Freeman Family

4 июля 2019

EPIC CASH

EPIC PRIVATE INTERNET CASH

Одноранговая система электронных денег

СРЕДСТВО СОХРАНЕНИЯ СТОИМОСТИ+СРЕДСТВО ОБМЕНА+ЕДИНИЦА УЧЕТА

1.7 миллиарда взрослых людей не имеют доступа к глобальной финансовой системе, в то время как еще 1,3 миллиарда недостаточно охвачены услугами. Epic Cash раскрывает человеческий потенциал, связывая отдельных людей с глобальным рынком. Быстро, практически бесплатно и доступно для всех.

Версия 7.1b

Содержание

I. Аннотация

Epic Cash – конечная остановка в путешествии к истинным P2P-интернет деньгам, являющимся краеугольным камнем конфиденциальной финансовой системы. Валюта Epic стремится стать наиболее эффективной в мире формой защиты конфиденциальности цифровых денег. Чтобы полностью соответствовать этой цели, валюта Epic удовлетворяет трем основным функциям денег:

1. **Средство накопления** – можно сохранить, восстановить и обменять позднее по предсказуемой цене;
2. **Средство обращения** – все, что принимается в качестве стандарта стоимости, и может быть обменено на товары или услуги;
3. **Мера стоимости** – единица, по которой учитывается и сравнивается стоимость вещи.

	$ USD	BTC	EPIC
Средство накопления	✗	✓	✓
Средство обращения	✓	✗	✓
Мера стоимости	✓	✗	✓

В 2009, Биткоин стал первой цифровой валютой, основанной на блокчейне, и тогда были определены три характеристики, по которым стали оцениваться другие криптовалюты :

- **Отсутствие необходимости доверия** – для того, чтобы сеть функционировала, нет необходимости в доверии какому-либо центральному органу или контрагенту;
- **Неизменность** – транзакции не могут быть отменены;
  a.Переписать историю крайне маловероятно или сложно;
  b.Никто, кроме владельца приватного (закрытого) ключа , не может перевести средства, связанные с этим приватным (закрытым) ключом;
  c. Все транзакции записываются в блокчейн.
- **Децентрализация** – “Блокчейны политически децентрализованы (никто не управляет ими) и архитектурно децентрализованы (нет инфраструктурной точки отказа...”[1].

Биткоин технологически проложил новые пути, придерживаясь проверенных временем основ в структуре своей монетарной политики. Успех биткоина тесно связан с его ограниченной эмиссией в сочетании с не требующим доверия, неизменным и децентрализованным блокчейном. Epic Cash эмулирует монетарную политику биткоина в плане сокращения инфляции и ограничения денежной массы; это позволяет валюте Epic стать эффективным средством сохранения стоимости.

Несмотря на успех биткоина, за прошедшие 10 лет с момента его создания были выявлены некоторые его недостатки. Другие проекты пытались преодолеть их, и мы исследовали лучшие из них, чтобы сделать их нашей отправной точкой. Мы решили использовать кодовую базу Grin и лучшие достижения некоторых других проектов; это поможет нам улучшить то, что было исследовано с большим трудом, и исправить ошибки у предшественников Epic Cash. Epic Cash обладает следующими ключевыми характеристиками идеальной валюты:

- **Взаимозаменяемость** – Стоимость конкретной единицы Epic всегда должна быть равна стоимости другой единицы Epic, также как одна Йена или Юань всегда равна и может быть заменена другой Йеной или Юанем. Достижение взаимозаменяемости в значительной степени зависит от конфиденциальности.
- **Масштабируемость** – Epic Cash поддерживает компактный блокчейн, на котором можно легко установить новые ноды без использования ресурсоемкого оборудования. Блокчейн Epic Cash способен по крайней мере удвоить пропускную способность биткоина.
- **Конфиденциальность** – Блокчейн Epic Cash гарантирует анонимность холдеров Epic и пользователей, защищая подробности транзакций от доступа третьих лиц; он разработан так, чтобы быть неотслеживаемым и невидимым для наблюдающих.
- **Скорость** – Транзакции Epic Cash проходят гладко, без задержек, и выполняются намного быстрее, чем при использовании блокчейн-технологии предыдущих поколений. В то время как биткоину требуется шесть 10-минутных блоков для получения полного подтверждения транзакции, для подтверждения транзакции Epic необходимо всего одно подтверждение блока; то есть, все завершается, как только будет намайнен 1-минутный блок.

[1] Buterin, Vitalik, *The Meaning of Decentralization*, 6 February, 2017, https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

II.Конфиденциальность

Современное использование денег можно понимать как коллективный перенос учетных единиц между людьми и учреждениями. Положение денег в любой момент времени может быть отображено после получения ответов на следующие вопросы:

1. Кто держит их, и сколько держит?

2. Кто и с кем совершает сделку и за сколько?

Мы можем получить ответы на эти вопросы как в отношении традиционных фиатных валют, так и в отношении биткоина. При этом, многое можно узнать о жизни людей – например, о моделях потребления, собственности, и контрагентах по сделкам. Достаточно точные выводы об интересах и намерениях человека можно сделать путем отслеживания передачи стоимости. При отсутствии конфиденциальности, данные о сделках могут стать опасной информацией в руках хищных третьих сторон.

Использование криптовалюты в прошлом десятилетии показывает континуум "конфиденциальности" в различных реализациях блокчейна. Следует учитывать, что шкала конфиденциальности варьируется от открытой и печально известной на одном конце, до анонимной на другом. При подрыве конфиденциальности, разрушается один из основных краеугольных камней криптовалюты - отсутствие необходимости в доверии. Так как в последнее время можно наблюдать успешность сервисов анализа блокчейна биткоина, то можно сказать, что уровень конфиденциальности биткоина становится все ниже. Пользователи все чаще должны предпринимать меры, чтобы не допустить непреднамеренного совершения транзакций с испорченным Биткоином. Решение Epic Cash делает упор на анонимность и восстанавливает это важное свойство, гарантируя, что как конфиденциальность личности, так и конфиденциальность транзакций заложены в систему на фундаментальном уровне.

Конфиденциальность личных данных

Конфиденциальность транзакций

Конфиденциальность личных данных

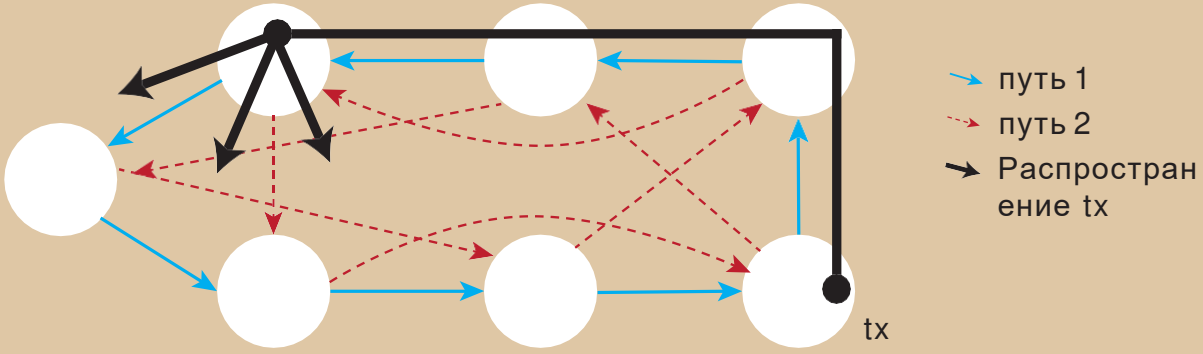
Большинство криптовалют, подобных биткоину, хранится в кошельках, адреса которых являются публичными (открытыми) ключами , полученными из приватных (закрытых) ключей кошельков. Эти адреса можно рассматривать как локаторы частного хранилища в цифровом мире. Блокчейн Epic Cash полностью исключает использование адресов, предлагая вместо этого воспользоваться одной большой мультиподписью , из которой генерируются все публичные и приватные ключи для однократного использования.

Поскольку адрес кошелька Биткоина является локатором хранилища в цифровом мире, то этот кошелек может быть отслежен по IP-адреса владельца, который привязывает владельца к компьютеру в уникальном месте в определенный момент времени. Проще говоря: когда совершается транзакция биткоина, то транзакция транслируется из коммуникационного центра, называемого “нодой”, и распространяется среди других нод, называемых “пирами”. Затем информация быстро передается каждому из пиров нод последовательно по всей сети. Этот процесс совершенно справедливо называют “протоколом сплетни”. То есть, каждый биткоин имеет видимую онлайн-позицию и физическую локацию, где он – или, скорее, владелец биткоина, - может быть найден. Как отметила журналистка Грейс Кэффин, Биткойн «не более секретен, чем поиск в Google с помощью домашнего интернет соединения»”[2]

В дополнение к исключению использования адресов кошельков, блокчейн Epic Cash обеспечивает конфиденциальность личных данных, и делает невозможным отслеживание IP-адресов. Это происходит благодаря интеграции протокола Dandelion++ (одуванчик). Улучшенный по сравнению с предшественником, оригинальным протоколом Dandelion, протокол Dandelion++ является результатом продолжающейся работы 7 исследователей по борьбе с атаками, нацеленными на деанонимизацию на блокчейне. Благодаря Dandelion++, транзакции передаются по случайно переплетенным путям, или “кабелям”, а затем неожиданно рассеиваются среди большой сети нод подобно капсулам цветка одуванчика, выдуваемым из стебля (рисунок 1). Это делает почти невозможным отслеживание транзакций до их источника и следовательно, исходящих IP-адресов.

Рисунок 1: Анонимные транзакции при использовании протокола *Dandelion++* .

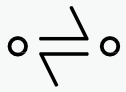
Dandelion++ пересылает сообщения по одному из двух переплетенных путей на 4-регулярном графе, а затем транслирует их, используя диффузию. На рисунке, транзакция распространяется по выделенному синим пути[3]. Этот процесс чрезвычайно усложняет отслеживание транзакции до их источника, тем самым сохраняя конфиденциальность.



[2] F2Caffyn, Grace, ***Chainalysis CEO Denies ‘Sybil Attack’ on Bitcoin’s Network,*** 14 March, 2015, https://www.coindesk.com/chainalysis-ceo-denies-launching-sybil-attack-on-bitcoin-network

[3] Fanti, G, Venkatakrishnan, S B, Bakshi, S, Denby, B, Bhargava, S, Miller, A & Viswanath, P 2018, ‘Dandelion++: Lightweight Cryptocurrency Networking with Formal Anonymity Guarantees’, ***Proc. ACM Meas. Anal. Comput. Sys.***, Vol. 2, Article 29, pg. 8, https://www.readkong.com/page/dandelion-lightweight-cryptocurrency-networking-with4805755-?p=1

Конфиденциальность транзакций



The Блокчейн Epic Cash обеспечивает конфиденциальность транзакций, скрывая суммы и взаимосвязь “отправитель-получатель” транзакции. Это достигается за счет применения идей, знакомых по методам Confidential Transactions (CT)[4] и CoinJoin[5], в значительной степени разработанным Грегори Максвеллом (разработчиком Bitcoin Core, соучредителем и техническим директором Blockstream).

CT, оригинально созданный Адамом Бэком и позднее усовершенствованный Максвеллом, функционирует, разбивая транзакции на более мелкие части при помощи гомоморфного шифрования, метода выполнения вычислений зашифрованной информации без предварительного ее дешифрования для сохранения конфиденциальности. После разделения, наблюдатели не могут видеть фактическую сумму транзакций из-за ослепляющих факторов, - системы, которая выбрасывает случайные числа при микшировании фрагментов транзакций, чтобы скрыть значения этих фрагментов. В конечном счете, только транзакционные стороны могут знать стоимость сделки; при этом, транзакция проверяется сетью посредством подтверждения того, что сумма выходных значений равна сумме входных значений, а сумма выходных ослепляющих факторов равна сумме входных ослепляющих факторов.

Чтобы еще больше усложнить задачу для любопытных глаз, все транзакции Epic Cash маскируются при помощи CT, а затем смешиваются вместе, чтобы скрыть взаимосвязь между транзакционными сторонами. Это происходит при использовании второго концепта Максвелла, CoinJoin.

Проиллюстрируем *CoinJoin* упрощенно, представьте, что A, B и C отправляют Epic X, Y и Z, соответственно. При отправлении через среду *CoinJoin*, все, что известно, - это то, что A, B и C отправляют, а X, Y и Z получают, в то время как суммы транзакций остаются невидимыми. Система *CoinJoin является* фундаментальной для Epic Cash благодаря использованию Односторонних агрегированных подписей (OWAS), которые объединяют все транзакции внутри блока в одну транзакцию.

Конфиденциальность: Сводка

Блокчейн Epic Cash защищает конфиденциальность частных лиц и их транзакций:

- **Исключение адресов кошельков – внутри блокчейна отсутствуют идентификаторы локаций для цифровых хранилищ. Транзакции строятся на основе “от человека к человеку” “от кошелька к кошельку”;**
- ***Протокол Dandelion++* – производит сокрытие цифровых путей транзакции, начиная с IP-адреса отправителя;**
- ***Конфиденциальные транзакции* – происходит разбиение транзакций на множество частей с введением ослепляющих факторов в коллекцию из этих частей для того, чтобы значения частей и другие параметры транзакций остались неизвестны;**
- ***CoinJoin* – объединяет транзакции в пакеты, чтобы скрыть взаимосвязь между транзакционными сторонами.**

[4] Maxwell, Gregory, ***Confidential Transactions,*** Technical Report (2015), https://people.xiph.org/~greg/confidential_values.txt

[5] Maxwell, Gregory, ***CoinJoin: Bitcoin Privacy for the Real World***, 22 August, 2013, post on Bitcoin Forum, https://bitcointalk.org/index.php?topic=279249.0

III Взаимозаменяемость

Чарли Ли, создатель Litecoin, утверждал, что взаимозаменяемость – единственное свойство надежных денег, которое отсутствует у Биткоина и Litecoin, и признал, что конфиденциальность и взаимозаменяемость стали следующим полем битвы для этих монет. Андреас Антонопулос, один из ведущих мировых экспертов в области блокчейна, заявил, что "... Скомпроментированные монеты разрушительны. Если вы нарушаете взаимозаменяемость и конфиденциальность, вы разрушаете валюту."[7]

Взаимозаменяемость - это свойство набора товаров или активов, которое гарантирует, что отдельные единицы этого набора имеют равную ценность и являются взаимозаменяемыми. Это то, что отличает самые ранние формы валюты от предшествующих им бартерных систем. Деньги быстро теряют свою полезность, если отсутствует уверенность во взаимозаменяемости. Как будет показано ниже, взаимозаменяемость большинства валют не определена, в то время как архитектура конфиденциальности Epic Cash гарантирует, что она невосприимчива к таким угрозам.

Большинство криптовалют, сходных с биткоином вследствие прозрачности их блокчейнов, на которых они построены, могут быть достоверно отслежены через каждый кошелек, в котором они хранятся. Частные третьи стороны и правительства осуществляют мониторинг блокчейна биткоина при помощи все более изощренных средств для быстрой идентификации монет, использованных ранее в какой-либо деятельности. Это, естественно, приводит к опасениям, что грязные монеты могут когда-нибудь быть запрещены для транзакций, оставляя их последующих добросовестных владельцев в убытке.

19 марта 2018 года, Управление по контролю за иностранными активами США (OFAC) объявило, что рассматривает вопрос о включении адресов цифровых валют в перечень специально обозначенных национальных лиц (SDN), являющимися лицами, с которыми физическим и юридическим лицам США запрещено совершать сделки. Еще более беспокоит то, что OFAC также не исключает включения адресов, на которых хранятся в настоящее время грязные монеты, в список SDN, что фактически означает помещение невиновных владельцев грязной криптовалюты в черный список преступников из-за владения грязными монетами. Это привело к тому, что профессор права Нью-Йоркского Университета Эндрю Хинкес сказал "прощай, взаимозаменяемость, до свидания", и что общественность должна ожидать "высшей цены за только что отчеканенные монеты или за доказанно чистые монеты."

Учитывая все это, нетрудно представить себе переворот на рынке криптовалют и проблемы или даже исчезновение многих устоявшихся криптовалют. Тем не менее, Epic Cash является одной из немногих криптовалют, которые избегут этой проблемы благодаря мощным функциям конфиденциальности, описанным в этой бумаге. Из-за исключения связи между личностью и собственностью, а также из-за невозможности установления взаимосвязи между сторонами сделки, монеты Epic никогда не могут быть связаны с конкретным человеком или деятельностью. Таким образом, ценность Epic не зависит от пользователей; при этом, Epic обеспечивает высокую степень конфиденциальности и безопасности, которая значительно осложнит злоумышленникам возможность манипуляций в криминальных, финансовых и политических целях.

> **“…ГРЯЗНЫЕ МОНЕТЫ РАЗРУШИТЕЛЬНЫ. ЕСЛИ ВЫ НАРУШАЕТЕ ВЗАИМОЗАМЕНЯЕМОСТЬ И КОНФИДЕНЦИАЛЬНОСТЬ, ВЫ РАЗРУШАЕТЕ ВАЛЮТУ.”**
>
> **АНДРЕАС АНТОНОПУЛОС**

[6] Njui, John P, ***Charlie Lee: Litecoin (LTC) To Soon Have Confidential Transactions for Fungibility***, 29 January, 2019, https://ethereumworldnews.com/charlie-lee-litecoin-ltc-to-soon-have-confidential-transactions-for-fungibility/

[7] Carl T, ***Andreas Antonopoulos Says If Fungibility Is Not Fixed Bitcoin Could Be Attacked,*** 9 April, 2019, https://bitcoinexchangeguide.com/andreas-antonopoulos-says-if-fungibility-is-not-fixed-bitcoin-could-be-attacked/

[8] Hinkes, Andrew, Ciccolo, Joe, ***OFAC's Crypto Blacklist Could Change Crypto***, 24 March, 2018, https://www.coindesk.com/goodbye-fungibility-ofacs-bitcoin-blacklist-remake-crypto

IV. Масштабируемость

Epic Cash – реализация блокчейна MimbleWimble , обеспечивающая масштабируемость благодаря экономичному изайну в плане занимаемого места, который избавляет от избыточных данных транзакций. Функциональные возможности метода Cut-Through отвечающего за это, гарантируют то, что блокчейн с течением времени будет экономить больше пространства по сравнению со многими криптовалютами, включая биткоин, и что новые ноды могут быть созданы с минимальными затратами на память и вычислительную мощность. Эффективное использование блокчейном пространства будет способствовать организации сильно рассредоточенной сети и децентрализации. Более того, в то время как каждая нода Биткоина должна хранить всю цепь, ноды Epic Cash способны вносить свой вклад в безопасность сети, храня небольшое подмножество блоков.

Большинство криптовалют требуют практически неограниченного места для хранения всех данных транзакций в их блокчейнах. Цепь биткоина в настоящий момент увеличивается на 0.1353 Гб памяти каждый день, а цепь Ethereum растет с еще большей скоростью - 0.2719 Гб в день. Если цепь Биткоина продолжит расти такими темпами, то к 2140 году – когда будет намайнен (добыт) последний блок, ее размер достигнет примерно 6 Тб. Размер цепи Ethereum к этой дате превысит 10 Тб[9].

В большинстве блокчейнов, не использующих MimbleWimble, транзакции должны верифицироваться нодами по всему миру. По мере увеличения количества данных, увеличивается нагрузка на каждую ноду. Даже при размере цепи всего в 200 ГБ (примерный размер цепи Биткоина в данный момент), для синхронизации данных необходима стабильная работа сети, и высокая скорость чтения с диска и записи на диск.

Следовательно, майнинг становится все более централизованным, и центр майнинга смещается в сторону больших пулов, которые могут себе позволить использовать дорогостоящие централизованные ресурсы. **Если бы вся история блокчейна биткоина хранилась бы блокчейне Epic Cash, то она заняла бы на 90% меньше пространства.** Чем меньше, тем быстрее; каждая транзакция будет требовать меньше времени для передачи и защиты.

MimbleWimble решает затруднительную ситуацию, связанную с организацией хранения данных, при помощи инновационного метода обрезки блоков, который называется ‘Cut-Through' (разрезать). Чтобы лучше понять, как работает метод Cut-Through, стоит увидеть, как транзакции и блоки составляются внутри блокчейна MimbleWimble.

Входы:

Ссылки на старые входы;

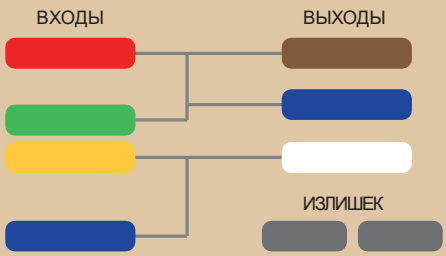
Выходы:

Выходы конфиденциальных транзакций и rangeproofs;

Излишек:

Разница между выходами и входами, плюс сигнатуры (для аутентификации и доказательства отсутствия инфляции

Рисунок 2:
Транзакционные части MimbleWimble.



[9] Li, Crypto, ***Blockchain's Big Data Problem,*** 27 January, 2019, https://www.longhash.com/news/blockchains-big-data-problem

Все блоки Epic Cash содержат:

Деревья Merkle входов транзакций;

Деревья Merkle выходов транзакций и rangeproofs;

Перечень значений излишков и сигнатур.

На рисунках 2 и 3, адаптированных из презентаций Андрю Поэльстры[10], мы можем увидеть недавно намайненные монеты Epic, представленные в виде белых входных ячеек. Одинаково окрашенные ячейки представляют собой выходы с соответствующими потраченными входами. Благодаря процессу Cut-Through, входы и соответствующие им потраченные выходы удаляются, чтобы освободить место в блоке, что уменьшает объем данных, который необходимо хранить в блокчейне. В процессе исключения транзакций из реестра, оставшиеся избыточные ядра (всего 100 байт) постоянно документируют то, что транзакции осуществлены.

Поскольку блоки продолжают создаваться, то MimbleWimble использует метод Cut-Through и блоков; в итоге, все, что остается в долгосрочной перспективе – заголовки блоков (примерно 250 байт), неизрасходованные транзакции, и ядра транзакций (примерно 100 байт). На примере Grin, второй запущенной имплементации MimbleWimble, видно, что общий размер цепи MimbleWimble с таким же количеством транзакций, что и у цепи Биткоина, составляет всего 10% от общего размера цепи биткоина[11]. Более того, размер ноды будет «порядка нескольких ГБ для цепочки Биткойна и потенциально может быть оптимизирован до нескольких сотен мегабайт."[12]

Это резко отличается от блокчейна Биткоина, где КАЖДАЯ нода должна хранить ВЕСЬ блокчейн. Со временем, когда пространственная эффективность блокчейна Epic Cash вырастет по сравнению с блокчейном Bitcoin, то вырастет и эффективность затрат относительно участия нод в сети Epic Cash. Снижение барьеров для участия поможет обеспечить критически важную устойчивость на уровне нод при проектировании сетей.

Благодаря реализации MimbleWimble и сокращению цепи при помощи процесса Cut-Through, блокчейн Epic Cash предлагает масштабируемость, которая часто упускается из виду сообществом криптовалют. Epic cash служит выполнению основной задачи Биткоина и аналогичных проектов-единомышленников: децентрализации. Независимо от того, сколько транзакций в секунду способна обработать монета, что толку от нее, если она не поддерживается широкой и разнородной сетью? Если требования к памяти таковы, что валидация в конечном итоге тяготеет к сильным конгломератам майнинга, то все усилия криптовалютного сообщества по созданию децентрализованной системы будут тщетны. Чтобы обеспечить дополнительную пропускную способность, план развития Epic Cash предусматривает реализацию уровня 2 в стиле Lightning в качестве краткосрочной цели.

Рисунок 3:
Транзакции MimbleWimble до и после Cut-Through.

[10] SF Bitcoin Developers, *MimbleWimble with Andrew Poelstra,* 24 November, 2016, https://www.youtube.com/watch?v=aHTRlbCaUyM&t=940s

[11] Grin Forum, *Grin Blockchain Size,* December, 2018, https://www.grin-forum.org/t/grin-blockchain-size/1334

[12] GandalfThePink, *Introduction to Mimblewimble and Grin,* 28 March, 2019, https://github.com/mimblewimble/grin/blob/master/doc/intro.md

V. Монетарная политика

Монетарная политика Epic Cash и Биткоина очень сходна. Циркуляционный запас Epic Cash сначала будет увеличиваться довольно быстро, и в 2028 году он синхронизируется с циркуляционным запасом биткоина. После этого, скорость эмиссии будет падать, пока Epic Cash не достигнет своего максимального запаса - 21 миллион Epic в 2140 году. Epic Cash – безопасное хранилище долгосрочной стоимости, так как циркуляционный запас известен в любой конкретный момент времени на протяжении жизненного цикла эмиссии, и имеет фиксированную максимальную эмиссию. Монетарная политика Epic Cash характеризуется следующими 4 особенностями:

- В течение первых 9 лет жизненного цикла, будет происходить быстрая эмиссия; во время данного цикла, будет намайнено 20,343,750 Epic (96.875% от общей эмиссии). Точные параметры эмиссии указаны в разделе График эмиссии этой бумаги;
- Максимальная эмиссия – 21 миллион Epic – будет достигнута к 2140 году; это произойдет примерно в то же время, когда Биткоин достигнет своей максимальной эмиссии в 21 миллион единиц;
- Циркулирующий запас Epic и скорость эмиссии будут синхронизированы с биткоином в Точке сингулярности Epic примерно 24 мая 2028 года. После достижения сингулярности, скорость эмиссии начнет уменьшаться с нарастающей скоростью, в то время как циркуляционный запас будет расти с уменьшающейся скоростью
- Epic имеет структуру делимости до 8 знаков после запятой – по аналогии с Биткоином. 1 Epic равен 100,000,000 фрименов (аналогично, 1 Биткоин равен 100,000,000 сатоши).

Монетарная политика Epic Cash смоделирована по аналогии с биткоином по следующим причинам:

- Согласие с экономическими основами биткоина – а именно с тем, что в основе сохранения ценности лежат дефицит и предсказуемость оборотных средств.
- Публика уже знакома с моделью Биткойн и ее проверенной репутацией за последние десять лет, прошедших с момента создания биткоина. Приблизительно синхронизируясь с циркуляционным запасом Биткоина и наследуя максимальный запас биткоина и структуру делимости, Epic идет по пути наименьшего сопротивления к массовому принятию.

VI. График эмиссии

Epic Cash имеет всего 33 майнинговых эры, при наступлении каждой из которых происходит уменьшение награды за блок, по сравнению с предыдущей эрой. Генезис Epic, - дата, когда произойдет майнинг первого блока Epic – августа 2019 года. За минуту будет майниться один блок. За первые 5 эр, будет намайнено около 97% от максимального запаса Epic. и эмиссия Epic за первые 9 лет в результате будет примерно совпадать с эмиссией биткоина за 20 лет. Это можно расценивать как “шанс повернуть время вспять” для тех, кто пропустил впечатляющий рост биткоина.

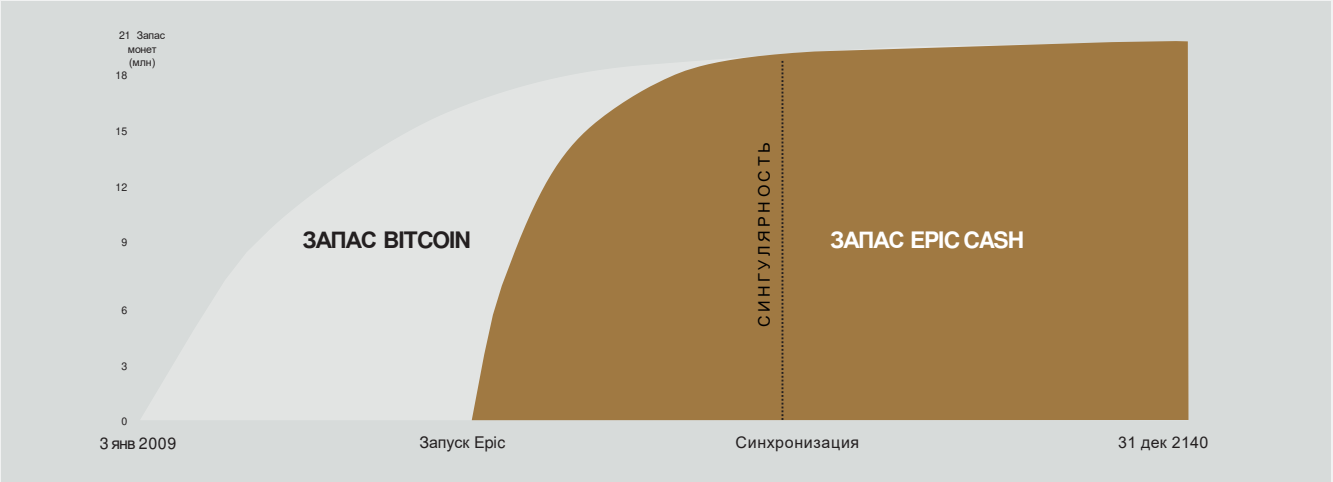
В графике эмиссии на таблице 1 указаны даты начала и окончания первых 7 эр майнинга, соответствующие эрам награды за блок, и последующий циркуляционный запас для каждой эры. Для краткости, эры с 8 по 33 не включены в таблицу. Достаточно понять, что для этих эр, награда за блок равна половине от суммы награды, которая имела место в предыдущую эру (также, как и у биткоина). Количество монет Epic, эмитированных во время каждой эры, будет равно сумме вознаграждений за блок за 4-летнюю эру (примерно 1460 дней).

Когда наступит Сингулярность (2028), циркуляционный запас Epic будет почти соответствовать циркуляционному запасу биткоина, после чего Epic Cash примет модель награды за блоки и халвинга такую же, как и у биткоина, при которой награда за блок уменьшается наполовину каждые 4 года. Единственное исключение состоит в том, что блоки Epic продолжат майниться со скоростью 1 блок в минуту (блок биткоина майнится со скоростью 1 блок в 10 минут). Благодаря этому, циркуляционный запас Epic будет примерно соответствовать циркуляционному запасу биткоина.

Таблица 1: График эмиссии для первых 7 эр майнинга. Даты указаны приблизительно

Эра	1	2	3	4	5	СИНГУЛЯРНОСТЬ	6	7
Награда за блок	16	8	4	2	1		0.15625	0.078125
Дата начала	Aug 1, 2019	Jun 29, 2020	Oct 11, 2021	Jun 3, 2023	Aug 10, 2025		May 24, 2028	May 22, 2032
Дата окончания	Jun 29, 2020	Oct 11, 2021	Jun 3, 2023	Aug 10, 2025	May 24, 2028		May 22, 2032	May 20, 2036
Длина (в днях)	334	470	601	800	1019		1460	1460
Начальный запас	0	7,695,360	13,109,760	16,571,520	18,875,520		20,342,880	20,671,380
Конечный запас	7,695,360	13,109,760	16,571,520	18,875,520	20,342,880		20,671,380	20,835,630
% от максимального запаса	36.6%	62.4%	78.9%	89.9%	96.9%		98.4%	99.2%

Рисунок 4: Графики эмиссии Epic и Bitcoin



VII. Майнинг

Блокчейн Epic Cash обеспечивает децентрализацию за счет того, что майнинг может осуществляться на широком спектре вычислительного оборудования. Майнинг Epic исходно доступен на CPU, GPU, и ASIC, с использованием соответственно трех алгоритмов хэширования: RandomX, ProgPow, и CuckATоо31+. Алгоритмы могут быть тривиально заменены “в горячем режиме” без ущерба для целостности цепи..

1 RandomX и CPU

RandomX - Proof-of-Work (PoW) алгоритм, оптимизированный для CPU общего назначения. Он случайным образом запускает на выполнение программы для сильной загрузки памяти (метод memory-hard), что позволяет достичь несколько целей:

- Предотвращение разработки однокристальных чипов ASIC;
- Минимизация преимущества в эффективности специализированного оборудования над CPU общего назначения.

Для майнинга Epic на CPU необходимо постоянное выделение 2 ГБ физического RAM, 16 Кб кэша первого уровня L1, 256 Кб кэша второго уровня L2, и 2 Мб кэша третьего уровня L3 на майнинговый поток[13]. Устройства Windows 10 требуют 8 Гб RAM или более. Не исключено, что когда-либо в недалеком будущем, мобильные телефоны станут жизнеспособными майнинговыми нодами. Ранняя интеграция CPU в майнинговую сеть Epic Cash – отличная возможность для многих, обладающих лишь скромными вычислительными средствами, получать награду за блок за помощь в защите сети Epic Cash.

2 ProgPow и GPU

Программное Proof-of-Work (ProgPow) - алгоритм, который зависит от пропускной способности памяти и базовых вычислений рандомизированных математических последовательностей; он использует преимущества многих вычислительных функций графического процессора и, тем самым, эффективно берет под контроль общий расход энергии для аппаратного обеспечения. Поскольку ProgPow специально разработан для того, чтобы в полной мере использовать преимущества обычных графических процессоров, то одновременно и сложно, и дорого, добиться значительно более высокой эффективности с помощью специализированного оборудования. Таким образом, алгоритм ProgPow ослабляет стимулы для больших ASIC-пулов вытеснить графические процессоры, что часто наблюдается во многих других алгоритмах PoW, таких как SHA-256 для Биткоина. Графические процессоры, хотя и не так распространены, как процессоры, но все еще достаточно популярны. Благодаря технологическому развитию, которое мы наблюдаем в отношении Nvidia и AMD, GPU могут параллельно обрабатывать множество решений для майнинга, что выгодно отличает их от CPU. Именно из-за сочетания общедоступности и высокой вычислительной мощности, графические процессоры станут основой для осуществления большинства операций майнинга в начальные периоды, как показано в таблице 2.

3 CuckATоо+31 и ASIC

CuckATоо31 + - это дружественный к ASIC вариант алгоритма CuckooCycle, разработанного голландским программистом Джо-ном Тромпом. Являясь родственником устойчивого к ASIC CuckARоо29, CuckATоо31+ генерирует случайные двудольные графы и предоставляет майнерам задачу найти петлю заданной длины "N", проходящую через вершины этого графа.

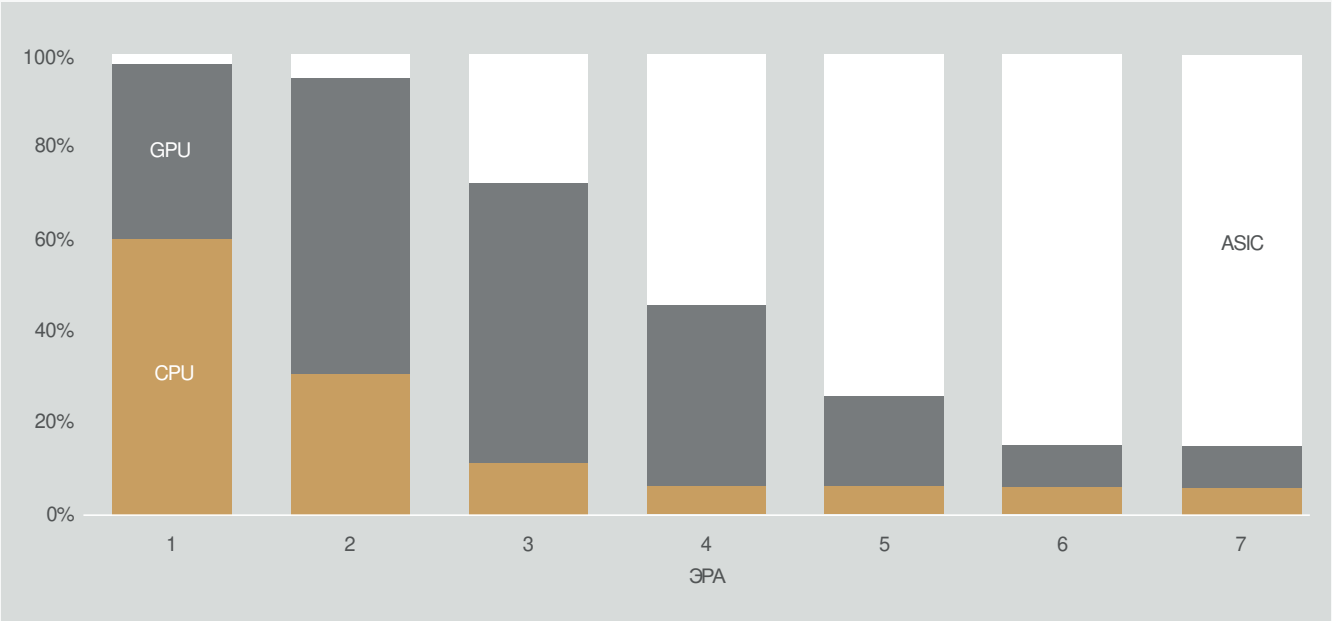
[13] Tevador, ***RandomX***, 28 March, 2019, https://github.com/tevador/RandomX

Это – задача, связанная с использованием памяти; время решения зависит от пропускной способности памяти, а не от скорости CPU или GPU. В результате, алгоритмы Cuckoo Cycle приводят к меньшему выделению тепла и потреблению значительно меньшего количества энергии, чем традиционные POW-алгоритмы. Совместимый с ASIC CuckATоо31+, позволяет повысить эффективность по сравнению с графическими процессорами благодаря использованию сотен МБ SRAM что является узким местом для I/O памяти[14]. В конечном счете, ASIC предлагает наибольшую потенциальную экономию за счет трех вариантов майнинга. В интересах инклюзивности, на ранних этапах ASICи будут получать небольшую часть от награды за майнинг по сравнению с CPU и GPU; в дальнейшем, ASICи получат мажоритарную долю от награды за добытый блок при условии, что будет существовать конкурентная экосистема производителей устройств для CuckATоо31 +.

Таблица 2: Распределение награды за майнинг. Подлежит пересмотру. Варианты распределения будут направлены на достижение максимальной децентрализации в соответствии с долгосрочными интересами сети.

Эра	1	2	3	4	5	6	7
Дни	334	470	601	800	1019	1460	1460
CPU	60%	30%	10%	5%	5%	5%	5%
GPU	38%	65%	62%	40%	20%	10%	10%
ASIC	2%	5%	28%	55%	75%	85%	85%

Рисунок 5: Распределение награды за майнинг для каждой эры согласно таблице 2. Возможно внесение изменений.



[14] Le Sceller, Quentin, *An Introduction to Grin Proof-of-Work,* 16 November, 2018, https://blog.blockcypher.com/an-introduction-to-grin-proof-of-work-103aaa9f66ce

4 Майнинговые взносы

Начиная с генезиса Epic (2019) и заканчивая сингулярностью Epic (2028), при осуществлении процесса майнинга будет происходить выделение определенного процента от майнинга (майнинговый взнос) в Блокчейн-фонд EPIC.

Блокчейн-фонд EPIC создан для обеспечения технического развития и продвижения проекта Epic Cash в первые годы существования благодаря осуществлению маркетинговой деятельности и развитию партнерских отношений в индустрии финансовых технологий.

После сингулярности, роль фонда EPIC возьмет на себя Распределенная автономная корпорация EPIC (EDAC), которая будет разработана фондом для передачи функций.

Блокчейн-фонд EPIC будет финансироваться за счет определенного процента от награды за майнинг блоков, вычитаемого из общей награды за блок, в соответствии со следующими ежегодными ставками:

Таблица 3: Ежегодные ставки майнинговых взносов в фонд – процент от награды за майнинг блока.

Год	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028
% от награды за майнинг блоков	8.88 %	7.77 %	6.66 %	5.55 %	4.44 %	3.33 %	2.22 %	1.11 %	1.11 %	0 %

VIII. Заключение

Epic стремится стать признанным ‘децентрализованным цифровым серебром', средством обмена, аналогом признанной позиции Биткоина, как децентрализованного цифрового золота. Вновь введя утраченную взаимозаменяемость в гораздо более энергоэффективную и экологически безопасную аппаратную магистраль, Epic Cash меняет баланс сил в пользу отдельных пользователей, что резко контрастирует с последними тенденциями централизации. Сочетание экономики Биткоина, теории игр и проверенной формулы доказательства работы с лучшими современными технологиями блокчейна приводит к созданию надежной, неизменной и децентрализован-ной валюты (Epic), которая является масштабируемой, взаимозаменяемой и защищает конфиденциальность ее пользователей. Блокчейн Epic Cash является открытым, общедоступным, без границ, и устойчивым к цензуре. Он сохраняет конфиденциальность и ценности своих пользователей и вознаграждает тех, кто использует свое оборудование для поддержки сети с помощью майнинга. Каждая монета Epic майнится при использовании POW. Эмиссия начинается с нуля (нет премайна), поэтому запуск сети организован честно; в настоящий момент, работает функциональная тестовая сеть.

Ключевые факты о Epic Cash:

- **Майнинг начинается августа 2019.**

- **Блокчейн Epic Cash основан на MimbleWimble.**

  Определяющими особенностями протокола являются:

  1. **Cut-Through** – удаление избыточной информации из блокчейна для повышения эффективности использования пространства, поощрения широкомасштабного участия в валидации сети и управления децентрализацией;
  2. ***CoinJoin*** – объединение транзакций в блоке для обеспечения взаимозаменяемости криптовалюты Epic;
  3. ***Протокол Dandelion++*** – распространение транзакций путем коммутации через переплетенные каналы и разделение через широкую сеть нод, что приводит к разрыву связи между транзакциями и их источником;
  4. **Нет адресов кошельков** – использование большой мультиподписи для генерации одноразовых приватных(закрытых) ключей для транзакционных сторон, что полностью устраняет необходимость в использовании адресов кошельков.

- **Монетарная политика Epic Cash** предназначена для синхронизации циркуляционного запаса Epic и циркуляционного запаса Биткоина примерно за 9 лет, и достижения максимальной эмиссии одновременно с Биткоином – в 2140 году. Такая дефляционная политика гарантирует прозрачность, предсказуемость эмиссии и дефицит, что способствует безопасности долгосрочного хранения стоимости.

- **Майнинг** который инкорпорирует CPU, GPU, и ASIC при использовании соответствующих алгоритмов, RandomX, ProgPow, и CuckA-Too31+, чтобы облегчить массовое внедрение и эффективность сети.

IX. Технические характеристики

Имя проекта: EpicCash
Имя валюты: Epic
Время блока: 60 секунд
Размер блока: 1 Мб
Начальный запас: 0
Окончательный запас: 21,000,000
Генезис-блок: августа 2019
Консенсус: RandomX (CPU), ProgPow (GPU) и CuckATоо31+ (ASIC)

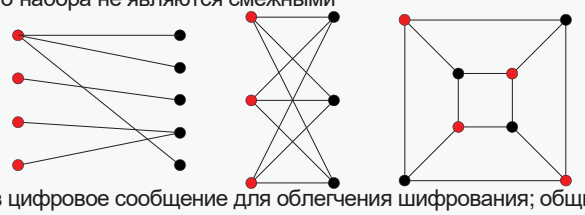
Ссылки:

www.epic.tech

t.me/EpicCash – Telegram

t.me/EpicCashRussian

X. Глоссарий

ASIC	Интегральные схемы специального назначения; чипы, разработанный для одной цели
Двудольный граф	Набор вершин графа, разложенных на два непересекающихся набора таким образом, что никакие вершины графа в пределах одного набора не являются смежными [15]. 
Ослепляющий фактор	случайный элемент, введенный в цифровое сообщение для облегчения шифрования; общий секрет между двумя сторонами, который используется при шифровании входных и выходных данных конкретной транзакции, а также открытый и закрытый(приватный) ключи транзакционных сторон[16].
Награда за блок	новые монеты Epic, распределенные сетью в качестве награды за вычисления, выполненные для проверки транзакций в новом блоке
Кэш	аппаратный или программный компонент, который хранит данные, чтобы в будущем запросы на эти данные могли обслуживаться быстрее.
Циркуляционный запас	количество монет Epic, существующих в данный момент времени
CPU	Центральный процессор: компьютерный компонент, отвечающий за интерпретацию и выполнение большинства команд из другого аппаратного и программного обеспечения компьютера.
Cut-Through	процесс блокчейна MimbleWimble, при котором входы и соответствующие потраченные выходы удаляются, чтобы освободить место в блоке, уменьшая объем данных, необходимых для хранения в блокчейне.
Децентрализация	состояние дисперсии в отношении операций и управления в сети..
Эмиссия	создание новых монет Epic, заработанных майнерами в виде награды за блок. Монеты Epic создаются каждые 60 секунд после подтверждения транзакций в блокчейне
Сингулярность Epic	точка, в которой Циркуляционный запас Epic будет синхронизирован с циркуляционным запасом Биткоина (май 2028).
Избыток (MimbleWimble)	разница между выходами и входами, плюс сигнатуры (для аутентификации и доказательства отсутствия инфляции).
Взаимозаменяемость	это свойство товара или сырья, при котором отдельные единицы, по существу, взаимозаменяемы, и каждая из частей взаимозаменяема с другой частью.
Генезис (Событие)	майнинг первого блока Epic и официальное начало блокчейна.
GPU	Графический процессор: блок, содержащий программируемый логический чип (процессор), предназначенный для отображения функций. Пользовательские графические процессоры могут хорошо подходить для майнинга криптовалюты.
Халвинг (для Биткоина)	происходит каждые 4 года. Уровень предложения снижается на 50% после каждого события халвинга.
Хэш	значение, вычисленное на основе базового входного числа с использованием хэш-функции
Алгоритм хэширования (функция)	математический алгоритм, который преобразовывает данные произвольного размера в хэш фиксированного размера, используемый для генерации и проверки цифровых подписей, кодов аутентификации сообщений (MAC) и других форм аутентификации.
Гомоморфное шифрование	метод выполнения вычислений зашифрованной информации без ее предварительного дешифрования (в программировании)
Неизменность	состояние, при котором объект не может быть изменен после его создания.
Вход (MimbleWimble)	Компонент транзакции MimbleWimble, представляющий отправляющую сторону транзакции; создан из выходов предыдущих транзакций.
I/O	ввод/вывод; взаимодействие между системой обработки информации, такой как компьютер, и внешним миром, человеком или другой системой обработки информации.

[15] http://mathworld.wolfram.com/BipartiteGraph.html

[16] Macdonald, Andrew, *Grin Coin and MimbleWimble: An Introductory Guide*, 18 October, 2018, https://cryptobriefing.com/grin-coin-mimblewimble-introduction/

Максимальный запас	количество монет Epic, после достижения которого циркуляционный запас больше не будет увеличиваться (21,000,000 Epic).
Memory-Hard	использование большого количества оперативной памяти для предотвращения одновременных попыток запуска параллельных подключений. Функции Memory-hard - это алгоритмы, для которых время вычислений в основном определяется доступной памятью для хранения данных.
Дерево Меркла	структура данных, используемая в приложениях информатики. В блокчейнах, деревья Merkle обеспечивают эффективную и безопасную проверку контента в больших структурах данных
MimbleWimble	протокол , выдвинутый автором под прозвищем Том Элвис Джедусор, в чате разработчиков Биткоина.
Мультиподпись	схема цифровой подписи, которая позволяет группе пользователей подписывать один документ. Как правило, алгоритм мультиподписи создает объединенную подпись, которая более компактна, чем набор отдельных сигнатур от всех пользователей[17].
Нода	компьютер, который подключается к сети блокчейна и разветвляется к другим нодам в сети, для однорангового распространения информации о транзакциях и блоках.
Односторонняя агрегированная сигнатура (OWAS)	подпись транзакции, состоящая из множества подписей (сигнатур), которая зашифрована таким образом, что очень сложно вычислить отдельные сигнатуры, которые являются частью совокупности.
Output (MimbleWimble)	компонент транзакции MimbleWimble, представляющий собой получателя транзакции; используется в качестве входных данных для последующих транзакций
Схема обязательств Педерсена	криптографический примитив, который позволяет проверяющему зафиксировать выбранное значение без раскрытия какой-либо информации о нем и без того, чтобы проверяющий мог отменить фиксацию значения.
Приватный (закрытый) ключ	небольшой кусочек кода, который в сочетании с открытым ключом используется для запуска алгоритмов шифрования и дешифрования текста. Он создается как часть криптографии с открытым ключом во время асимметричного шифрования и используется для дешифрования и преобразования сообщения в читаемый формат.
Proof of Work (PoW)	часть данных, которую сложно (дорого и занимает много времени) создать, но которую легко проверить другим, и которая удовлетворяет определенным требованиям. Proof of Work часто используются при генерации криптовалютных блоков.
Публичный (открытый) ключ	открытый ключ создается в криптографии с открытым ключом, использующей алгоритмы шифрования с асимметричным ключом. Открытые ключи используются для преобразования сообщения в нечитаемый формат.
RAM (Запоминающее устройство с произвольной выборкой)	чипы быстрого доступа для хранения данных, в которых хранятся операционная система (ОС), прикладные программы и данные, используемые в текущий момент; благодаря этому, процессор может получить быстрый доступ к данным
Rangeproof	верификация обязательства, которое проверяет, что сумма входных данных транзакции больше, чем сумма выходных данных транзакции, и что все значения транзакции являются положительными. Rangeproofs гарантирует, что монетарная эмиссия не была подделана.
(Цифровая) сигнатура	(Цифровая) Подпись - стандартная часть протокола блокчейна, в основном используемая для защиты транзакций и блоков транзакций, передачи информации, управления контрактами и для любых других случаев, когда важно обнаружение и предотвращение любых внешних вмешательств. Она обеспечивает три преимущества хранения и передачи информации в блокчейне: • Она показывает, были ли отправленные данные подделаны; • Проверяет участие конкретной стороны в сделке; • Может иметь юридическую силу.
SRAM (Статическая память с произвольным доступом)	Random Access Memory (RAM), которая сохраняет биты данных в своей памяти до тех пор, пока подается питание.
Пропускная способность	количество транзакций в секунду, которое может быть выполнено данным протоколом криптовалюты.
Trustlessness (не требует доверия)	Качество криптовалютной сети, позволяющее соблюдать правила протокола без принуждения со стороны центрального органа.

[17] Bellare, Mihir, Neven, Gregory, 2007, *Identity-based Multi-signatures from RSA*, Lecture Notes in Computer Science vol. 4377, https://link.springer.com/chapter/10.1007%2F11967668_10

EPIC CASH

EPIC PRIVATE INTERNET CASH