Информационные системы электронной коммерции

Доцент Филиппов Ф.В.
E-mail: 9000096@mail.ru

Криптовалюта

По данным CoinMarketCap - Forbes, в мире криптовалют на сегодняшний день существует более 1100 видов цифровых денег. А общая капитализация этого рынка - 133 миллиарда долларов.

Криптовалю́та — разновидность цифровой валюты, создание и контроль за которой базируются на криптографических методах.

Bitcoin — это виртуальная валюта для платежей в интернет-пространстве (bit - единица информации "бит" и coin - "монета"). На официальном сайте она именуется, как «open source P2P digital currency» — «свободная пиринговая цифровая валюта».

Сатоши (10^{-8} биткойна) — минимальная передаваемая величина (наименьшая величина дробления) названа в честь создателя Сатоси Накамото

Биткоин — пиринговая платёжная система, использующая одноимённую единицу для учёта операций и одноимённый протокол передачи данных. Вся информация о транзакциях между адресами системы доступна в открытом виде.

http://ecommercelaw.ru/taxonomy/term/45

Майнинг Криптовалюты
информационно-аналитический портал

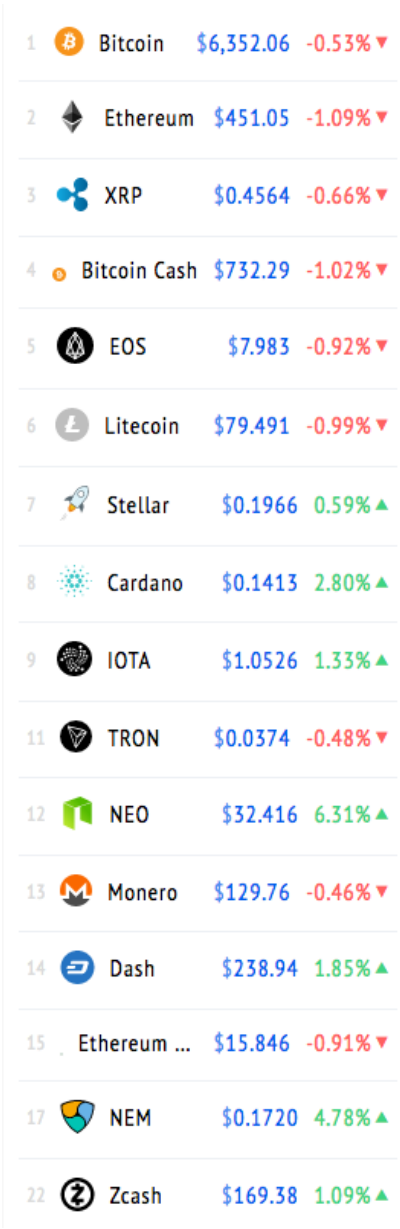
https://mining-cryptocurrency.ru/chto-takoe-kriptovalyuta/

Ключевые особенности криптовалюты:

- ❑ Отсутствует понятие «регистрация», любой может участвовать в сети, Кошелек не привязан к личности пользователя, каждый может создавать неограниченное число кошельков и реквизитов.
- ❑ Дешевые, анонимные и неограниченные денежные переводы по всему миру.
- ❑ Нет никаких посредников, цифровые деньги напрямую пересылаются между пользователями.
- ❑ Невозможно заблокировать перевод, заморозить деньги в кошельке пользователя или «откатить» уже совершенные транзакции.
- ❑ Нет никакой контролирующей организации, цена криптовалюты определяется только рыночным спросом и предложением.

Таким образом, криптовалюта одновременно обладает свойствами обычных наличных денег, электронных валют, системы денежных переводов и «цифрового золота».

Курсы криптовалют онлайн



Биржи криптовалют

https://www.okchanger.ru/trading-platforms

Криптовалюты

https://www.okchanger.ru/cryptocurrencies

Биткоин

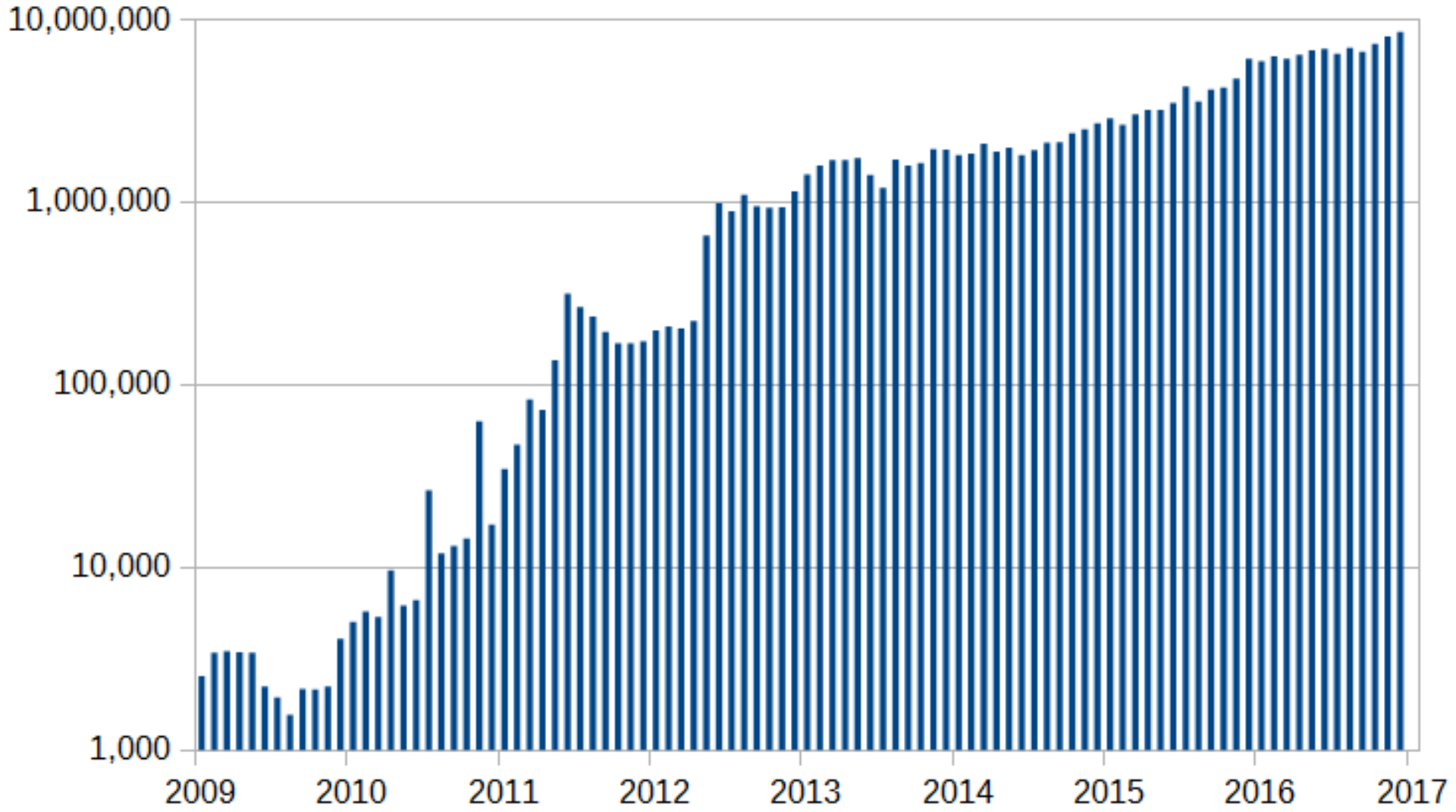
Отличия Bitcoin от обычных денег

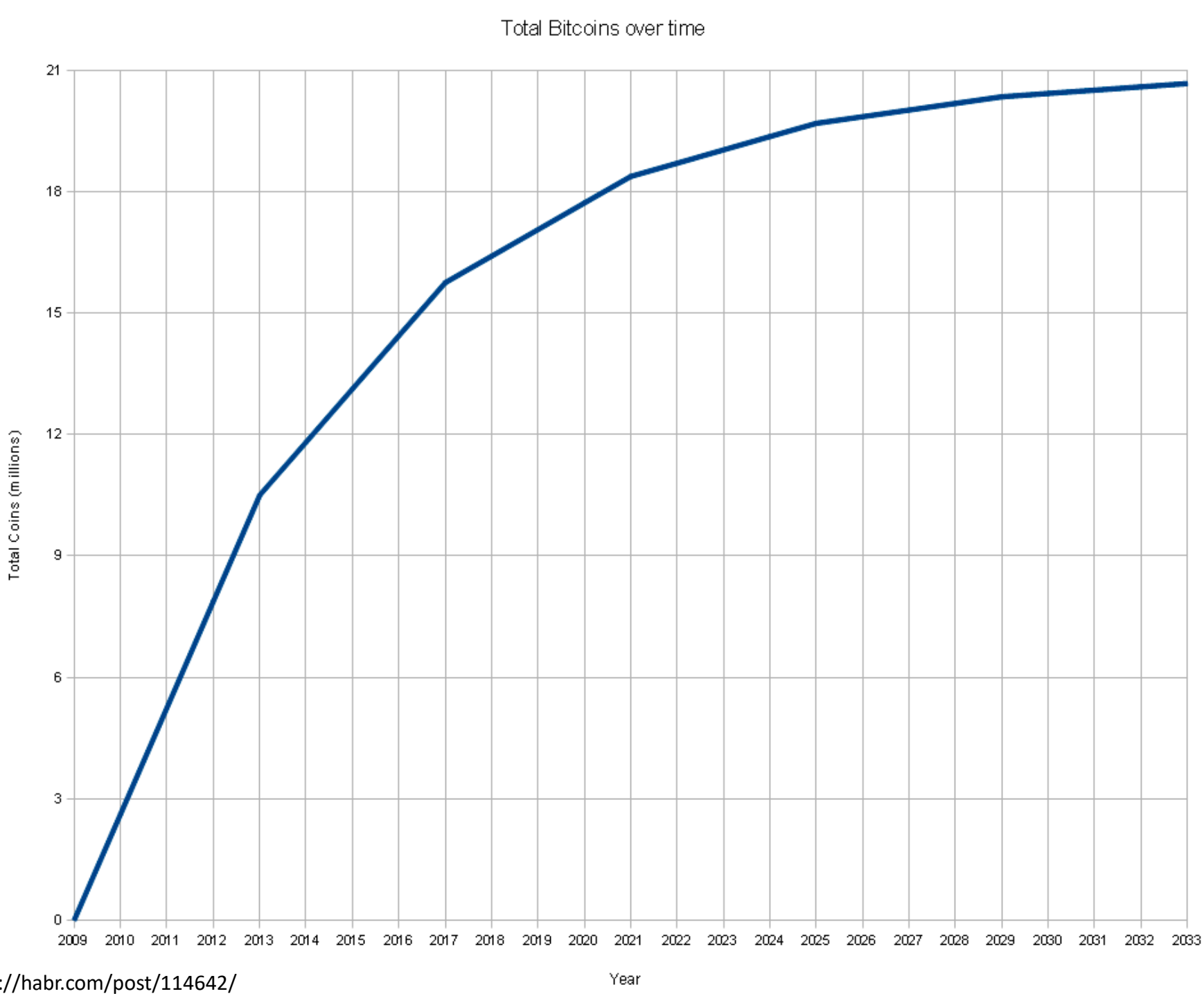
- Теоретическая невозможность инфляции. «Допечатать» еще биткоина не получится даже у создателей системы – их количество заложено на уровне программного кода. Если ранее, возможно, было заниматься созданием новых единиц валюты (майнинг), то сейчас её количество безвозвратно стабилизировалось.
- Отсутствие любых посредников при проведении операций с биткоин: никакой обменник, сервер или другой пользователь не сможет ни случайно, ни намеренно заблокировать перевод или остановить работу системы – BTC не подвержен влиянию извне.
- Децентрализованность означает, что работу системы обеспечивает каждый подключённый к ней компьютер в отдельности – фактически виртуальная валюта будет существовать до того момента, пока работает хотя бы одно устройство. А сейчас в мире их десятки миллионов и число растёт по экспоненте.
- Отсутствие центрального узла, администрации и управления, значит, что никакие законодательные и региональные запреты на интернет-деньги биткоин не действуют – при совершении переводов внутри системы криптовалюта биткоин не поддаётся юрисдикции ни одного государства или частного лица.
- Очень высокое быстродействие. Даже международные переводы занимают до нескольких минут вне зависимости от времени суток и вашего местоположения, а комиссия за одну операцию минимальна. В этом компоненте электронная валюта биткоин не имеет равных.
- Записи о переводах публичны и общедоступны. Вы можете отследить, куда ушли ваши деньги и откуда пришли. При этом анонимность криптовалюты остаётся на высоком уровне.
- Лёгкая регистрация: интернет-валюта bitcoin не требует раскрытия личных данных. Для создания биткоин кошелька не нужно проходить сложные процедуры, процесс занимает от силы несколько минут. Количество счетов также не ограничено.
- Разделение на сверхмалые доли открывает совершенно новые возможности для торговли и предпринимательства, недоступные ранее. В большинстве случаев комиссия за перевод, вообще, отсутствует либо равна менее 0.01 доллара США.
- Никто и ни при каких обстоятельствах не может заблокировать ваш счёт. После создания он будет существовать столько же, сколько работать сама система.
- Отнять деньги, расположенные на вашем кошельке, не может никто – даже государство. Если только вы владеете ключом к учётной записи, то имеете настоящую стопроцентную гарантию сохранности своих денег – цифровая валюта bitcoin полностью безопасна.
- Количество переводов, объем пересылаемых или принимаемых биткоинов попросту отсутствуют.
- За всё время поисков в системе не обнаружили практически ни одного критического бага, клиент для работы постоянно обновляется. Софт удобен даже тем, кто не знает, зачем нужны биткоины.
- Взлёт стоимости. Ни один вид фиатных денег не возрастал на несколько тысяч раз за десятилетие. Интернет-валюта bitcoin, курс которой составляет уже свыше 1800 долларов за штуку, смог легко приумножить спрос и подняться в цене.

https://mining-cryptocurrency.ru/bitcoin-btc/

https://ru.wikipedia.org/wiki/Bitcoin_Cash

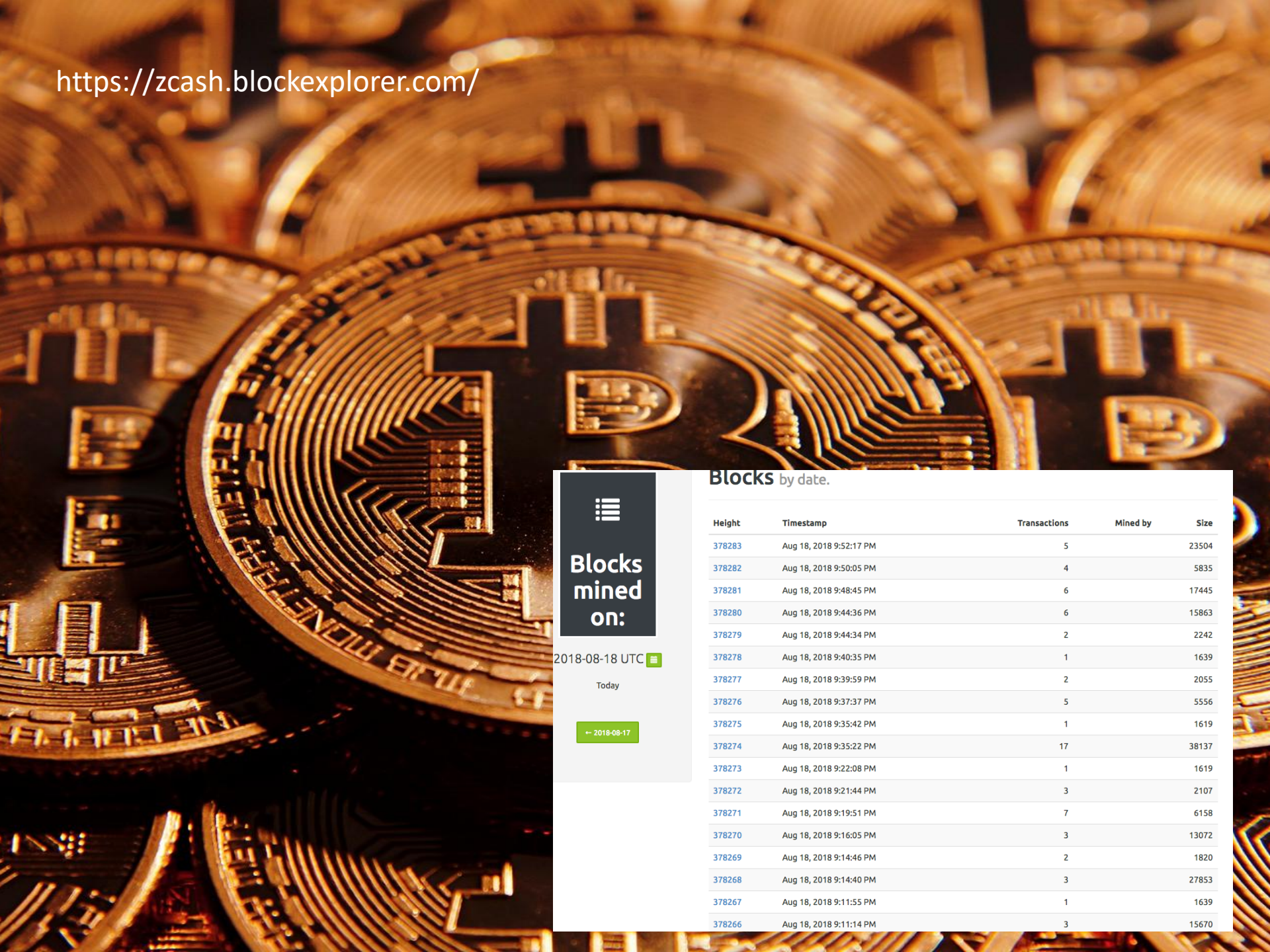
Количество транзакций в системе «Биткоин» за месяц





https://habr.com/post/114642/

https://zcash.blockexplorer.com/



Blocks mined on:

2018-08-18 UTC

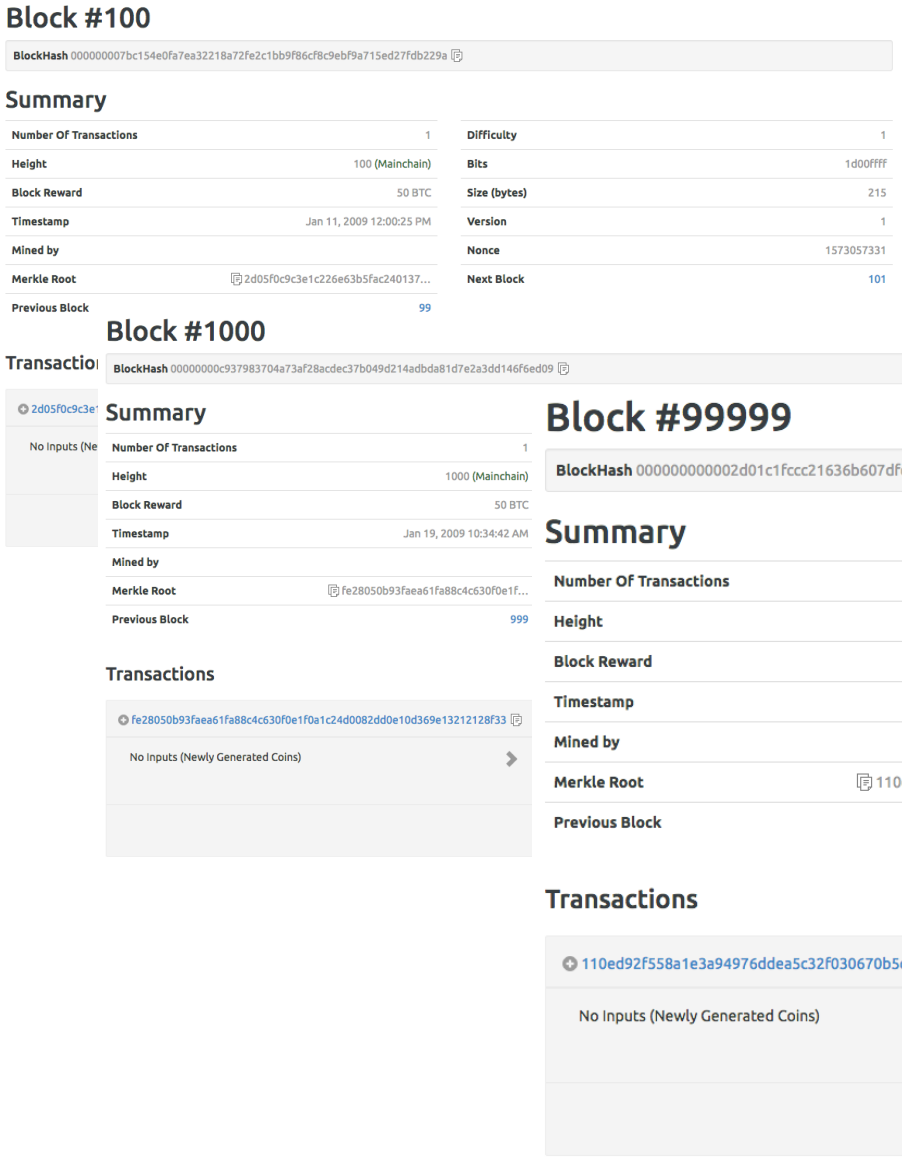
Today

← 2018-08-17

Blocks by date.

Height	Timestamp	Transactions	Mined by	Size
378283	Aug 18, 2018 9:52:17 PM	5		23504
378282	Aug 18, 2018 9:50:05 PM	4		5835
378281	Aug 18, 2018 9:48:45 PM	6		17445
378280	Aug 18, 2018 9:44:36 PM	6		15863
378279	Aug 18, 2018 9:44:34 PM	2		2242
378278	Aug 18, 2018 9:40:35 PM	1		1639
378277	Aug 18, 2018 9:39:59 PM	2		2055
378276	Aug 18, 2018 9:37:37 PM	5		5556
378275	Aug 18, 2018 9:35:42 PM	1		1619
378274	Aug 18, 2018 9:35:22 PM	17		38137
378273	Aug 18, 2018 9:22:08 PM	1		1619
378272	Aug 18, 2018 9:21:44 PM	3		2107
378271	Aug 18, 2018 9:19:51 PM	7		6158
378270	Aug 18, 2018 9:16:05 PM	3		13072
378269	Aug 18, 2018 9:14:46 PM	2		1820
378268	Aug 18, 2018 9:14:40 PM	3		27853
378267	Aug 18, 2018 9:11:55 PM	1		1639
378266	Aug 18, 2018 9:11:14 PM	3		15670

Структура блоков Bitcoin



Block #100

BlockHash 000000007bc154e0fa7ea32218a72fe2c1bb9f86cf8c9ebf9a715ed27fdb229a

Summary

Number Of Transactions	1	Difficulty	1
Height	100 (Mainchain)	Bits	1d00ffff
Block Reward	50 BTC	Size (bytes)	215
Timestamp	Jan 11, 2009 12:00:25 PM	Version	1
Mined by		Nonce	1573057331
Merkle Root	2d05f0c9c3e1c226e63b5fac240137...	Next Block	101
Previous Block	99		

Block #1000

Transactio

BlockHash 00000000c937983704a73af28acdec37b049d214adbda81d7e2a3dd146f6ed09

2d05f0c9c3e

No Inputs (Ne

Summary

Number Of Transactions	1
Height	1000 (Mainchain)
Block Reward	50 BTC
Timestamp	Jan 19, 2009 10:34:42 AM
Mined by	
Merkle Root	fe28050b93faea61fa88c4c630f0e1f...
Previous Block	999

Transactions

fe28050b93faea61fa88c4c630f0e1f0a1c24d0082dd0e10d369e13212128f33

No Inputs (Newly Generated Coins)

Block #99999

BlockHash 000000000002d01c1fccc21636b607dfd930d31d01c3a62104612a1719011250

Summary

Number Of Transactions	1	Difficulty	14484.16236122
Height	99999 (Mainchain)	Bits	1b04864c
Block Reward	50 BTC	Size (bytes)	215
Timestamp	Dec 29, 2010 3:55:31 PM	Version	1
Mined by		Nonce	3892545714
Merkle Root	110ed92f558a1e3a94976ddea5c32f...	Next Block	100000
Previous Block	99998		

Transactions

110ed92f558a1e3a94976ddea5c32f030670b5c58c3cc4d857ac14d7a1547a90 mined Dec 29, 2010 3:55:31 PM

No Inputs (Newly Generated Coins)

1XPLDXBheQyN2JCujEYTdHHxz66i3QJJA 50 BTC (S)

437396 CONFIRMATIONS 50 BTC

Blockhash — SHA-256 хэш блока

Merkle root —хэш списка транзакций

Bits —целевое значение хэша

Nonce — число, которое, начиная с нуля, инкрементируется после каждой итерации вычисления хэша

https://blockexplorer.com/

Bits — Одно из самых важных свойств. Является сокращенной формой целевого значения хэша. Блок считается сгенерированным (валидным), когда его хэш меньше этого целевого значения. Целевое значение определяет сложность создания блока. Чем оно меньше, тем меньше вероятность подобрать подходящий хэш за одну итерацию. Это свойство обновляется каждые две недели.

Происходит это следующим образом. Подсчитывается число сгенерированных блоков за последние две недели и сравнивается с эталоном (1 блок каждые 10 минут). Если блоков слишком много, то сложность увеличивается. Если блоков слишком мало — уменьшается. Таким образом система адаптируется к увеличению числа пользователей и, как следствие, суммарной мощности их компьютеров.

Nonce — Число, которое, начиная с нуля, инкрементируется после каждой итерации вычисления хэша. Собственно, так и происходит перебор, пока хэш не будет меньше целевого значения. Чтобы каждый новый хэш отличался от предыдущего, должно отличаться хотя бы одно из свойств заголовка блока.

Например, версия никогда не меняется. Хэш предыдущего блока обновляется тогда, когда кто-нибудь нас опередит и сгенерирует новый блок. Merkle root обновляется при добавлении транзакции. Время — каждые несколько секунд. Bits (целевое значение, сложность) — каждые две недели. Все это слишком долго. Чтобы не ждать, пока обновится одно из свойств и существует nonce.

Рассмотрим гипотетическую ситуацию. Все значения nonce были проверены и ни одно из них не подходит. За это время ни одно другое свойство не изменилось. Происходит переполнение nonce и оно снова начинается с нуля. Получается, что далее хэши будут повторяться. Чтобы избежать подобных ситуаций, после переполнения nonce, меняется специальное свойство одной из транзакций. После этого обновляется Merkle root и хэши заголовка блока уже не будут повторяться.

Bitcoin <–> Bitcoin Cash

Block #478558

BlockHash 000000000000000011865af4122fe3b144e2cbeea86142e8ff2fb4107352d43

Summary

Number Of Transactions	331	**Difficulty**	860221984436.2223
Height	478558 (Mainchain)	**Bits**	18014735
Block Reward	12.5 BTC	**Size (bytes)**	135661
Timestamp	Aug 1, 2017 5:16:14 PM	**Version**	536870914
Mined by		**Nonce**	1968823574
Merkle Root	5b65144f6518bf4795abd428acd0c3...	**Next Block**	478559
Previous Block	478557		

Transactions

d89853f0fb659caad5b7680656b0aaca8f3093fffe525d4ba422b93f8a52f070 mined Aug 1, 2017 5:16:14 PM

No Inputs (Newly Generated Coins)

3NA8hsjfdgVkmmVS9moHmkZsVCoLxUkvvv 12.61890202 BTC (S)

Unparsed address [0] 0 BTC (U)

58929 CONFIRMATIONS 12.61890202 BTC

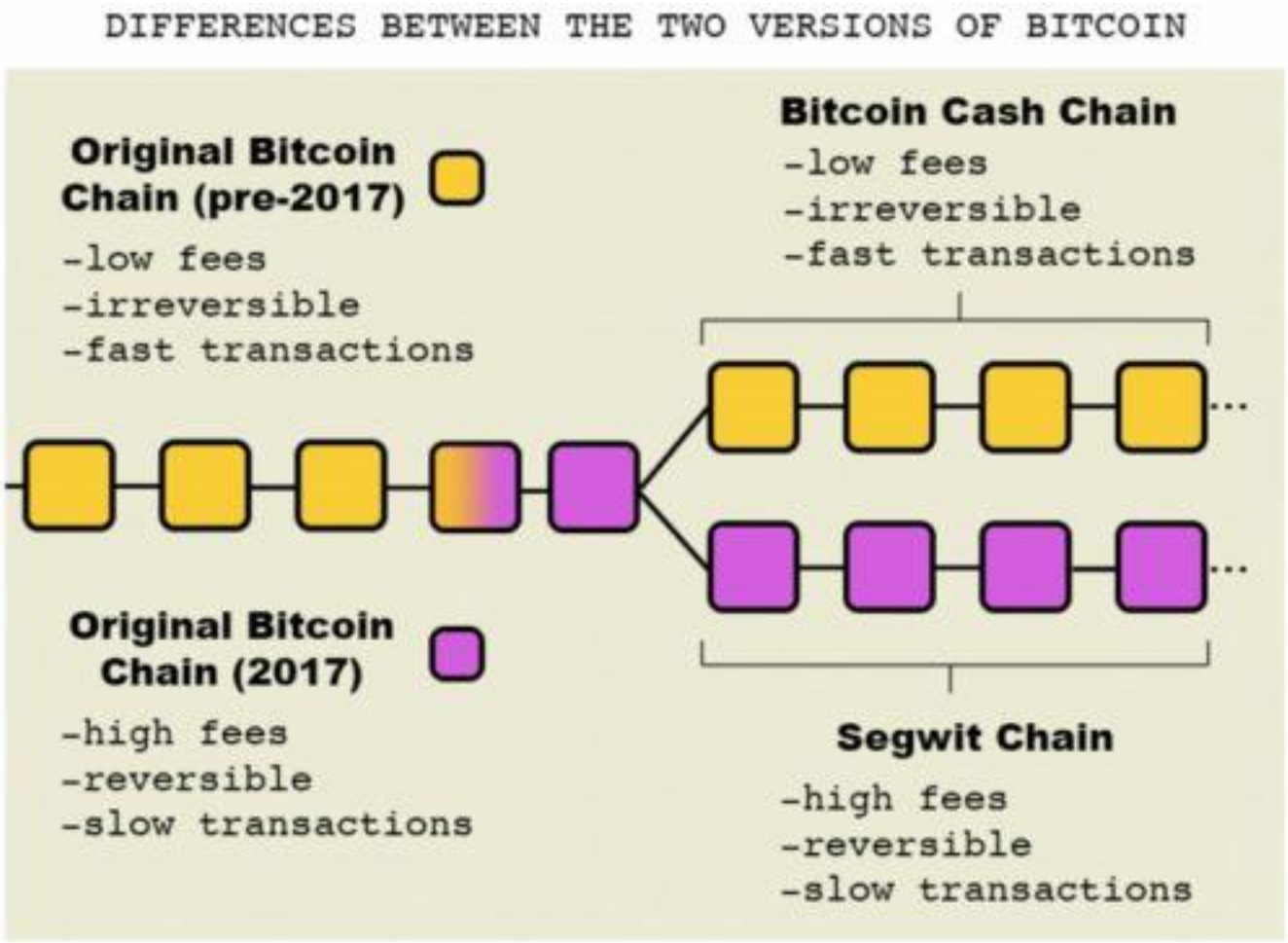
Bitcoin <–> Bitcoin Cash

1 августа 2017 года состоялось «принудительное ветвление» (хардфорк). У обеих криптовалют общая начальная история. Блок 478558 стал последним общим блоком. Следующий блок с номером 478559 был сформирован дважды в разных форматах. Один из них соответствует протоколу SegWitx, другой — Bitcoin Cash, который фактически стал первым блоком новой криптовалюты.

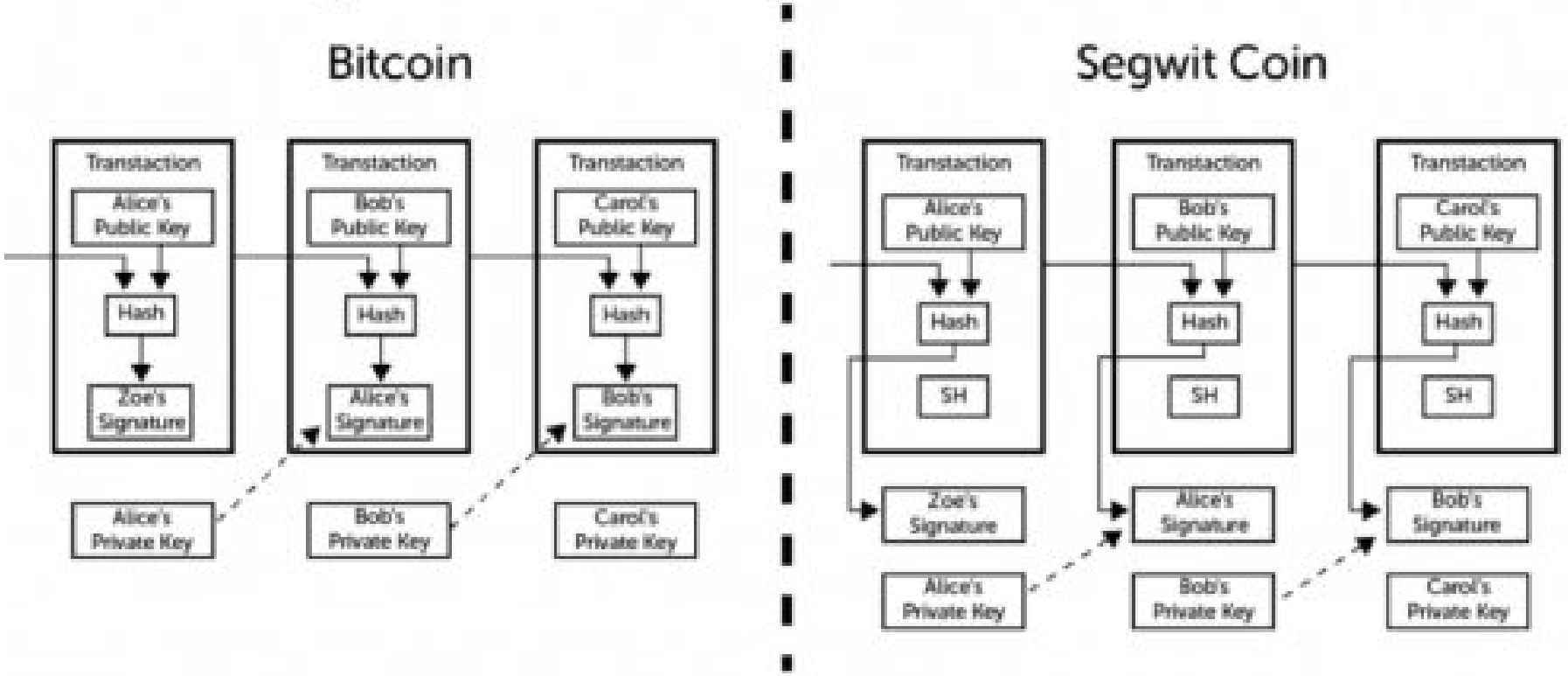
Все последующие транзакции разделены — попадают в разные ветки блокчейна, так как программы каждой из веток работают с предыдущими форматами блоков, но отвергают новые форматы друг друга.

		Mining	Capacity			User Experience		Features	
Fork	Ticker	Mining Algo	Max Block Size	Data Used For Max	Max Tx/Sec	Avg. Fee	Avg. Time To Confirm	Irreversible	Contains Signature Data
2014 Bitcoin	BTC	SHA-256	1MB	1MB	3	$0.10	10mins	Yes	Yes
2017 Bitcoin	BTC	SHA-256	1MB	1MB	3	~$1 to $8.9	114mins	No	No
Bitcoin Cash	BCH	SHA-256	8MB	8MB	23	$0.07	15mins	Yes	Yes

Bitcoin <–> Bitcoin Cash



How is a Segwit coin different?

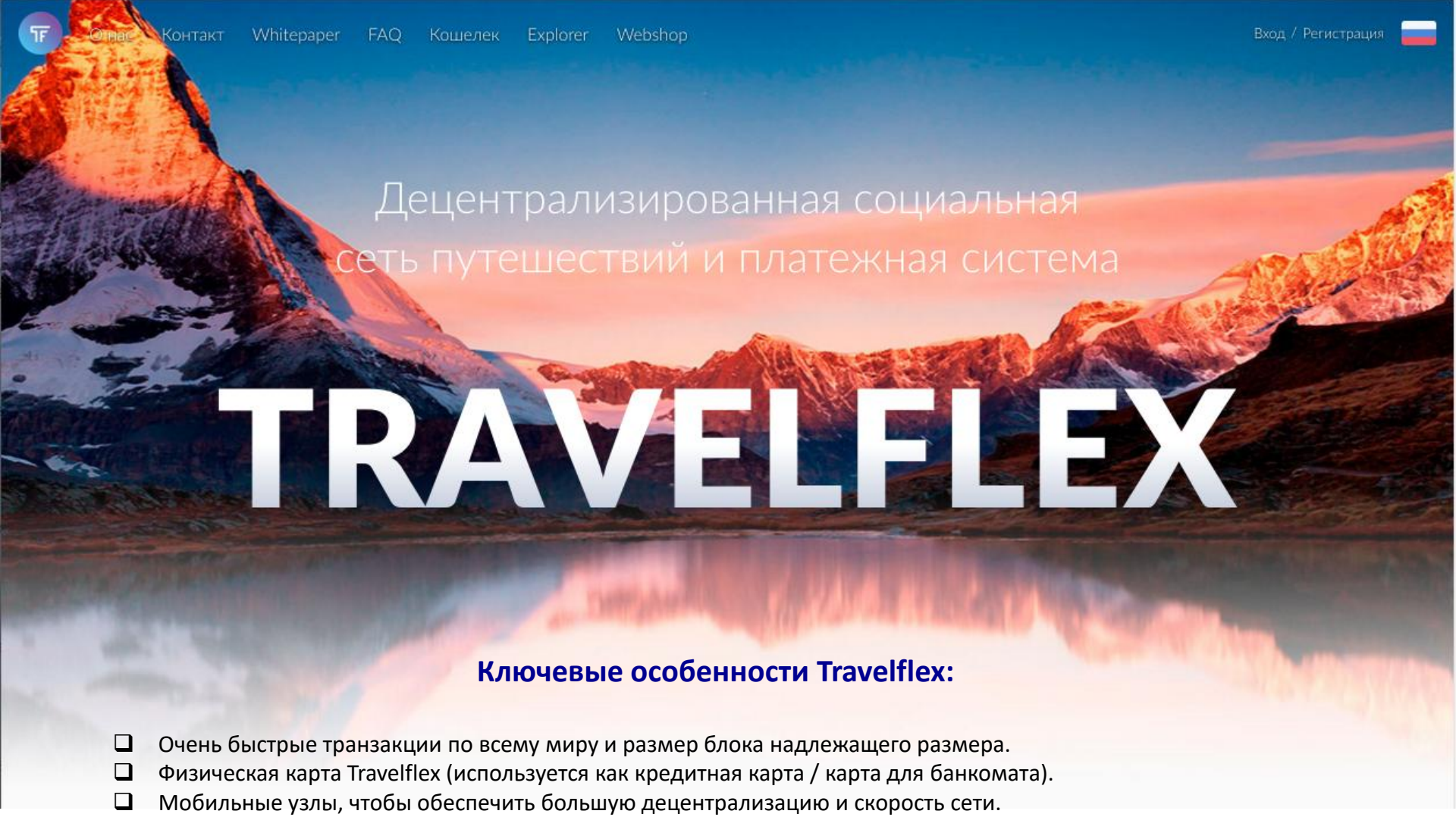


Криптовалюта Dash

https://miningbitcoinguide.com/kriptovalyuty/vidy/dash

- Даш сам себе хозяин. Разработку блокчейна биткоина финансируют различные институты вроде Blockstream, Chaincode Labs Inc., Ciphrex. Даш является проектом, который окупает себя сам
- Операции с Dash существенно дешевле транзакций с биткоином. Можно снизить затраты на проведение сделок с биткоином, если есть возможность ждать. Но придется потратить до нескольких дней на это. Даш намного быстрее и дешевле. Он также более конфиденциален, чем биткоин. В сети Dash есть функция «PrivateSend», которая защищает сделку дополнительным уровнем секретности. Причем эта опция является дополнительной. У биткоина ее вообще нет.
- У валюты даш нет активного сообщества. Биткоин пережил несколько форков за последний год, когда сеть разветвлялась на несколько параллельных цепей. Это происходило потому, что внутри сообщества держателей и разработчиков биткоина не было согласия по поводу усовершенствования алгоритмов работы блокчейна. Новые ответвления сети Bitcoin появились в ответ на перегрузку основной сети, где сделки стали проводиться медленно, а их ускорение требовало больших затрат на комиссии. Каждый раскол в среде разработчиков биткоина – это риск того, что однажды сеть может быть угроблена попытками усовершенствования протокола. Валюта Dash имеет систему голосования, в которой разработчики могут улаживать споры путем опросов. Процесс масштабирования сети протекает в более мягком ключе, он не приводит к проблемам и эксцессам.
- Dash использует систему алгоритмов X11 (включает в себя 11 функций хеширования). Биткоин использует один алгоритм — SHA-256.

http://ww 1.45’

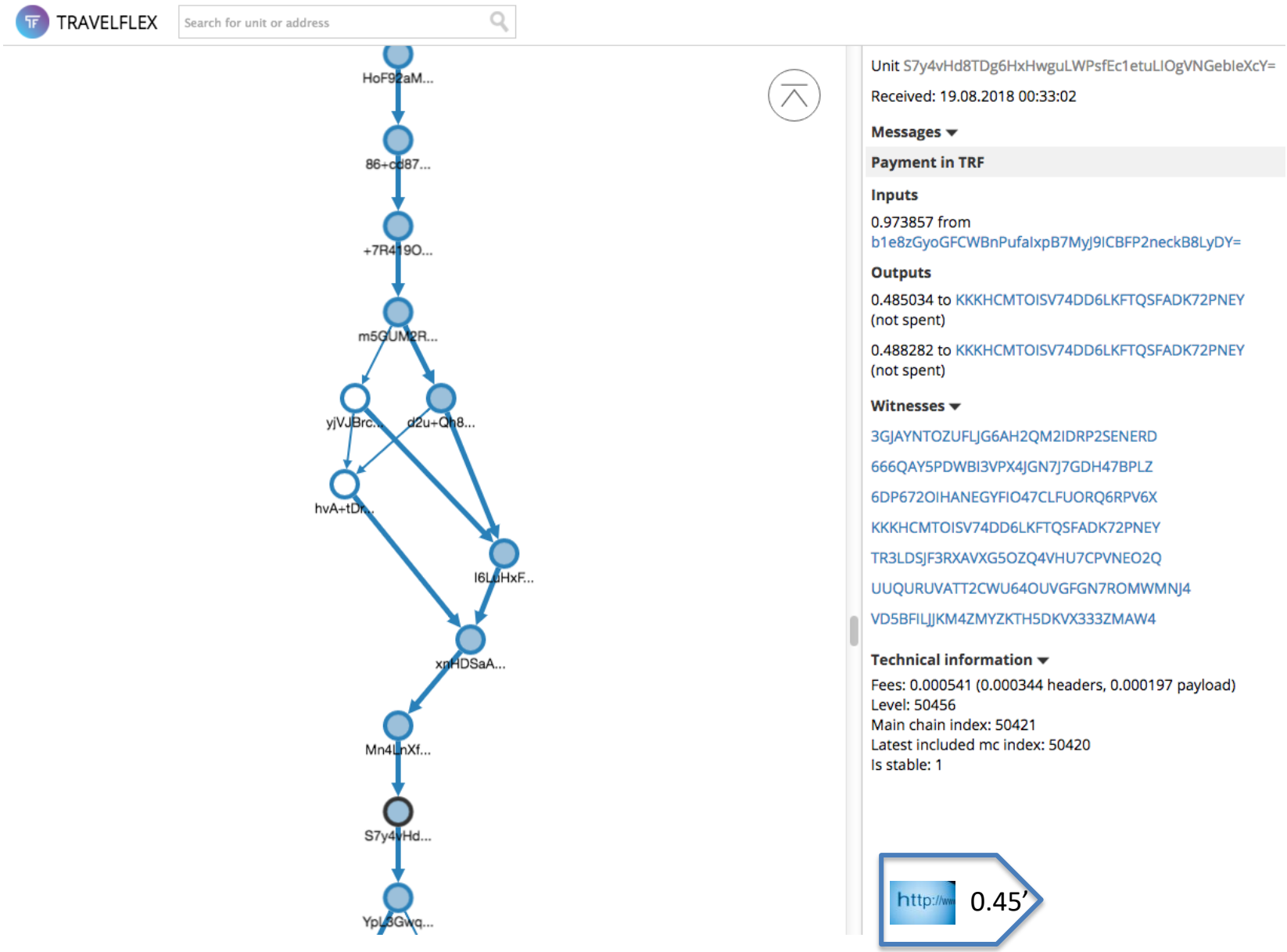


Ключевые особенности Travelflex:

- Очень быстрые транзакции по всему миру и размер блока надлежащего размера.
- Физическая карта Travelflex (используется как кредитная карта / карта для банкомата).
- Мобильные узлы, чтобы обеспечить большую децентрализацию и скорость сети.
- Полностью безопасный и децентрализованный чат между кошельками (peer-to-peer).
- Возможность использования любимых социальных сетей и добавления друзей в Ваш список контактов.
- Функция ближней бесконтактной связи (NFC), позволяет видеть пользователей Travelflex рядом с Вами.
- Монета устойчива к устройствам ASIC, децентрализованный майнинг с использованием протокола PoW. GPU майнинг.
- Участие в благотворительности через майнинг.
- Поддержка 24/7

https://travelflex.org/ru/?utm_source=coinzilla&utm_campaign=banner

https://explorer.travelflex.app/#lysNWuUilvzryPoGH168oIDHUzLL+UC6DRLrwQGUcKs=



Кошельки для криптовалюты

- Онлайн кошельки
- Мобильные кошельки
- Десктопные приложения
- Браузерные расширения
- Аппаратные кошельки

- **Криптонатор** – один и лидеров в русскоязычном сегменте. Поддерживает 14 криптовалют, позволяет осуществлять обмен между разными типами счетов. Имеет простой интерфейс и множество дополнительных инструментов. Баланс можно пополнить подарочными картами или через мобильное приложение. Вывод денежных средств не представляет никаких сложностей. Из минусов – ключи хранятся у третьей стороны, отсутствует мультиподпись, нет бэкапа в HD Wallet и отсутствует ПК поддержка.
- **HolyTransaction** – поддерживает все основные криптовалюты. Имеет «холодный» и «горячий» виды доступа. Мгновенные переводы между валютами в хранилище, удобный и защищенный. Из минусов – территориальные ограничения. Кошельком не могут пользоваться жители США и некоторых других стран;
- **Coinomi** – поддерживает свыше 60 криптовалют. Имеет высокую степень защиты и полную анонимность. Поддерживает все языки. Доступ осуществляется с помощью seed-ключа. Из минусов – нет двухфакторной аутентификации и мультиподписи, ограниченное количество возможностей для использования криптоденег;
- **CoinsBank** – аналог Криптонатора из Шотландии. Относится к типу криптобанков, выпускает чипованые карты Visa. Активно работает с большинством валют (доллар, евро, рубль среди основных). Преимущества и недостатки те же, что и у Криптонатора;
- **Jaxx** – очень удобный, универсальный сервис, который поддерживает почти все типы кошельков (некоторые из них пока в разработке). Подходит для «холодного» хранения. Поддерживает все основные криптовалюты, мгновенные переводы.

http:// 15’

https://miningbitcoinguide.com/kriptovalyuty/vidy/multi-wallet-top

https://karbo.io/

https://bipcoin.org/