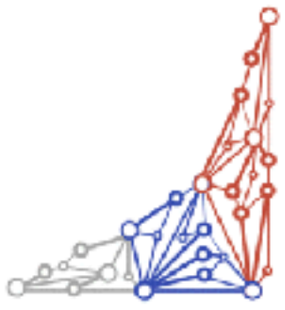


Financial
University's
blockchain
laboratory

Варнавский
Андрей
Владимирович

Блокчейн

FinTech 2018

Financial University's blockchain laboratory

Технократическая утопия.

FinTech 2018

Financial University's blockchain laboratory

«Утопии страшны тем, что они сбываются», - Н. Бердяев

- беспилотный атомобиль
  https://youtu.be/Bx08yRsR9ow
- MIT курс Introduction to Computer Science and Programming Using Python
  https://www.edx.org/course/introduction-computer-science-mitx-6-00-1x-11
- сельскохозяйственные роботы
  https://youtu.be/MRbGbNrqvLk?t=2m55s
- холодильник
  https://ichip.ru/samsung-family-hub-kholodilnik-s-wi-fi-kamerami-i-ehkranom.html
- дрон
  https://youtu.be/lBWHx86Hzl0

Вводная в блокчейн.

Вводная в блокчейн.

Financial University's
BlockchainLab

Транзакция
(Transaction)

адрес

1Seatd3tr**IVAN**4f2B2eUduYXmcM4U9jDoc

хочу переслать **3 BTC**

по адресу

1FgzTPb**ELENA**pfF6VxPdmDoLPhinygut2A

Financial University's
BlockchainLab

Транзакция
(Transaction)

адрес

1Seatd3tr**IVAN**4f2B2eUduYXmcM4U9jDoc

публичный ключ 1

хочу переслать **3 BTC**

по адресу

1FgzTPb**ELENA**pfF6VxPdmDoLPhinygut2A

публичный ключ 2

Financial University's BlockchainLab

Транзакция
(Transaction)

адрес

1Seatd3tr**IVAN**4f2B2eUduYXmcM4U9jDoc

хочу переслать **3 BTC**

по адресу

1FgzTPb**ELENA**pfF6VxPdmDoLPhinygut2A

кошелек

проверка их взаимосвязи

приватный ключ 1

публичный ключ 1

публичный ключ 2

Financial University's
BlockchainLab

Транзакция
(Transaction)

адрес

1Seatd3tr**IVAN**4f2B2eUduYXmcM4U9jDoc

публичный ключ 1

хочу переслать **3 BTC**

приватный ключ 1

по адресу

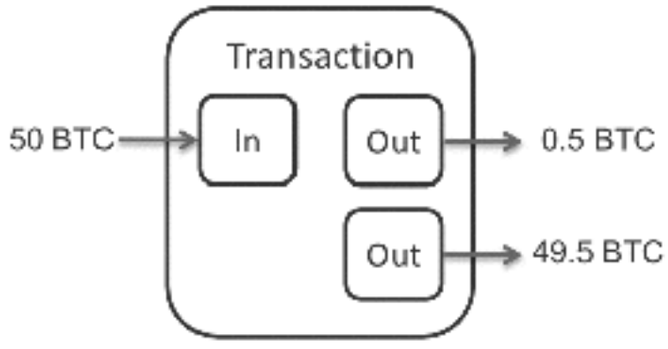
1FgzTPb**ELENA**pfF6VxPdmDoLPhinygut2A

публичный ключ 2

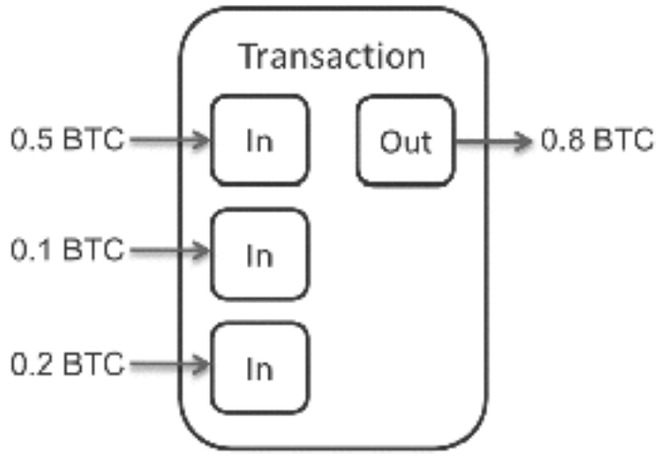
Financial University's
BlockchainLab

Транзакция
(Transaction)

инпут-аутпут



инпут-аутпут



Вводная в блокчейн.

Financial University's
BlockchainLab

Блок
(Block)

адрес1Seatd3tr**IVAN**4f2B2eUduYXmcM4U9jDocхочупереслать
3BTCпоадресу1FgzTPb**ELENA**pfF6VxPdmDoLPhinygut2A....a
дрес1Seatd3tr**PETR**4f2B2eUduYXmcM4U9jDocхочупереслать
30BTCпоадресу1FgzTPb**SEMEN**pfF6VxPdmDoLPhinygut2A

2eUWYfF6duYXmcM4U9jp1KeatDCtrEEeER42B2eUduYXmcM4
U9jphDfF6duYVxPdm1FTgzPJCbpCWYfF6VxPdmCMDDDBfygut
2AVxPdmp1KeatDCtr

Вводная в блокчейн.

Financial University's
BlockchainLab

Блок -> Цепь

(Block -> Chain)

2eUWYfF6duYXmcM4U9jp1KeatDCtrEEeER42B2eUduYXmc
M4U9jphDfF6duYVxPdm1FTgzPJCbpCWYfF6VxPdmCMDD
DBfygut2AVxPdmp1KeatDCtr

КЛЮЧ

(transactions + nonce) < target, где target->0

Вводная в блокчейн.

Financial University's
BlockchainLab

Блок -> Цепь

(Block -> Chain)

2eUWYfF6duYXmcM4U9jp1KeatDCtrEEeER42B2eUduYXmcM4U9jphDfF6duYVxPdm1FTgzPJCbpCWYfF6VxPdmCMDDDBfygut2AVxPdmp1KeatDCtr	ключ1
M4U9jp1KeatDCtrEEeER42B2eUduYXmcM4U9jphDfF6duYVx2eUWYfF6duYXgzPJCbpCWYfF6VxPdmCdmp1KeatDCtrMDmcPdm1FTDDBfygut2AVxP	ключ2

Вводная в блокчейн.

Financial University's
BlockchainLab

Блок -> Цепь

(Block -> Chain)

Financial University's
BlockchainLab

Вводная в блокчейн.

Блок -> Цепь

(Block -> Chain)

. . .

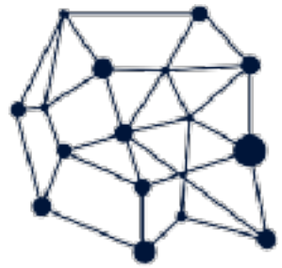
СВОЙСТВО
(BlockChain)

невозможность
подмены данных
в прошлом

Вводная в блокчейн.

Financial University's
BlockchainLab

Распределенный реестр
(distributed ledger)



публичность
свойство
(BlockChain)

невозможность
подмены данных
незаметно

распределенность
свойство
(BlockChain)

стабильная
работа
системы

Financial University's
BlockchainLab

Вводная в блокчейн.

https://coinmarketcap.com

Bitcoin 6 303,03 US$ 17,317,950 BTC 21 million BTC

Блок -> Шахтер XXI века

(Block -> Miner)

50 BTC
25 BTC at block 210000
12.5 BTC at block 420000
0 satoshi with block 6930000

78 787,88 US$

+ transaction
fee

Financial University's
BlockchainLab

https://www.blockchain.com/ru/explorer

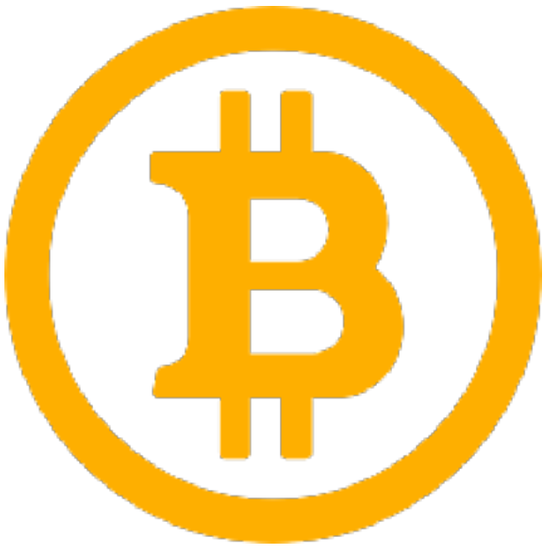
Блок #545436

Сводные данные	
Количество транзакций	2988
Всего выходов	16,839.0116699 BTC
Предполагаемый объем транзакций	1,004.57116089 BTC
Комиссия за транзакцию	0.17791225 BTC
Высота	545436 (Главная цепочка)
Временная отметка	2018-10-12 08:10:00
Время получения	2018-10-12 08:10:00
Передано по	ViaBTC
Сложность	7,454,966,648,263.24
Биты	386350353
Размер	1214.439 kB
вес	3992.733 kWU
Версия	0x20000000
Nonce (случайно перебираемое число)	1344613772
Награда за блок	12.5 BTC

Вводная в блокчейн.

Financial University's
BlockchainLab

Bitcoin (BTC)



3 января 2009 года был сгенерирован первый блок
сентябре 2009 года — 5050 биткойнов=$5,02

Financial University's
BlockchainLab

Вводная в блокчейн.

24/07/2016

Ethereum (ETH)

Ethereum Classic (ETC)

СВОЙСТВО
(BlockChain)

невозможность
подмены данных
без согласия всех

консенсус

(лат. *consensus* —
согласие,
сочувствие,
единодушие)

$20.74 $11.5 $0.90

Name	Price	Price max
Ethereum	$197.62	$1413.72
Ethereum Classic	$9.52	$45.51

Вводная в блокчейн.

Financial University's
BlockchainLab

01/08/2017

Bitcoin Cash (BCH)

блок 478559 был сформирован дважды в разных форматах:
SegWit2x (часть информации хранить за пределами блокчейна и размер блоков постепенно увеличить до 2 Мб)
Bitcoin Cash (без хранения информации за его рамками, но увеличении размера блока до 8 Мб)

Вводная в блокчейн.

Financial University's
BlockchainLab

Голос/Steem

ГОЛОС

steemit

Вводная в блокчейн.

Financial University's
BlockchainLab

Waves

Financial University's
BlockchainLab

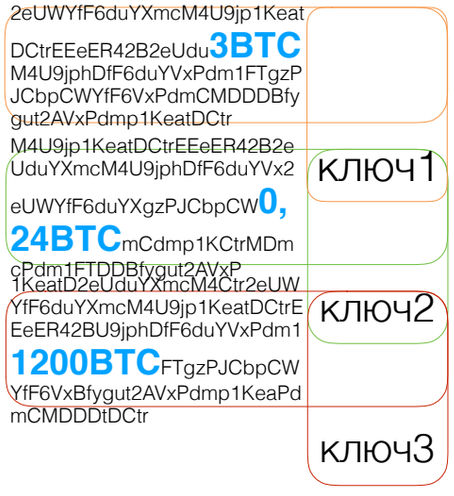
Кто получит деньги?

Proof-of-Work **(PoW)** - доказательство работой
Proof-of-Stake **(PoS)** - доказательство владением
Proof of Autority **(PoA)** - доказательство полномочиями

Вводная в блокчейн.

Financial University's
BlockchainLab

Блокчейн -> Токен/Актив (CryptoAsset)



. . .

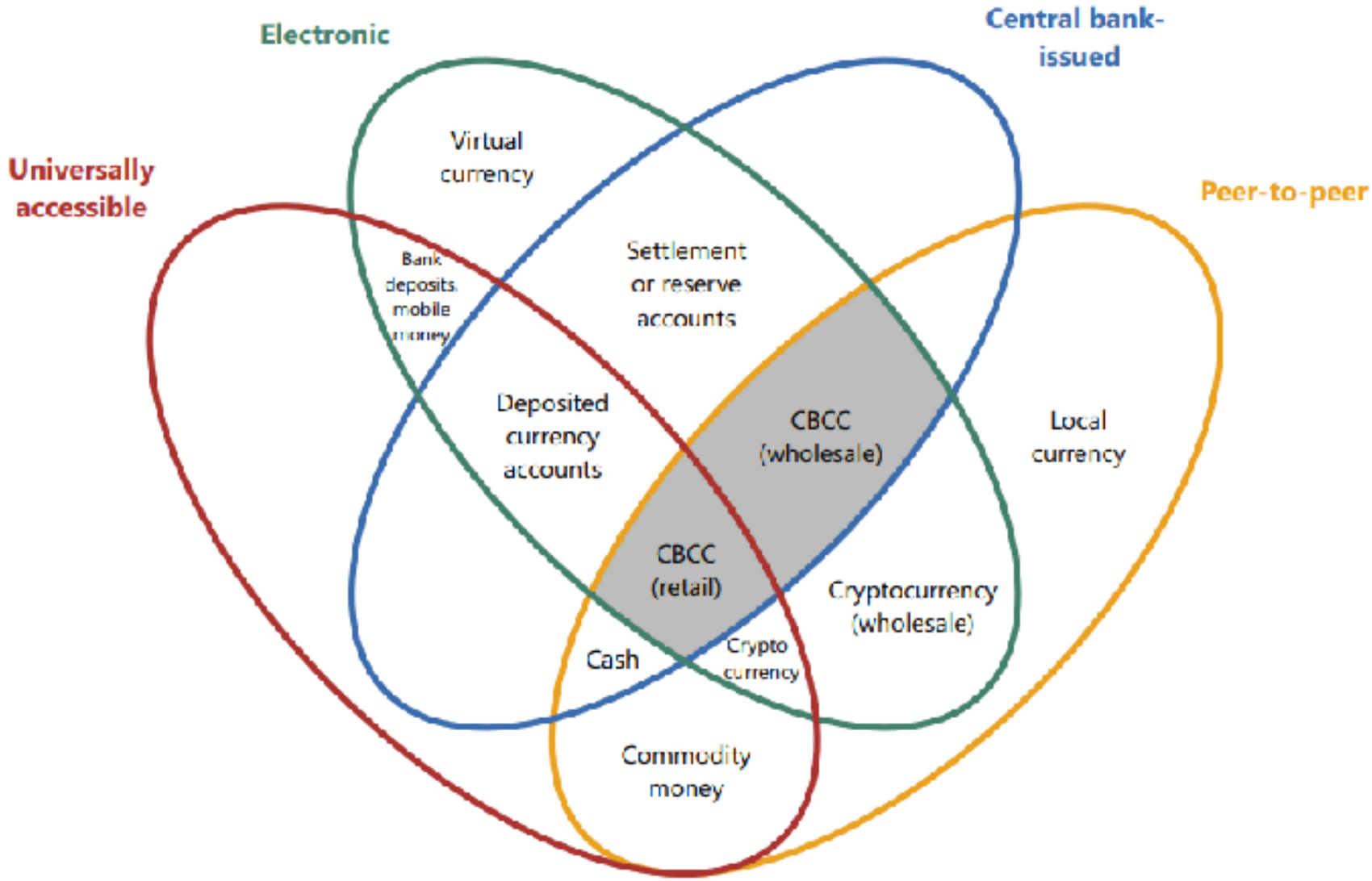
BTC

Вводная в блокчейн.

Financial University's
BlockchainLab

Financial University's
BlockchainLab

денежный цветок



09/2017 года Базельским комитетом по банковскому надзору был выпущен аналитический обзор «Central bank cryptocurrencies»

Financial University's BlockchainLab

	P	Cc	CBCc	PCc	RPCc	TCc
Мера стоимости	+	(+)	+	(+)	(+)	+
Средство обращения	+	(+)	+	(+)	(+)	+
Средство платежа	+	(+)	+	(+)	(+)	+
Средство накопления	+	(+)	+	(+)	(+)	+
Цифровой формат	+	+	+	+	+	+
Свойства Y={crypto}		+	+	+	+	+
Обязательство частного эмитента	+			+	+	+
Наличие ресурса					+	[+]
Обеспечиваются государством			+			

RCC={resource cryptocurrency}

Token Rights

SMITH + CROWN

Digital tokens being sold in ICOs confer a combination of rights to holders

Payment

Token is the only way to make payments on the network

GNT are the only way to pay for services on the network.

Access

Token provide the ability to use the platform itself

LSK is needed to pay transaction fees on the network.

Profit or Fee

Holders get a portion of revenues or profits

Holders of TIME earn the fees from Labour-hour tokens.

Contribution

Tokens needed to play certain roles on the platform or app

1ST allow holders to determine who won gaming matches

Block Creation

Tokens determine who secures the blockchain

KMD holders select the notary nodes who secure the blockchain

Governance

Holders influence features, project direction, protocol details, or more

DGD holders determine how DigixDAO funds are spent

use cases

Страхование:

- P2P страхование (immutable ledger)
- Параметрическое страхование (смарт-контракты)

Financial University's blockchain laboratory

use cases

Здравоохранение:

- Персонализированная медицина (история болезни в блокчейне)
- Хранение результатов клинических испытаний
- Supply chains, контроль качества

Financial University's blockchain laboratory

use cases

Энергетика и коммуналка:

- Управление сетью, децентрализованная генерация энергии.
- P2P торговля энергией («убер» для энергетики)

Financial University's blockchain laboratory

use cases

НРД
Мегафон
>> коммерческие облигации >>
Райффайзенбанка
октябре 2017

МТС
>> полугодовые облигации на 750 млн руб.
с квартальным купоном 6,8% годовых >>
Sberbank CIB
15 мая 2018

Financial University's blockchain laboratory

«Использование смарт-контрактов позволяет обеспечить снижение на 5–10% технологических затрат за счет отсутствия необходимости резервирования данных», — указывает господин управляющий директор по депозитарной деятельности НРД Денис Буряков.

Financial University's blockchain laboratory

«Использование смарт-контрактов позволяет обеспечить снижение на 5–10% технологических затрат за счет отсутствия необходимости резервирования данных», — указывает господин управляющий директор по депозитарной деятельности НРД Денис Буряков.

Financial University's blockchain laboratory

use cases

Полис групп

ДДУ

Financial University's blockchain laboratory

Спасибо за внимание!

Варнавский Андрей Владимирович
кэн, доцент
Заведующий блокчейн-лаборатории
Института развития цифровой экономики
Финансового университета при Правительстве РФ

AVVarnavskiy@fa.ru
facebook.com/avarnavskii

vk.com/avarnavskii

Financial University's blockchain laboratory