Costs of the Digital Currency Provision from the Macroeconomic Prospective

Crypto-currencies in a digital economy

Anna Almosova

Humboldt University Berlin

November 17, 2017

Research Question

The role of money provision costs for:

1. market outcome in the economy with purely private money provision
2. competition between private and public currencies
3. welfare maximizing monetary policy

Motivation

- Recent development of private (digital and decentralized) currencies
  - We need a macroeconomic model to analyze them

Motivation

- Recent development of private (digital and decentralized) currencies
  - We need a macroeconomic model to analyze them
- Private money are provided by private rational agents
  - compete with each other and public fiat money

Motivation

- Recent development of private (digital and decentralized) currencies
  - We need a macroeconomic model to analyze them
- Private money are provided by private rational agents
  - compete with each other and public fiat money
- In a decentralized network money provision is done by miners through proof-of-work (energy costs)

Cyrptocurrencies

- About 1200 different cryptocurrencies (`coinmarketcap.com`)
- BTC market capitalization appr. $116 billion or 3% of the US M1 ($3,600 billion) (`blockchain.info`)
- About 300,000 transaction per day in BTC

Proof-of-work: (electricity) costs

- are an essential part of the algorithm
  - "cheap talk" problem

Proof-of-work: (electricity) costs

- are an essential part of the algorithm
  - "cheap talk" problem
- are significant
  - O'Dwyer, Malone (2014): Ireland's annual electricity consumption app. 3 GW, BTC 1 to 10GW

Proof-of-work: (electricity) costs

- are an essential part of the algorithm
  - "cheap talk" problem
- are significant
  - O'Dwyer, Malone (2014): Ireland's annual electricity consumption app. 3 GW, BTC 1 to 10GW
- affect the amount of mining
  - positive correlation with electricity prices

Proof-of-work: (electricity) costs

- are an essential part of the algorithm
  - "cheap talk" problem
- are significant
  - O'Dwyer, Malone (2014): Ireland's annual electricity consumption app. 3 GW, BTC 1 to 10GW
- affect the amount of mining
  - positive correlation with electricity prices
- are compensated by a reward = increase a money supply

Macro literature on currency competition

Literature on private money (inside money) provision & currency competition

1. Klein (1974)
2. Taub (1985)
3. Marimon et al (2000,2003), Marimon et al (2012)
4. Berentsen (2006)
5. Fernandez-Villaverde, Sanches (2016)

Macro literature on currency competition

Literature on private money (inside money) provision & currency competition

1. Klein (1974)
2. Taub (1985)
3. Marimon et al (2000,2003), Marimon et al (2012)
4. Berentsen (2006)
5. Fernandez-Villaverde, Sanches (2016)
    - Monetary search model Lagos, Wright (2005)
    - Rational private money issuers
    - Linear costs of money creation

Model Specifications

- Money is required due to the "double-coincidence" problem

Model Specifications

- Money is required due to the "double-coincidence" problem
- Perfect foresight, full commitment or optimization problem

Model Specifications

- Money is required due to the "double-coincidence" problem
- Perfect foresight, full commitment or optimization problem
- Miner can decide on the money supply (constant difficulty, 1 unit reward, 1 transaction per block)

Model Specifications

- Money is required due to the "double-coincidence" problem
- Perfect foresight, full commitment or optimization problem
- Miner can decide on the money supply (constant difficulty, 1 unit reward, 1 transaction per block)
- Linear costs of private money creation, zero costs of public money creation

Preview of the Results (compared to zero costs)

Equilibrium with private money provision:

Preview of the Results (compared to zero costs)

Equilibrium with private money provision:

1. Constant price (zero inflation) equilibrium does not exist
2. Equilibrium path with constant positive inflation and positive constant money growth rate

Preview of the Results (compared to zero costs)

Equilibrium with private money provision:

1. Constant price (zero inflation) equilibrium does not exist
2. Equilibrium path with constant positive inflation and positive constant money growth rate
3. Level of production and trade is smaller
4. Continuum of equilibrium trajectories with value of money converging to zero as in the standard model

Preview of the Results

Mixed symmetric equilibrium with public and private money:

Preview of the Results

Mixed symmetric equilibrium with public and private money:

5. Competition imposes a maximum sustainable level of π which becomes a function of costs
6. Government can drive private money out of circulation even under a positive money growth
7. Purely public money equilibrium is not necessarily welfare superior

Preview of the Results

Mixed symmetric equilibrium with public and private money:

5. Competition imposes a maximum sustainable level of π which becomes a function of costs
6. Government can drive private money out of circulation even under a positive money growth
7. Purely public money equilibrium is not necessarily welfare superior
8. Standard Friedman rule ($\pi = \beta - 1 < 0$) applies
9. Costs of money creation only affect welfare through miners' decisions

Monetary Search Model

[0,1] buyers, [0,1] sellers and countable ∞ of inactive miners and 1 active miner and free-entry

Monetary Search Model

[0,1] buyers, [0,1] sellers and countable ∞ of inactive miners and 1 active miner and free-entry

Centralized market (CM) and decentralized market (DM) or day and night

Monetary Search Model

[0,1] buyers, [0,1] sellers and countable ∞ of inactive miners and 1 active miner and free-entry

Centralized market (CM) and decentralized market (DM) or day and night

DM is anonymous. Sellers (only sell) randomly meet buyers (only buy) with probability σ. They see each other once and never again.

Monetary Search Model

[0,1] buyers, [0,1] sellers and countable ∞ of inactive miners and 1 active miner and free-entry

Centralized market (CM) and decentralized market (DM) or day and night

DM is anonymous. Sellers (only sell) randomly meet buyers (only buy) with probability σ. They see each other once and never again.

CM and quasi-linear preferences - distribution of money holdings is degenerate

Monetary Search Model

[0,1] buyers, [0,1] sellers and countable ∞ of inactive miners and 1 active miner and free-entry

Centralized market (CM) and decentralized market (DM) or day and night

DM is anonymous. Sellers (only sell) randomly meet buyers (only buy) with probability σ. They see each other once and never again.

CM and quasi-linear preferences - distribution of money holdings is degenerate

Miners can produce intrinsically worthless tokens (medium of exchange, perfect substitutes). Their trade history is public. Mining activity is costly with linear cost function

Monetary Search Model

[0,1] buyers, [0,1] sellers and countable ∞ of inactive miners and 1 active miner and free-entry

Centralized market (CM) and decentralized market (DM) or day and night

DM is anonymous. Sellers (only sell) randomly meet buyers (only buy) with probability σ. They see each other once and never again.

CM and quasi-linear preferences - distribution of money holdings is degenerate

Miners can produce intrinsically worthless tokens (medium of exchange, perfect substitutes). Their trade history is public. Mining activity is costly with linear cost function

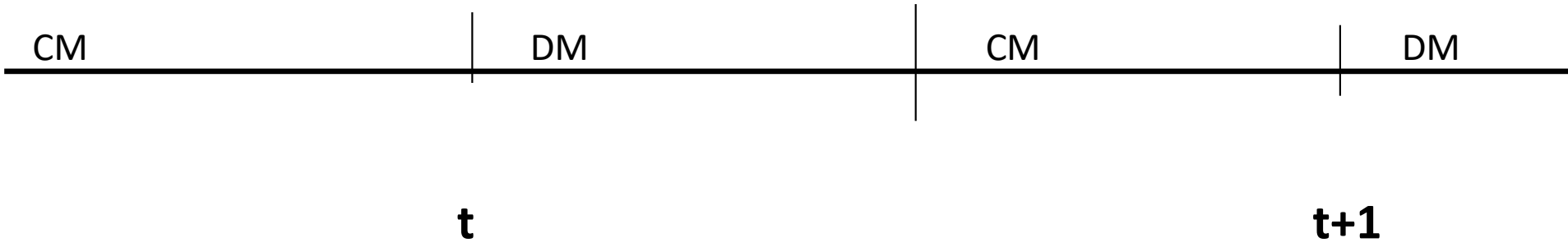
Miners are rational agents that maximize profit (commitment device)

Timeline

N^b, N^s $\quad$ $m_t = M_t$

$(m_t - m_{t-1})\phi_t + x^b + x^s = N^b + N^s$ $\quad$ $q_t = q(m_t)$

$x^M = \phi_t (M_t - M_{t-1})$



Buyer

$$W_t^b(\hat{m}_t) = \max_{x_t^b, \hat{m}_t} [x_t^b + \sigma \left(u(q_t(\hat{m}_t, \hat{m}_t^s)) + \beta W_{t+1}^b(\hat{m}_t - d_t(\hat{m}_t, \hat{m}_t^s)) \right) + \\ + (1-\sigma)\beta W_{t+1}^b(\hat{m}_t)]$$

$$\text{s.t. } \phi_t \hat{m}_t + x_t^b + \tau_t = \phi_t m_t$$

Buyer

$$W_t^b(\hat{m}_t) = \max_{x_t^b, \hat{m}_t} [x_t^b + \sigma \left(u(q_t(\hat{m}_t, \hat{m}_t^s)) + \beta W_{t+1}^b(\hat{m}_t - d_t(\hat{m}_t, \hat{m}_t^s)) \right) + \\ + (1-\sigma)\beta W_{t+1}^b(\hat{m}_t)]$$

$$\text{s.t. } \phi_t \hat{m}_t + x_t^b + \tau_t = \phi_t m_t$$

$$W_t^b(\hat{m}_t) = \phi_t m_t + \max_{\hat{m}_t} [-\phi_t \hat{m}_t + \sigma \left(U(q_t(\hat{m}_t, \hat{m}_t^s)) + \beta W_{t+1}^b(\hat{m}_t - d_t(\hat{m}_t, \hat{m} \right. \\ + (1-\sigma)\beta W_{t+1}^b(\hat{m}_t)]$$

$$u(0) = 0, u'(0) = \infty, u'(\cdot) > 0, u''(\cdot) < 0$$

Seller

$$W_t^s(\hat{m}_t^s) = \max_{x_t^s, \hat{m}_t^s} [x_t^s + \sigma \left(w(q_t(\hat{m}_t, \hat{m}_t^s)) + \beta W_{t+1}^s(\hat{m}_t^s + d_t(\hat{m}_t, \hat{m}_t^s)) \right) + \\ + (1-\sigma)\beta W_{t+1}^s(\hat{m}_t^s)]$$

$$\text{s.t. } \phi_t \hat{m}_t^s + x_t^s + \tau_t = \phi_t m_t^s$$

$w(\cdot)$ is a disutility from labor, production function $q_t = n_t$

$w(0) = 0, w'(\cdot) > 0, w''(\cdot) > 0$

Bargaining: take-it-or-leave-it offer from a buyer

$$\max_{q_t, d_t} [u(q_t) - \beta \phi_{t+1} d_t]$$

$$\text{s.t.} \quad -w(q_t) + \beta \phi_{t+1} d_t \geq 0 \qquad \text{PC}$$

$$d_t < \hat{m}_t \qquad \text{LC}$$

Bargaining: take-it-or-leave-it offer from a buyer

$$\max_{q_t, d_t} [u(q_t) - \beta \phi_{t+1} d_t]$$

$$\text{s.t.} \quad -w(q_t) + \beta \phi_{t+1} d_t \geq 0 \qquad \text{PC}$$

$$d_t < \hat{m}_t \qquad \text{LC}$$

$$q_t = \begin{cases} q^* \text{ if } \phi_{t+1} \hat{m}_t \geq \beta^{-1} w(q_t^*) \\ w^{-1}(\beta \phi_{t+1} \hat{m}_t) \text{ if } \phi_{t+1} \hat{m}_t < \beta^{-1} w(q_t^*) \end{cases}$$

$$\phi_{t+1} d_t = \begin{cases} \beta^{-1} w(q^*) \text{ if } \phi_{t+1} \hat{m}_t \geq \beta^{-1} w(q_t^*) \\ \phi_{t+1} \hat{m}_t \text{ if } \phi_{t+1} \hat{m}_t < \beta^{-1} w(q_t^*) \end{cases}$$

Bargaining: take-it-or-leave-it offer from a buyer

Solution exists only with $\frac{\phi_{t+1}}{\phi_t} \leq \beta^{-1}$. Denote $\gamma_{t+1} \equiv \frac{\phi_{t+1}}{\phi_t}$.

$u'(q^*) = w'(q^*)$.

From the buyer's problem $-\phi_t + \frac{dW^b(\hat{m}_t)}{d\hat{m}_t} \leq 0$ and $= 0$ if $\hat{m}_t > 0$.

Bargaining: take-it-or-leave-it offer from a buyer

Solution exists only with $\frac{\phi_{t+1}}{\phi_t} \leq \beta^{-1}$. Denote $\gamma_{t+1} \equiv \frac{\phi_{t+1}}{\phi_t}$.

$u'(q^*) = w'(q^*)$.

From the buyer's problem $-\phi_t + \frac{dW^b(\hat{m}_t)}{d\hat{m}_t} \leq 0$ and $= 0$ if $\hat{m}_t > 0$.

$$\sigma \frac{u'(q_t)}{w'(q_t)} + 1 - \sigma = \frac{\phi_t}{\beta \phi_{t+1}} -> q(\gamma_{t+1})$$

$$d_t = \hat{m}_t$$

$$\phi_{t+1}\hat{m}_t = \beta^{-1} w(q_t) -> \phi_{t+1}\hat{m}_t = z(q_t)$$

Seller (second look)

$$W_t^s(m_t^s) = \max_{x,\hat{m}_t^s}[x + \sigma\left(w(q_t(\hat{m}_t, \hat{m}_t^s)) + \beta W_{t+1}^s(\hat{m}_t^s + d_t(\hat{m}_t, \hat{m}_t^s))\right) + \\ + (1-\sigma)\beta W_{t+1}^s(\hat{m}_t^s)]$$

$$\text{s.t. } \phi_t \hat{m}_t^s + x_t^s + \tau_t = \phi_t m_t^s$$

Seller (second look)

$$W_t^s(m_t^s) = \max_{x,\hat{m}_t^s}[x + \sigma\left(w(q_t(\hat{m}_t, \hat{m}_t^s)) + \beta W_{t+1}^s(\hat{m}_t^s + d_t(\hat{m}_t, \hat{m}_t^s))\right) + \\ + (1-\sigma)\beta W_{t+1}^s(\hat{m}_t^s)]$$

$$\text{s.t. } \phi_t \hat{m}_t^s + x_t^s + \tau_t = \phi_t m_t^s$$

Since bargaining does not depend on seller's money the seller chooses not to hold any (if $\frac{\phi_{t+1}}{\phi_t} < \beta^{-1}$)

Note: since only the buyers hold money, they are be fully compensated in a DM bargaining

Miner (N=1)

$$\max_{\{x^i\}_t} \sum_{t=0}^{\infty} \beta^t x_t^M$$

$$\text{s.t. } x_t^M = \phi_t(M_t - M_{t-1}) - \psi\phi_t M_t$$

Miner (N=1)

$$\max_{\{x^i\}_t} \sum_{t=0}^{\infty} \beta^t x_t^M$$

$$\text{s.t. } x_t^M = \phi_t(M_t - M_{t-1}) - \psi\phi_t M_t$$

Linear costs $Costs(M_t) = \psi M_t$

Miner (N=1)

$$\max_{\{x^i\}_t} \sum_{t=0}^{\infty} \beta^t x_t^M$$

$$\text{s.t. } x_t^M = \phi_t(M_t - M_{t-1}) - \psi\phi_t M_t$$

Linear costs $Costs(M_t) = \psi M_t$

$$\sum_{t=0}^{\infty} \beta^t \phi_t M_t(1-\psi) - \phi_t M_{t-1} = 0$$

$$\phi_t M_t(1-\psi) - \phi_t M_{t-1} = 0 \ \forall t$$

$$M_t(1-\psi) - M_{t-1} = 0 \ \forall t \text{ if } \phi_t > 0$$

from consumption non-negativity and free entry

Miner

$$M_t(1-\psi) - M_{t-1} = 0 \ \forall t$$

$$M_t = \frac{1}{1-\psi} M_{t-1}$$

Proposition 1:

1) with no costs of money creation, free entry forces miner to keep money supply constant.

2) constant money supply growth and positive seigniorage is needed to compensate for money creation costs.

BTC example

$$M_t(1-\psi) - M_{t-1} = 0 \ \forall t$$

$$M_t = \frac{1}{(1-\psi)} M_{t-1}$$

	2015	2016	2017
Money growth*	1,2	1,09	1,07
Implied ψ	0,17	0,09	0,07

source: blockchain.info and author's calculations. *number of confirmed transactions

Miner

$$\phi_t M_t(1-\psi) - \phi_t M_{t-1} = 0 \ \forall t$$

Denote real return on money i as $\gamma_t \equiv \frac{\phi_t}{\phi_{t-1}}$, note that $\gamma_t = \frac{1}{1+\pi_t}$

Denote the real total money supply as $b_t \equiv \phi_t M_t$

$$b_t(1-\psi) - \gamma_t b_{t-1} = 0 \ \forall t$$

$$m(q(\gamma_{t+1})) -> z(\gamma_{t+1}) = b_t$$

$$(1-\psi)z(\gamma_t) - \gamma_t z(\gamma_{t-1}) = 0$$

Equilibrium (purely private money)

$$(1-\psi)z(\gamma_t) - \gamma_t z(\gamma_{t-1}) = 0 \text{ with } 0 \leq \gamma_t \leq \beta^{-1}$$

Equilibrium (purely private money)

$$(1-\psi)z(\gamma_t) - \gamma_t z(\gamma_{t-1}) = 0 \text{ with } 0 \leq \gamma_t \leq \beta^{-1}$$

Proposition 2: with fixed costs of money creation there exist no equilibrium path with constant prices (zero inflation or $\gamma_t = 1$). Instead, $\bar{\gamma} = 1 - \psi$, which means constant decline of the real price to money or constant inflation.

Equilibrium (purely private money)

$$(1-\psi)z(\gamma_t) - \gamma_t z(\gamma_{t-1}) = 0 \text{ with } 0 \leq \gamma_t \leq \beta^{-1}$$

Proposition 2: with fixed costs of money creation there exist no equilibrium path with constant prices (zero inflation or $\gamma_t = 1$). Instead, $\bar{\gamma} = 1 - \psi$, which means constant decline of the real price to money or constant inflation.

	2015	2016	2017
Money growth*	1,2	1,09	1,07
Implied ψ	0,17	0,09	0,07
Implied π (const. q)	20%	9,8%	7,5%

Monetary Equilibrium

$$(1-\psi)z(\gamma_t) - \gamma_t z(\gamma_{t-1}) = 0 \text{ with } 0 \leq \gamma_t \leq \beta^{-1}$$

$$\gamma_{t+1}(\gamma_t)$$

Proposition 3: regardless of the money creation costs, there exist a steady state with no money circulation ($\bar{\gamma} = 0$) and a continuum of equilibrium trajectories along with the value of money converges to zero.

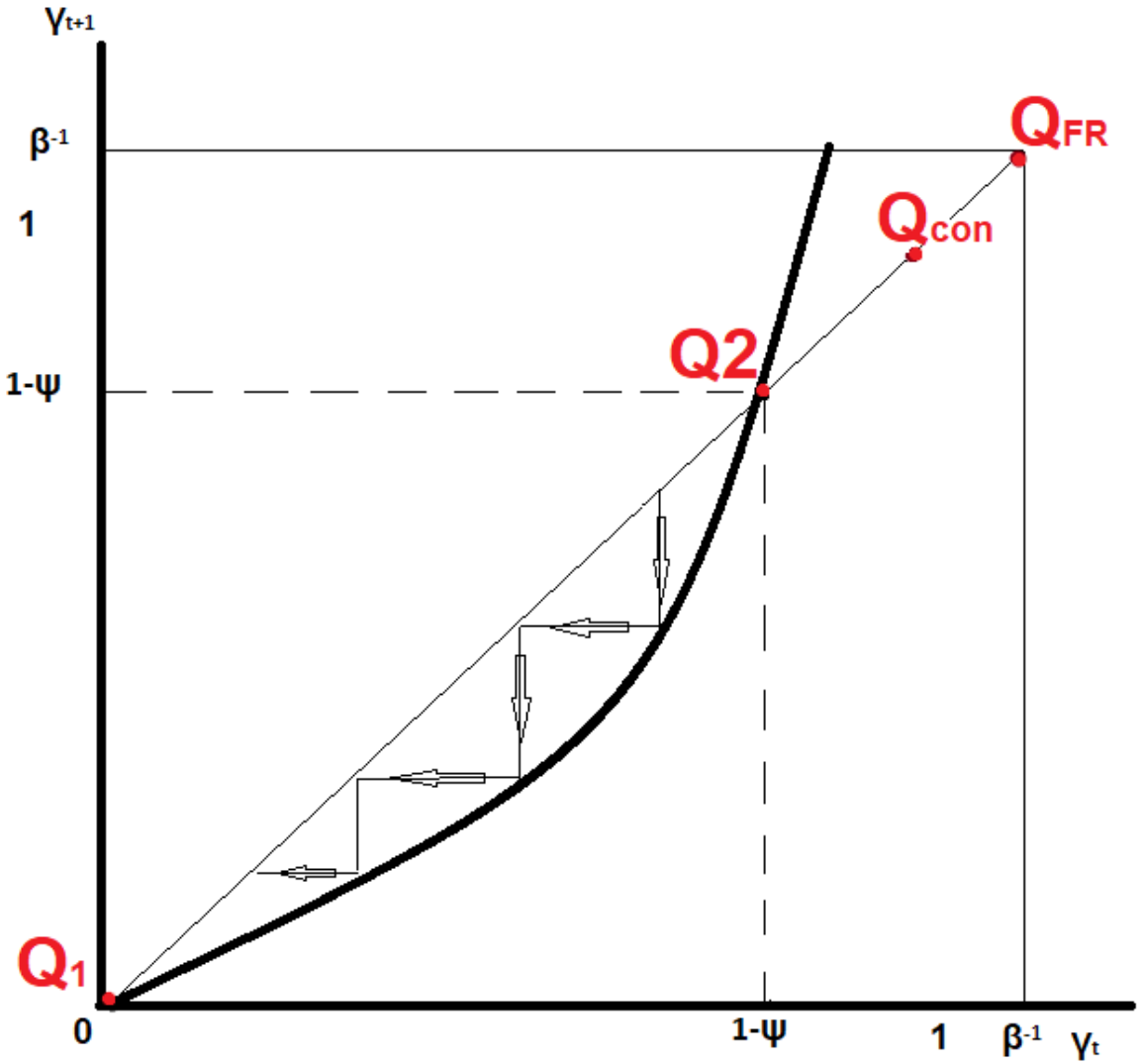
Monetary Equilibrium

$$(1-\psi)z(\gamma_t) - \gamma_t z(\gamma_{t-1}) = 0 \text{ with } 0 \leq \gamma_t \leq \beta^{-1}$$

$$\gamma_{t+1}(\gamma_t)$$

Proposition 3: regardless of the money creation costs, there exist a steady state with no money circulation ($\bar{\gamma} = 0$) and a continuum of equilibrium trajectories along with the value of money converges to zero.

Monetary Equilibrium



Efficiency

Proposition 3: with costly money creation the amount produced on the DM is smaller than in case of costly money provision and smaller than the efficient amount

$$\bar{\gamma} = 1 - \psi < \gamma^{nc} = 1$$

$$\sigma \frac{u'(q_t)}{w'(q_t)} + 1 - \sigma = \frac{1}{\beta \gamma_{t+1}}$$

$u'(q)$ is decreasing, $w'(q)$ is increasing

$$\bar{q} < q^{nc} < q*$$

Government

$$G = 2\tau_t + \phi_t(M_t^G - M_{t-1}^G)$$

Government can provide money at no costs.

Public and private money are perfect substitutes.

Under a constant money growth rule $M_t^G = (1+g)M_{t-1}^G$:

$$\text{CM: } X_t = n_t^s + n_t^b - 2\tau_t$$

$$\text{DM: } q_t$$

Mixed Symmetric Equilibrium

$$m_t^G \equiv M_t^G \phi_t^G, b_t = M_t \phi_t$$

$$m_t^G = (1+g)\gamma_t m_{t-1}^G$$

$$(1-\psi) b_t = \gamma_t b_{t-1}$$

$$z(\gamma_{t+1}) = m_t^G + b_t$$

$$2\tau_t = G - \gamma_t^G g m_{t-1}^G$$

$$b \geq 0, m_t \geq 0, 0 \leq \gamma_t \leq \beta^{-1} \ \forall t$$

Mixed Symmetric Equilibrium

$$m_t^G \equiv M_t^G \phi_t^G, b_t = M_t \phi_t$$

$$m_t^G = (1+g)\gamma_t m_{t-1}^G$$

$$(1-\psi) b_t = \gamma_t b_{t-1}$$

$$z(\gamma_{t+1}) = m_t^G + b_t$$

$$2\tau_t = G - \gamma_t^G g m_{t-1}^G$$

$$b \geq 0, m_t \geq 0, 0 \leq \gamma_t \leq \beta^{-1} \ \forall t$$

Mixed equilibrium ($b_t > 0, m_t^G > 0,\ b_t = m_t^G$):

$$\gamma = 1 - \psi, \qquad 1 + g = \frac{1}{1-\psi} = 1 + \pi$$

Mixed Equilibrium

$$\gamma = 1 - \psi, \qquad 1 + g = \frac{1}{1-\psi} = 1 + \pi \qquad \gamma = \gamma^G$$

$$M_t = \frac{1}{1-\psi} M_{t-1}, \qquad M_t^G = (1+g) M_{t-1}^G$$

- Maximum on the sustainable level of inflation in gov.money is positive and depends on costs, $g \leq \frac{\psi}{1-\psi}$. $g^{max}(\psi)$ convex
- Shocks to electricity prices affect government seigniorage
- Gov.money supply grows at the same rate as private money.
- Government can drive private money out of circulation by setting positive g lower than in mixed equilibrium

Efficiency

From bargaining:

$$\sigma \frac{u'(q_t)}{w'(q_t)} + 1 - \sigma = \frac{\phi_t}{\beta \phi_{t+1}} = \frac{1}{\beta \gamma_{t+1}}$$

Note:

- $\bar{q}$ is suboptimal
- if $\gamma_{t+1} = \frac{\phi_{t+1}}{\phi_t} = \beta^{-1}$ then $\bar{q} = q^*$ (efficient allocation is achieved by Friedman rule)

Friedman Rule

$\gamma_{t+1} = \frac{\phi_{t+1}}{\phi_t} = \beta^{-1}$ corresponds to the efficient allocation (Friedman rule)

$$\gamma_{t+1} = \frac{1}{1 + \pi_{t+1}}$$

which means $\pi = \beta - 1$ and $1 + i = (1 + r)(1 + \pi) - 1$ so $i = 0$

Friedman Rule

$\gamma_{t+1} = \frac{\phi_{t+1}}{\phi_t} = \beta^{-1}$ corresponds to the efficient allocation (Friedman rule)

$$\gamma_{t+1} = \frac{1}{1 + \pi_{t+1}}$$

which means $\pi = \beta - 1$ and $1 + i = (1 + r)(1 + \pi) - 1$ so $i = 0$

Proposition 4: efficient allocation on DM is achieved by the standard Friedman rule. It corresponds to growing price of money (deflation of prices and shrinking money supply).

Friedman Rule

$\gamma_{t+1} = \frac{\phi_{t+1}}{\phi_t} = \beta^{-1}$ corresponds to the efficient allocation (Friedman rule)

$$\gamma_{t+1} = \frac{1}{1 + \pi_{t+1}}$$

which means $\pi = \beta - 1$ and $1 + i = (1 + r)(1 + \pi) - 1$ so $i = 0$

Proposition 4: efficient allocation on DM is achieved by the standard Friedman rule. It corresponds to growing price of money (deflation of prices and shrinking money supply).

DM allocation is unaffected by money provision costs

Friedman (1969) interest rate should be equal to public costs of money creation

Welfare

$$G = 2\tau_t + \phi_t(M_t^G - M_{t-1}^G),\ g \leq \frac{\psi}{1-\psi},\ M_t^G = (1+g)M_{t-1}^G$$

CM: $X_t = n_t^s + n_t^b - 2\tau_t$ and DM: q_t

$$W^{mix} = \sum_0^\infty \beta^t \left(X_t - 2\tau_t^{mix} + u(\bar{q})\right),\ 2\tau_t^{mix} = G - \frac{\psi}{1-\psi}(1-\psi)m_{t-1}$$

$$W^G = \sum_0^\infty \beta^t \left(X_t - 2\tau_t^G + u(q^G)\right),\ 2\tau_t^G = G - g\frac{1}{1+g}m_{t-1}$$

$$W^F = \sum_0^\infty \beta^t \left(X_t - 2\tau_t^F + u(q^*)\right),\ 2\tau_t^F = G + (1-\beta)\frac{1}{\beta}m_{t-1}$$

Conclusion

1. Equilibrium path features constant positive inflation and positive constant money growth rate (to compensate for the costs). Constant price equilibrium does not exist
2. Level of production and trade is suboptimal compared to zero costs equilibrium
3. Regardless of the costs of money provision there exist a continuum of equilibrium trajectories at which money become useless and no trade occurs

Conclusion

4. Competition from private currencies imposes a maximum sustainable level for inflation which depends on mining costs
5. Government can drive private money out of circulation even with a positive inflation
6. System with solely government money is not necessarily welfare superior to the mixed monetary system
7. Regardless of the costs of money provision standard Friedman rule ($\pi = \beta - 1 < 0$) applies
8. Mining costs are internalized by miners - do not have a direct welfare effect

Thank you for your attention!

Decentralized monetary system (protocol)

Crypto-currency functions on the base of a blockchain protocol

Decentralized monetary system (protocol)

Crypto-currency functions on the base of a blockchain protocol

1. Pushed transactions are legal (C: "A $\rightarrow$ B")

Decentralized monetary system (protocol)

Crypto-currency functions on the base of a blockchain protocol

1. Pushed transactions are legal (C: "A $\rightarrow$ B")
   - Electronic signature (see public-private key encryption)

Decentralized monetary system (protocol)

Crypto-currency functions on the base of a blockchain protocol

1. Pushed transactions are legal (C: "A $\rightarrow$ B")
   - Electronic signature (see public-private key encryption)
2. Common history of payments ("A $\rightarrow$ B" and "A $\rightarrow$ C")

Decentralized monetary system (protocol)

Crypto-currency functions on the base of a blockchain protocol

1. Pushed transactions are legal (C: "A $\rightarrow$ B")
   - Electronic signature (see public-private key encryption)
2. Common history of payments ("A $\rightarrow$ B" and "A $\rightarrow$ C")
   - Public chain (of blocks) of transactions with time stamps (see hashing)

Decentralized monetary system (protocol)

Crypto-currency functions on the base of a blockchain protocol

1. Pushed transactions are legal (C: "A $\rightarrow$ B")
   - Electronic signature (see public-private key encryption)
2. Common history of payments ("A $\rightarrow$ B" and "A $\rightarrow$ C")
   - Public chain (of blocks) of transactions with time stamps (see hashing)
3. Double spending (add lots of transactions simultaneously)

Decentralized monetary system (protocol)

Crypto-currency functions on the base of a blockchain protocol

1. Pushed transactions are legal (C: "A $\rightarrow$ B")
   - Electronic signature (see public-private key encryption)
2. Common history of payments ("A $\rightarrow$ B" and "A $\rightarrow$ C")
   - Public chain (of blocks) of transactions with time stamps (see hashing)
3. Double spending (add lots of transactions simultaneously)
   - Adding blocks is costly and takes time (see mining)

Decentralized monetary system (protocol)

Crypto-currency functions on the base of a blockchain protocol

1. Pushed transactions are legal (C: "A $\rightarrow$ B")
   - Electronic signature (see public-private key encryption)
2. Common history of payments ("A $\rightarrow$ B" and "A $\rightarrow$ C")
   - Public chain (of blocks) of transactions with time stamps (see hashing)
3. Double spending (add lots of transactions simultaneously)
   - Adding blocks is costly and takes time (see mining)
4. Intrusion (Eve against a network)

Decentralized monetary system (protocol)

Crypto-currency functions on the base of a blockchain protocol

1. Pushed transactions are legal (C: "A $\rightarrow$ B")
   - Electronic signature (see public-private key encryption)
2. Common history of payments ("A $\rightarrow$ B" and "A $\rightarrow$ C")
   - Public chain (of blocks) of transactions with time stamps (see hashing)
3. Double spending (add lots of transactions simultaneously)
   - Adding blocks is costly and takes time (see mining)
4. Intrusion (Eve against a network)
   - Adding blocks is costly and takes computational power (see mining)

Decentralized monetary system (protocol)

Crypto-currency functions on the base of a blockchain protocol

1. Pushed transactions are legal (C: "A $\rightarrow$ B")
   - Electronic signature (see public-private key encryption)
2. Common history of payments ("A $\rightarrow$ B" and "A $\rightarrow$ C")
   - Public chain (of blocks) of transactions with time stamps (see hashing)
3. Double spending (add lots of transactions simultaneously)
   - Adding blocks is costly and takes time (see mining)
4. Intrusion (Eve against a network)
   - Adding blocks is costly and takes computational power (see mining)

Miners receive a reward for adding blocks = money supply growth

Costly money creation: Ideas

- Linear costs (more blocks more energy)
- Probabilistic function: money unit is created with probability $\sigma(CU_t)$, which positively depends on individual computational power (CPU), CPUs are costly
- "Matching function" with number of miners in the network being used as inputs. More miners will reduce the probability of success=probability of money creation

Idea 2: Endogenous probability

[0,1] buyers, [0,1] sellers and [0,1] miners

Idea 2: Endogenous probability

[0,1] buyers, [0,1] sellers and [0,1] miners

CM and DM. DM is anonymous. Sellers randomly assigned to buyers (every agent is in a pair). They see each other once and never again.

Trade and money transaction happens with probability $\sigma_t(\cdot)$

Idea 2: Endogenous probability

[0,1] buyers, [0,1] sellers and [0,1] miners

CM and DM. DM is anonymous. Sellers randomly assigned to buyers (every agent is in a pair). They see each other once and never again.

Trade and money transaction happens with probability $\sigma_t(\cdot)$

$\sigma(\cdot)$ depends on the computational units the miner can offer (CPU/GPU) and the total network computational power. Using CPU involves energy costs.

Idea 2: Endogenous probability

[0,1] buyers, [0,1] sellers and [0,1] miners

CM and DM. DM is anonymous. Sellers randomly assigned to buyers (every agent is in a pair). They see each other once and never again.

Trade and money transaction happens with probability $\sigma_t(\cdot)$

$\sigma(\cdot)$ depends on the computational units the miner can offer (CPU/GPU) and the total network computational power. Using CPU involves energy costs.

Miners decide on how many CPUs to use depending on the energy price and money price.

Idea 2: Endogenous probability

[0,1] buyers, [0,1] sellers and [0,1] miners

CM and DM. DM is anonymous. Sellers randomly assigned to buyers (every agent is in a pair). They see each other once and never again.

Trade and money transaction happens with probability $\sigma_t(\cdot)$

$\sigma(\cdot)$ depends on the computational units the miner can offer (CPU/GPU) and the total network computational power. Using CPU involves energy costs.

Miners decide on how many CPUs to use depending on the energy price and money price.

Miners are rational agents that maximize profit (commitment device)

Idea 2: Miner's Problem

$$\max_{\{x\}_t} \sum_{t=0}^{\infty} \beta^t x_t^M$$

$$\text{s.t. } x_t^M = \sigma(CU_t)\phi_t(M_t - M_{t-1}) - \psi CU_t, \; x_t^M \geq 0$$

$$\sigma(0) = 0, \sigma(\cdot) > 0, \; \sigma'(\cdot) > 0 \text{ and } \sigma''(\cdot) < 0, \lim_{CU_t \to \infty} \sigma(CU_t) = 1$$

Idea 2: Miner's Problem

$$\max_{\{x\}_t} \sum_{t=0}^{\infty} \beta^t x_t^M$$

$$\text{s.t. } x_t^M = \sigma(CU_t)\phi_t(M_t - M_{t-1}) - \psi CU_t,\ x_t^M \geq 0$$

$$\sigma(0) = 0, \sigma(\cdot) > 0,\ \sigma'(\cdot) > 0 \text{ and } \sigma''(\cdot) < 0, \lim_{CU_t \to \infty} \sigma(CU_t) = 1$$

$M_t - M_{t-1} = \sigma(CU_t)\omega$ - fixed reward for a miner

Idea 2: Miner's Problem

$$\max_{\{x\}_t} \sum_{t=0}^{\infty} \beta^t x_t^M$$

$$\text{s.t. } x_t^M = \sigma(CU_t)\phi_t(M_t - M_{t-1}) - \psi CU_t,\ x_t^M \geq 0$$

$$\sigma(0) = 0, \sigma(\cdot) > 0,\ \sigma'(\cdot) > 0 \text{ and } \sigma''(\cdot) < 0, \lim_{CU_t \to \infty} \sigma(CU_t) = 1$$

$M_t - M_{t-1} = \sigma(CU_t)\omega$ - fixed reward for a miner

$$\sum_{t=0}^{\infty} \beta^t \phi_t \omega \sigma(CU_t) - \psi CU_t$$

$$\phi_t \omega \sigma'(CU_t) - \psi = 0$$

Idea 2: Miner's Problem

$$\max_{\{x\}_t} \sum_{t=0}^{\infty} \beta^t x_t^M$$

$$\text{s.t. } x_t^M = \sigma(CU_t)\phi_t(M_t - M_{t-1}) - \psi CU_t,\ x_t^M \geq 0$$

$$\sigma(0) = 0, \sigma(\cdot) > 0,\ \sigma'(\cdot) > 0 \text{ and } \sigma''(\cdot) < 0, \lim_{CU_t \to \infty} \sigma(CU_t) = 1$$

$M_t - M_{t-1} = \sigma(CU_t)\omega$ - fixed reward for a miner

$$\sum_{t=0}^{\infty} \beta^t \phi_t \omega \sigma(CU_t) - \psi CU_t$$

$$\phi_t \omega \sigma'(CU_t) - \psi = 0$$

ψ increase - less mining; ϕ_t increase - more mining, M depends on ϕ_t!

Miner (N miners indexed by i)

$$\max_{\{x^i\}_t} \sum_{t=0}^{\infty} \beta^t x_t^i$$

$$\text{s.t. } x_t^i = \phi_t(M_t^i - M_{t-1}^i) - \psi\phi_t M_t^i$$

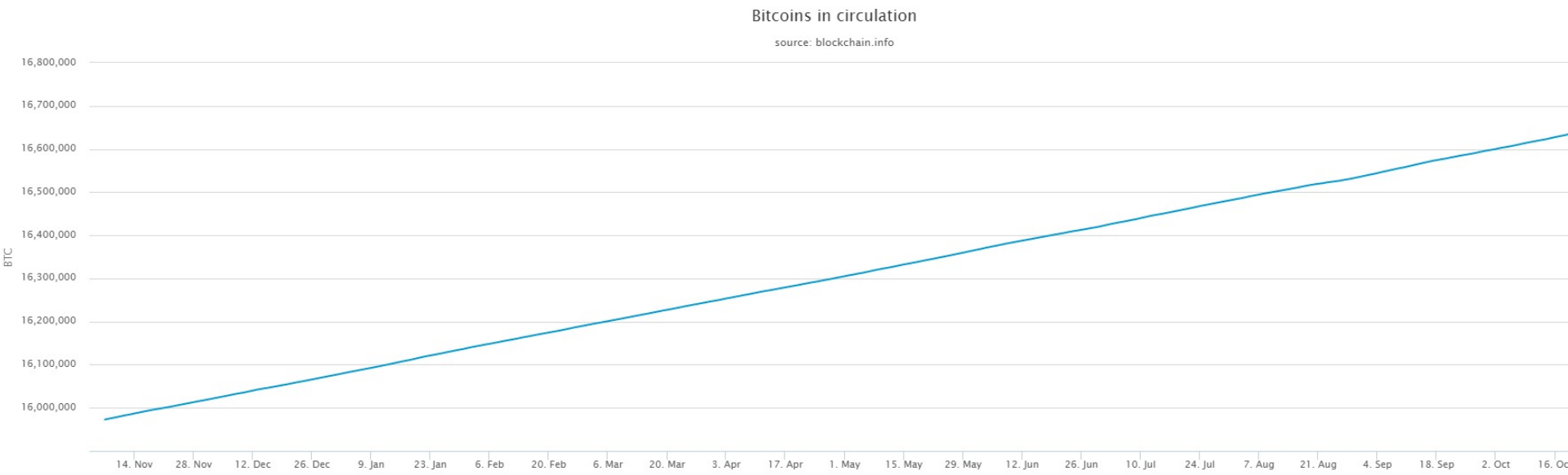
$$M_t^i(1-\psi) - M_{t-1}^i = 0 \ \forall t$$

from consumption non-negativity and free entry.

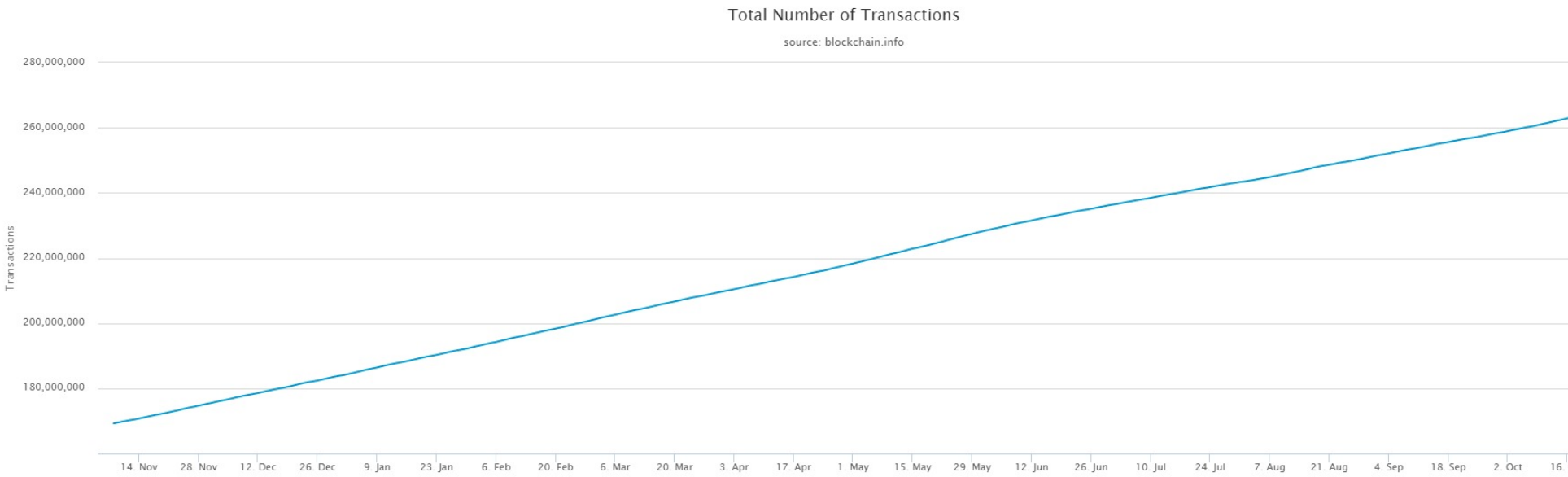
Perfect substitutes: returns to different currencies are equalized

The same cost function: market share of every miner is 1/N

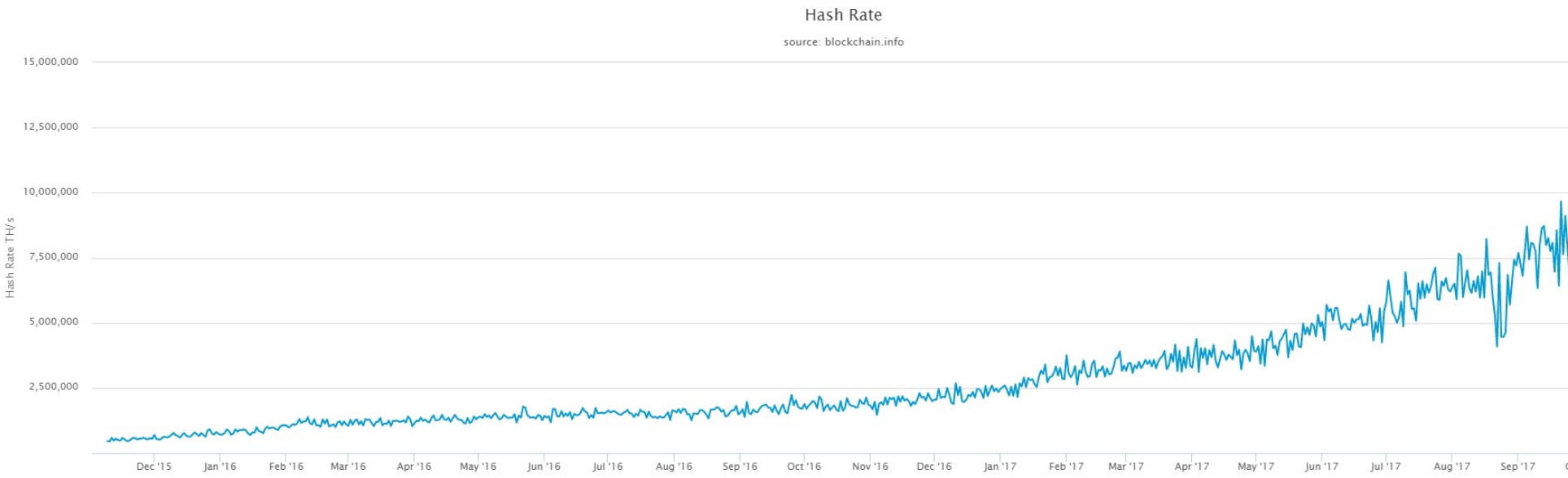
BTC in circulation

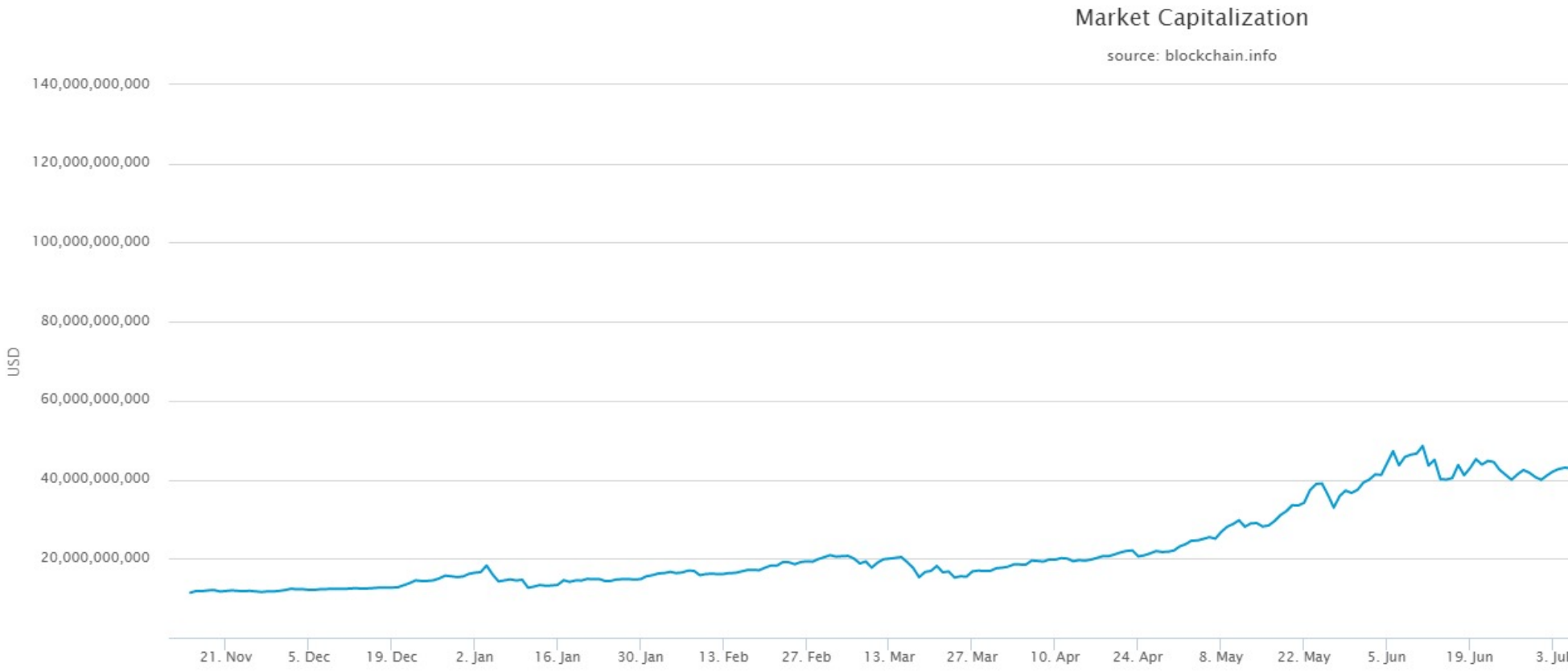


BTC transactions



BTC hash rate




Market Capitalization
source: blockchain.info
USD
140,000,000,000
120,000,000,000
100,000,000,000
80,000,000,000
60,000,000,000
40,000,000,000
20,000,000,000
21. Nov
5. Dec
19. Dec
2. Jan
16. Jan
30. Jan
13. Feb
27. Feb
13. Mar
27. Mar
10. Apr
24. Apr
8. May
22. May
5. Jun
19. Jun
3. Jul