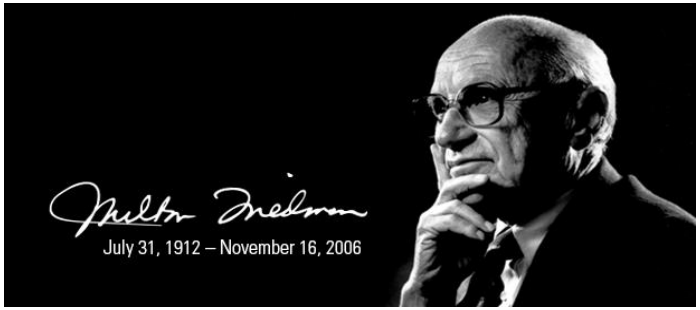
Всё, что вы хотели знать про блокчейн и криптовалюты, но боялись спросить

Сергей Ивлиев, руководитель лаборатории криптоэкономики
и блокчейн-систем экономического факультета ПГНИУ

Андрей Клименко, основатель ИТ-компаний Teleport и PiratePay

“Интернет станет одной из основных сил, способствующих снижению роли государства. Единственная вещь, которая отсутствует, но которая вскоре будет разработана, это надежные цифровые деньги”

Милтон Фридман, Лауреат Нобелевской премии по экономике (1999)



“С цифровой валютой, основанной на криптографическом подтверждении, и не требующей центрального доверенного посредника, деньги станут безопасными, а транзакции не требующими усилий”

Сатоши Накамото, создатель биткойна (2009)

“В целом финансовые транзакции станут дешевле...

Нам нужно развивать технологии на основе революции биткойна, одного биткойна не достаточно”

Бил Гейтс (2015)

“Я считаю блокчейн исключительно перспективной технологией.

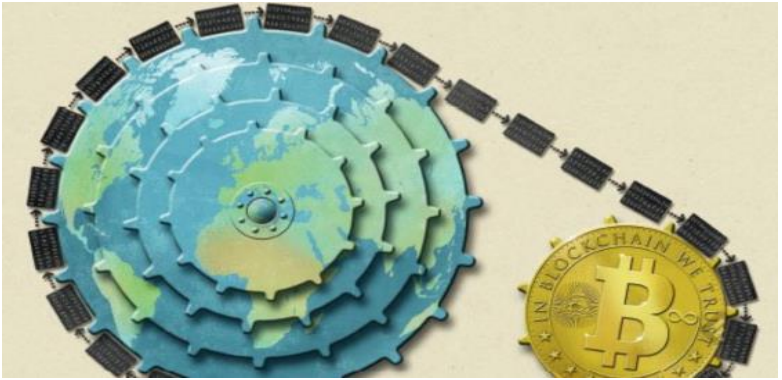
Через два-три года мало останется сфер, где бы она радикально не изменила вообще основы бизнес-модели”

Герман Греф (2016)

https://rns.online/finance/Gref-ozhidaet-chto-cherez-dva-tri-goda-blokchein-radikalno-izmenit-mnogie-biznes-modeli-2016-06-08/

“Технология в основе биткойна позволит людям, которые не знают или не доверяют другу осуществлять транзакции. Применение этого выходит далеко за рамки криптовалют”

The Economist «The great chain of being sure about things»



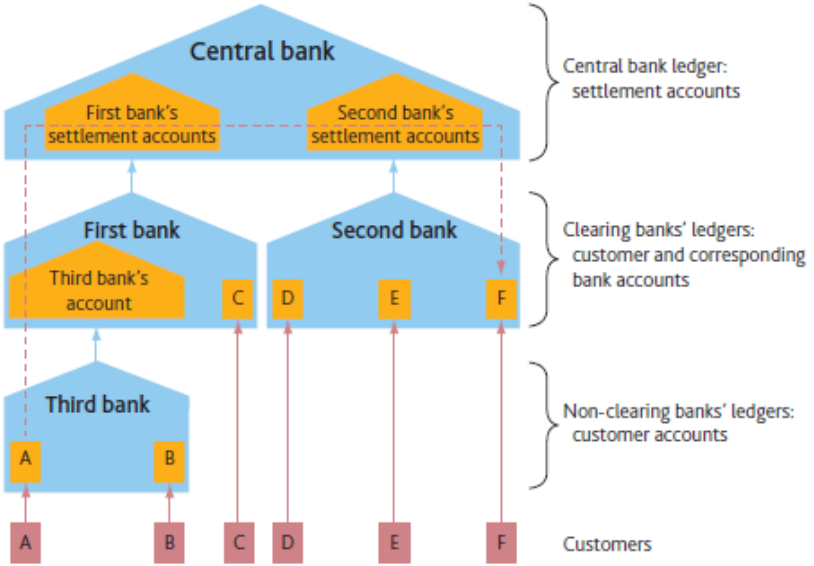
http://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable

58% экспертов ожидают, что биткойн и блокчейн станут мейнстримом, и будут обслуживать до 10% мирового ВВП к 2025 году

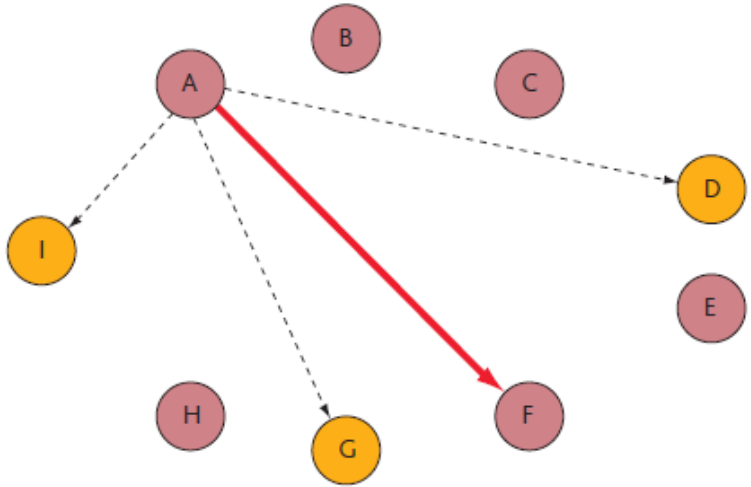
WEF «Deep Shift: Technology Tipping Points and Societal Impact»

http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf

Централизованная vs. Распределенная



Централизованная платежная система



Децентрализованная платежная система

Bitcoin: A Peer-to-Peer Electronic Cash System

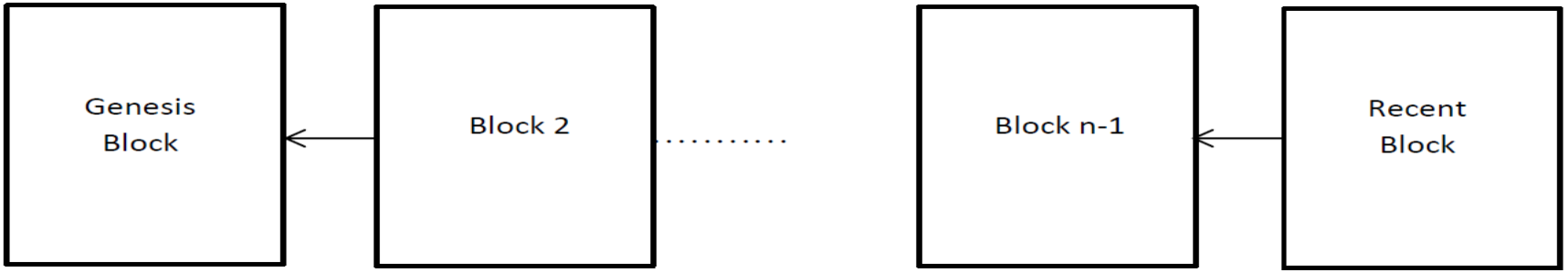
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

https://bitcoin.org/bitcoin.pdf

- Биткойны существуют в электронном виде
- Криптография используется при отправке и подтверждении транзакций:
  - Транзакции должны быть подписаны закрытым ключом
    - например, L4FHDBRN6Egz4kch3GZBcEoAucQGX2iBci4Ld7iNXjQ7V8fjkMH4
  - Для получения применяется открытый ключ (адрес)
    - например, akFHMX1KJGbCN1niSXFu6MKv7KCrezKDRVn

- Все данные хранятся всеми узлами сети
- Каждый узел содержит копию реестра транзакций (блокчейн)
- Блокчейн – цепочка блоков, содержащих информацию о транзакциях:
  - отправитель, получатель, количество, метаданные
- Каждый блок содержит ссылку на предыдущий блок



- Работает без единого центра
- Невозможно изменить прошлое
- Каждый может принять участие
- Доверие строится на криптографии и экономических принципах

- Сколько стоит 1 биткоин?

- Кто этим пользуется?

GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Tue Aug 01 2017 04:33:03 GMT+0500 (Russia TZ 4 Standard Time).

8715 NODES

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	2583 (29.64%)
2	Germany	1537 (17.64%)
3	France	597 (6.85%)
4	Netherlands	465 (5.34%)
5	Canada	358 (4.11%)
6	United Kingdom	320 (3.67%)
7	Russian Federation	312 (3.58%)
8	n/a	293 (3.36%)
9	China	264 (3.03%)
10	Singapore	153 (1.76%)

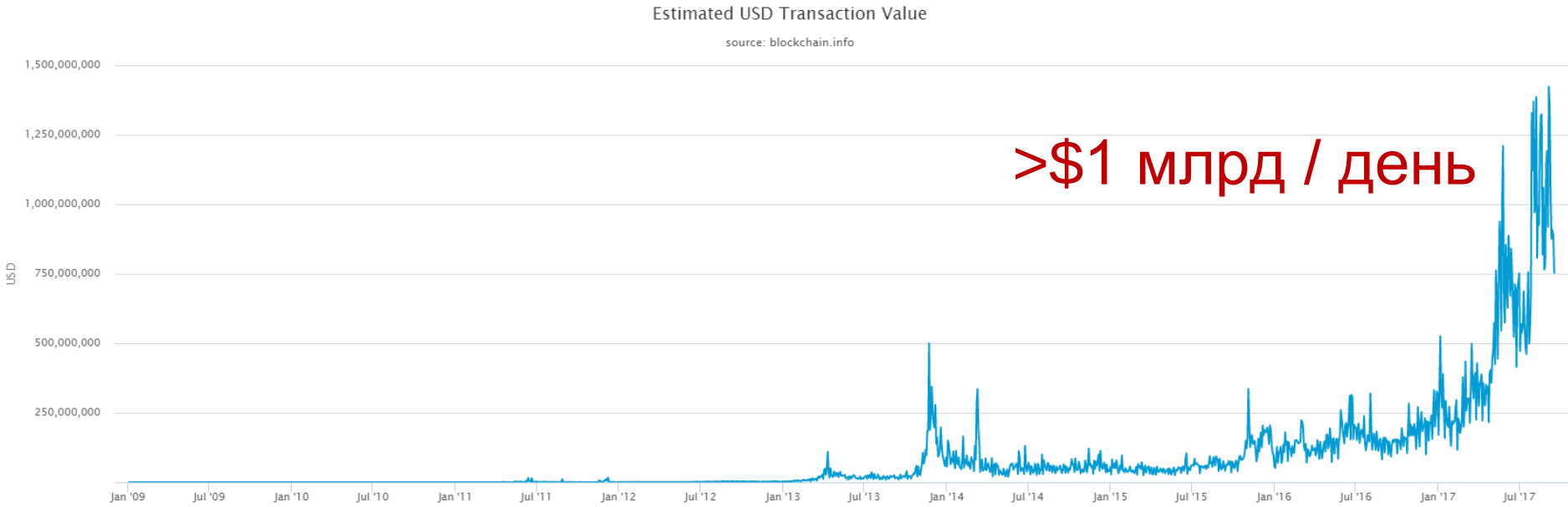
More (91) »

>10 млн. пользователей

Map shows concentration of reachable Bitcoin nodes found in countries around the world.

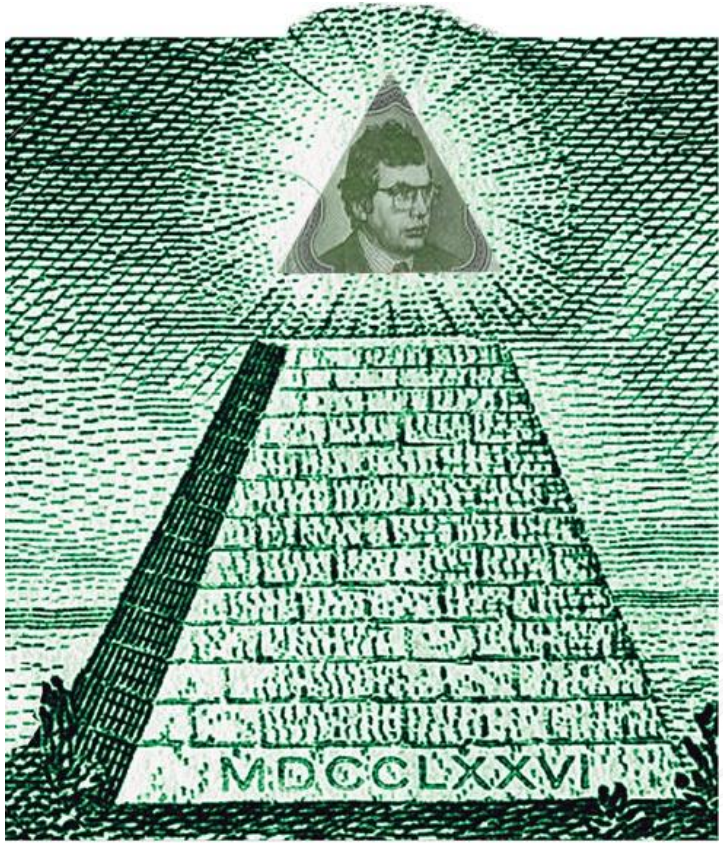
LIVE MAP

- Какая стоимость пересылается?



- Чем эта стоимость подтверждается?

- Пирамида ли это?



- Пузырь ли это?

- Что кроме биткойна?
  - Смарт-контракты (Ethereum)
  - Регистрация активов (NEM, NEO, Waves, NXT)
  - Интернет вещей / Экономика вещей (IOTA, Lisk)
  - Распределенные соц.медиа (Steem, Synereo)
  - Системы распределенного хранения данных и облачных вычислений (MaidSafe, Golem, SONM)
  - Рынки прогнозирования (Augur, Gnosis)
  - Распределенные автономные организации (Aragon)

“Блокчейн может изменить всё. От банкинга и платежей, до нотариата, систем голосования, реестров автомобилей, оружия и университетских дипломов, расчетов на рынке ценных бумаг, каталогов произведения искусства, распределенный реестр имеет потенциальную возможность сделать транзакции быстрее, дешевле и безопаснее”

Goldman Sachs - Emerging Theme Radar
http://www.goldmansachs.com/our-thinking/pages/macroeconomic-insights-folder/what-if-i-told-you/report.pdf

Что почитать?

- Bank of England – The emergence of digital currencies (2014)
  http://www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q3digitalcurrenciesbitcoin1.pdf

- WEF – The future of financial infrastructure (Aug 2016)
  http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf

- Lykke Exchange White Paper
  https://lykke.com/ico/Whitepaper_LykkeExchange.pdf