects via Initial Coin Offerings (discussed later)

Examples

Funfair, Basic Attention Token, Golem token, FileCoin ...

Tokenized real-world assets

Tokenized version of a real-world, physical asset

- Increases the liquidity of certain type of assets
- Make certain classes of assets available to the many
- Can be used as store of value or collateral

These token can be backed by

- fiat currency ⇒ stablecoin
- commodities like gold `https://ekon.gold/`
- stocks (security token) that includes voting right and profit sharing mechanism
- Art
- Digital art (Non Fungible tokens on the Ethereum blockchain)

Central authority

This requires a custodian to ensure that the tokens are actually backed by these off-chain assets (except for NFTs).

OECD, "The tokenisation of assets and potential implications for financial markets," tech. rep., 2020.

Decentralized Finance applications

- Fundraising instruments
- Decentralized exchange platforms
  - Trades are settled on-chain (verifiable)
  - Exchange do not own the users' funds (non-custodial)
  - Automated Market Makers (AMM) to provide liquidity `https://uniswap.org/`
- DeFi lending protocols
  - Peer-to-peer lending
  - Borrow against a smart contract reserves made ofa pool of users deposit
  - *Overcollateralization*

Valuation models

Cryptopricing

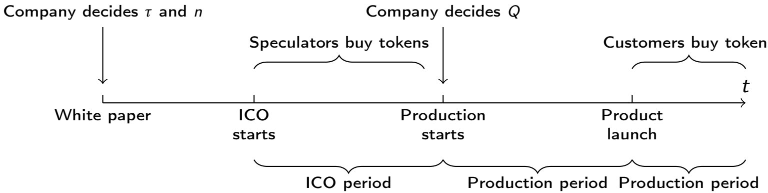
- Cryptocurrencies are medium of exchange and may be priced via transaction cost model (Beaumol-Tobin and such)
  - W. J. Baumol, "The transactions demand for cash : An inventory theoretic approach," *The Quarterly Journal of Economics*, vol. 66, p. 545, nov 1952.
  - L. Schilling and H. Uhlig, "Some simple bitcoin economics," *Journal of Monetary Economics*, vol. 106, pp. 16–26, oct 2019.
- Tokenized asset depends on the real asset that backs the token
  - J. Hargrave, N. Sahdev, and O. Feldmeier, "How value is created in tokenized assets," in *Blockchain Economics : Implications of Distributed Ledgers*, pp. 125–143, WORLD SCIENTIFIC (EUROPE), jan 2019.
- Utility tokens
  - J. R. Gan, G. Tsoukalas, and S. Netessine, "Initial coin offerings, speculation, and asset tokenization," *Management Science*, vol. 67, pp. 914–931, feb 2021.
  - L. W. Cong, Y. Li, and N. Wang, "Tokenomics : Dynamic adoption and valuation," *The Review of Financial Studies*, vol. 34, pp. 1105–1155, aug 2020.

ICO tuning and timeline

Cryptopricing

Game theoretic approach with three players : The firm, the speculators and the customers that interacts over three time period

1. ICO period
   - The firm publishes a white paper and set
     - The token price τ
     - The total number of token m
     - The number of tyoken issued to the investors during the ICO $n \leq m$.
   - s among $z >> m$ investors buy token
2. Production period
   - The firm uses the funds raised $s\tau$ to finance the production of Q units of goods
3. Market period
   - Customers purchase token to meet their needs $D \sim F(.)$



Searching for an equilibrium

Let

- c be the production cost of one unit of good (\$ per unit)
- p be the value of the good in tokens per unit
- v How much the good is worth from the customers' point of view (\$ per unit)
- τ_{eq} the token price at equilibrium

We have

$$\tau_{eq} = \frac{\min(Q,D)\cdot v}{m}$$

Because the firm is a monopoly then $p = \tau_{eq}\cdot v$, and therefore

$$p = \frac{m}{\min(Q,D)}.$$

J. R. Gan, G. Tsoukalas, and S. Netessine, "Initial coin offerings, speculation, and asset tokenization," *Management Science*, vol. 67, pp. 914–931, feb 2021.

L. W. Cong, Y. Li, and N. Wang, "Tokenomics : Dynamic adoption and valuation," *The Review of Financial Studies*, vol. 34, pp. 1105–1155, aug 2020.