**РЕФЕРАТ**

**Блокчейн** — выстроенная по определённым правилам непрерывная последовательная цепочка блоков, содержащих информацию.

В блокчейн можно хранить записи о денежных переводах. И в криптовалютах blockchain как раз используется для фиксирования информации о том, кто, кому и сколько виртуальных денег перевел. Но в нем также можно хранить и данные о выданных кредитах, правах на собственность, нарушении правил дорожного движения, бракосочетаниях. В общем, все, что можно записать на бумаге, можно записать и в блокчейн с одним лишь отличием – в блокчейн просто нереально подменить или подделать записи. Все это привело к тому, что за последние годы блокчейн завоевал немалую популярность как в финансовой области, так и в бизнесе, и даже в социальной сфере.

Однако, помимо пользы и удобства, новые разработки имеют и свои недостатки. Стоит проанализировать, какие риски технологии блокчейн упускают из вида многие энтузиасты и чем может быть чревато неосторожное применение незнакомой технологии. Для этого нужно разобраться, что такое блокчейн, устройство блокчейна, как технология влияет на различные сферы деятельности человека и как от них зависит, а также влияние и зависимость ее от других технологий.

//описать проблемы????

Поняв все это, можно убедиться, что в действительности блокчейн может отрицательно повлиять как на отдельную личность, так и на общество в целом. Однако знание и трезвая оценка негативных факторов помогут избежать ряда проблем, которые может повлечь за собой необдуманное использование механизма.

**2. Введение, цель и задачи проекта**:

Сегодня люди живут в мире стремительно развивающихся технологий, в мире индустриальной революции 4.0, во время массового внедрения киберфизических систем в производство. Прогресс несет в себе множество благ, новых перспектив, однако любое действие имеет противодействие, поэтому прогресс сопряжен с рисками и отрицательными эффектами, которые существуют вне зависимости от того, осведомлены люди о их существовании или нет.

Цель проекта – анализ и исследование последствий развития технологий блокчейн и связанных с ними рисков в социальной сфере.

На сегодняшний день технология Blockchain у всех на слуху. Она является ярким представителем новейших информационных технологий индустриальной революции 4.0. Как и другие технологии этой группы, она несет в себе глобальные риски.

В рамках данного студенческого научно исследовательского проекта будут рассмотрены следующие проблемы и риски связанные с развитием технологии Blockchain: *Отсутствие регулирования, Сложность системы, Проблема производительности,* **Преждевременное внедрение,** *Вред для экологии***.**

Целью данной проекта является анализ рисков и проблем, связанных с информационной технологией Blockchain, и поиск путей их минимизации и устранения.

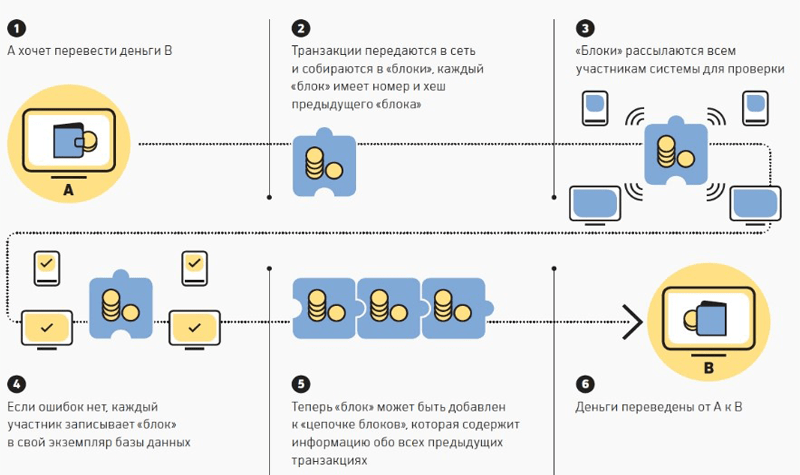
**3) Объект и предмет проекта**

Слово blockchain (блокчейн) состоит из двух слов. Первое – block и второе – chain. В переводе на русский язык означает цепь. Если не вдаваться в технические подробности функционирования, можно дать легкое, понятное определение данной технологии. Блокчейн – база данных, состоящая из цепочек транзакций, имеющая определенные правила и предоставляющая доступ к информации. Всё это исключает мошеннические действия, кражу персональных данных, защищает имущественные права и т. д.

В целом, блокчейн - это огромное количество электронных таблиц, объединенных в общую базу данных. Также понятие блокчейн можно отнести к группе реестров, позволяющих простым пользователям менять базовый код и наблюдать за общим прохождением процесса транзакции.

Основные принципы работы блокчейна достаточно легко понять: технология работает как распределенный реестр, где можно хранить любую информацию, которая будет скрыта от неавторизованных лиц благодаря криптографическому шифрованию, а копии данного реестра будут храниться на компьютерах всех пользователей. Взломать такой реестр практически невозможно, а информацию, которая содержится в нем, нельзя подделать, изменить или отредактировать.

Эта модель действительно очень проста в использовании, что позволяет работать в этой базе без посредников. Например, в результате продажи какой-то крупной компании один человек пообещал другому быстро выплатить оговоренную сумму. Но сделать это не просто. Во-первых, вывести деньги, во-вторых, доставить достаточно крупную сумму. Все эти пункты можно обойти, достаточно отправить эти деньги в базу, а там транзакция будет выполнена в кратчайшие сроки и на максимальном уровне безопасности.



В целом, идея создания этой финансовой модели в том, чтобы максимально обезопасить любую транзакцию, начиная от сделок «века» и заканчивая самыми маленькими денежными переводами. Но в то же время сделать все экономические операции наиболее просматриваемыми, легкодоступными и прозрачными. Кроме этого, технология блокчейн должна облегчить жизнь пользователям. Все операции, проводимые как конторами, так и частными лицами, станут намного быстрее и дешевле, так как перестанут быть нужными навыки таких профессий, как юрист, нотариус. Но всё же один из самых важных плюсов в создании таких систем – структурирование и объединение в единые базы данных все финансовые и любые, представляющие экономический интерес операции, проводимые на нашей планете.

Таким образом, блокчейн идеально подходит для сферы финансов и, в частности, для проведения международных платежей. Процесс международных переводов, который обычно занимает большое количество времени, средств и участвующих сторон, благодаря блокчейну значительно сократит время транзакций, расходы, а также уберет необходимость в сложной информационной структуре. Так, в сентябре 2016 года британский банк [Barclays](https://www.barclayscorporate.com/insight-and-research/technology-and-digital-innovation/what-does-blockchain-do.html) и стартап Wave провели первую успешную торговую сделку с использованием блокчейна. Более того, многие представители финансового сектора [объединяются](https://decenter.org/blockchain/94-why-microsoft-jpmorgan-and-bp-bet-on-blockchain-rus) в альянсы и консорциумы, такие как EEA, R3 и Hyperledger, для развития и внедрения блокчейн-решений в своем секторе.

### **Сферами применения блокчейна** являются: сфера криптовалют, Банковский сектор, инвестиции и биржи, Земельный реестр, Удостоверение личности, Платёжное средство.

### **1)Банковский сектор, инвестиции и биржи**

### В российском банковском секторе к технологии проявляют интерес такие компании как ВТБ и Сбербанк.О разработках и планах использования технологии блокчейн заявили платёжные системы VISA, Mastercard, Unionpay и SWIFT.Лондонское подразделение Дойче Банка Innovation Lab разрабатывает систему инвестиций на основе блокчейн-технологии, ускоряющую, упрощающую и удешевляющую процесс инвестирования засчёт исключения или сокращения роли посредников, адвокатов (поверенных), аудиторов и клиринговых агентов.В июле 2017 года S7 Airlines и Альфа-банк запустили в эксплуатацию блокчейн-платформу автоматизации торговых операций с агентами на базе Ethereum.

### **2)Земельный реестр**

### Швеция, Украина и ОАЭ планируют вести земельный реестр при помощи технологии блокчейн.

### Правительство Индии борется с земельным мошенничеством при помощи блокчейн. Андхра-Прадеш стал первым индийским штатом, где правительство предприняло шаги по внедрению блокчейн решений. Для этого в городе Вишакхапатнам будет создан технологический парк при участии блокчейн компаний Apla, Phoenix и Oasis Grace.

### В первом полугодии 2018 года будет проводиться эксперимент по использованию технологии блокчейн в целях мониторинга достоверности сведений Единого государственного реестра недвижимости (ЕГРН) на территории Москвы.

### **3)Удостоверение личности**

### В 2014 году основана компания Bitnation, предоставляющая услуги традиционного государства, такие как удостоверение личности, нотариат и ряд других.

### В июне 2017 Accenture и Microsoft представили систему цифровых удостоверений личности на блокчейне.

### В августе 2017 правительство Бразилии начало тестирование системы удостоверений личности на блокчейн.

### Финляндия идентифицирует беженцев при помощи блокчейн-технологий.

### В Эстонии работает блокчейн-система электронного гражданства.

### **4)Платёжное средство**

### Всемирная продовольственная программа использует технологию блокчейн для обеспечения беженцев продовольствием через существующие на местах торговые точки и сети вместо непосредственной раздачи продовольствия или выдачи беженцам наличных денег для покупки продуктов. Идея принадлежит Хуману Хададу (Houman Haddad). Для идентификации получателей продовольствия используется биометрия (сканирование радужной оболочки глаза). Экономия в 2018 году за счёт применения этой технологии только в Иордании составила 150 000 долларов в месяц.

### 

6) Математические модели и их описание

[модель энергопотребления](https://digiconomist.net/bitcoin-energy-consumption#assumptions)

Сегодня биткойн продолжает набирать популярность, а индустрия разрабатывать все новые приложения для работы с криптовалютой. Одной из причин такой популярности является строгая математическая база, на которой строится биткойн.

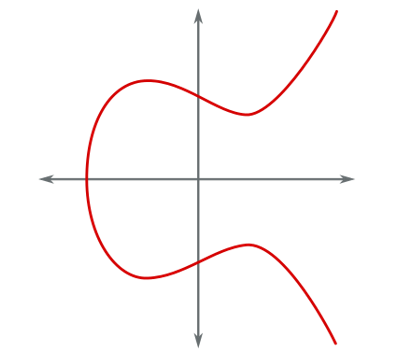
Благодаря этому система функционирует в условиях полного отсутствия доверия между участниками сети, исключая воздействие человеческого фактора.

Фундаментальной частью биткойна являются криптографические алгоритмы. В частности, алгоритм ECDSA — Elliptic Curve Digital Signature Algorithm, который использует эллиптические кривые (elliptic curve) и конечные поля (finite field) для подписи данных, чтобы третья сторона могла подтвердить аутентичность подписи, исключив возможность её подделки. В ECDSA для подписи и верификации используются разные процедуры, состоящие из нескольких арифметических операций.

Эллиптическая кривая над полем K — это кубическая кривая над алгебраическим замыканием поля K, задаваемая уравнением третьей степени с коэффициентами из поля K и «точкой на бесконечности». Одной из форм эллиптических кривых являются кривые Вейерштрасса.

y² = x³ + ax + b

Для коэффициентов a = 0 и b = 7 (используемых в биткойне), график функции принимает следующий вид:



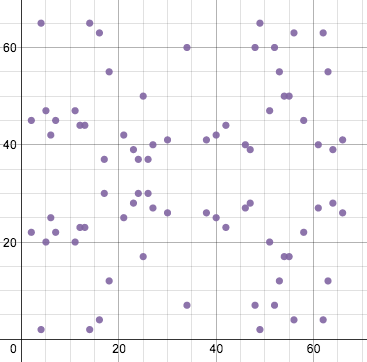
Эллиптическая кривая

В эллиптической криптографии (ECC) используется такая же кривая, только рассматриваемая над некоторым конечным полем. Конечное поле в контексте ECC можно представить как предопределенный набор положительных чисел, в котором должен оказываться результат каждого вычисления.

y² = x³ + ax + b (mod p)

Например, 9 mod 7 = 2. Здесь мы имеем конечное поле от 0 до 6, и все операции по модулю 7, над каким бы числом они ни осуществлялись, дадут результат, попадающий в этот диапазон.

Эллиптическая кривая биткойна, y² = x³ + 7, определенная на конечном поле по модулю 67, выглядит следующим образом:



*Эллиптическая кривая биткойна, определенная на конечном поле по модулю 67*

В протоколе биткойна зафиксирован набор параметров для эллиптической кривой и её конечного поля, чтобы каждый пользователь использовал строго определенный набор уравнений. Среди зафиксированных параметров выделяют уравнение кривой (equation), значение модуля поля (prime modulo), базовую точку на кривой (base point) и порядок базовой точки (order). Этот параметр подбирается специально и является очень большим простым числом.

В случае биткойна используются следующие значения:  
  
Уравнение эллиптической кривой: y² = x³ + 7  
  
Простой модуль: 2^256— 2^32 — 2^9 — 2^8 — 2^7 — 2^6 — 2^4 — 1 = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFC2F  
  
Базовая точка:  
  
04 **79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798** 483ADA77 26A3C465 5DA4FBFC 0E1108A8 FD17B448 A6855419 9C47D08F FB10D4B8  
  
Жирным шрифтом выделена координата X в шестнадцатеричной записи. За ней сразу следует координата Y.  
  
Порядок: FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE BAAEDCE6 AF48A03B BFD25E8C D0364141  
  
Этот набор параметров для эллиптической кривой известен как secp256k1 и является частью семейства стандартов SEC (Standards for Efficient Cryptography), предлагаемых для использования в криптографии. В биткойне кривая secp256k1 используется совместно с алгоритмом цифровой подписи ECDSA (elliptic curve digital signature algorithm). В ECDSA секретный ключ — это случайное число между единицей и значением порядка.

Это показывает, что максимальное количество секретных ключей (следовательно, биткойн-адресов) — конечно, и равняется порядку. Однако порядок является невероятно большим числом, так что случайно или намеренно подобрать секретный ключ другого пользователя нереально.

**7) РЕЗУЛЬТАТЫ ВЫПОЛНЕНИЯ ИССЛЕДОВАНИЯ**

*В ходе исследовательской работы были выявлены проблемы блокчейна.*

***Отсутствие регулирования***

Отсутствие регулирования в любом виде по умолчанию становится причиной возникновения небезопасной среды. В основном данная проблема на сегодняшний день относится к функционированию криптовалют. Сегодня проявлениями мошенничества, манипулирования рынком и спекуляциями в мире цифровых монет никого не удивишь. Так по данным веб - сайта <https://expandedramblings.com/index.php/blockchain-statistics/>

сумма похищенная хакерами из фонда DAO в 2016 году составил 50 млн. долларов.

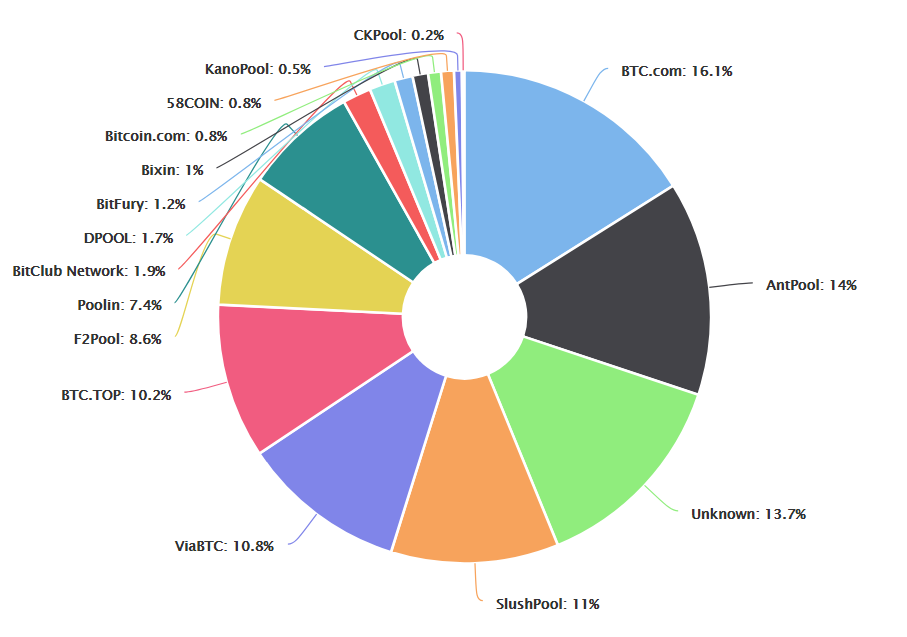
Определенная категория людей стала обвинять криптовалюту в том, что токены являются средством для отмывания денег, финансирования терроризма, торговли наркотиками, людьми и других вариантов преступной деятельности. А ведь после Биткоина появились Monero, Dash и еще ряд цифровых монет, обеспечивающих большую анонимность и конфиденциальность транзакций.

Майнинг превратился в прибыльный бизнес, которым стали заниматься люди, мотивированные не столько идеологией, сколько желанием обогатиться. По мере увеличения блокчейна росли и требования к производственным мощностям. Майнеры начали объединяться в пулы, многие из которых достигали гигантских масштабов. И именно в этот период появились риски блокчейн-контроля над нерегулируемой системой.

Захват контроля над сетью может произойти, если 51% и более мощностей окажутся сконцентрированными в руках одного человека или группы. В этом случае внутри доминирующего объединения будут подтверждаться только «свои» транзакции, в то время как все остальные будут отклоняться. В итоге все остальные участники окажутся перед выбором: присоединиться к доминантной структуре и играть по ее правилам, либо уйти из системы.

Риск подобного явления в сети Биткоина уже имел место. Тогда часть майнеров, руководствуясь идеологическими соображениями, покинула пул, и нарушения баланса не произошло. Однако на данный момент более 80% производственных мощностей контролируются 5 пулами, 4 из которых расположены в Китае. Основные производители оборудования для майнинга также находятся в Китае, кроме того, в Поднебесной одни из самых дешевых тарифов на электричество. Все эти факторы создают риск повторения ситуации предколлапса.

Распределение количества перебора хэшей

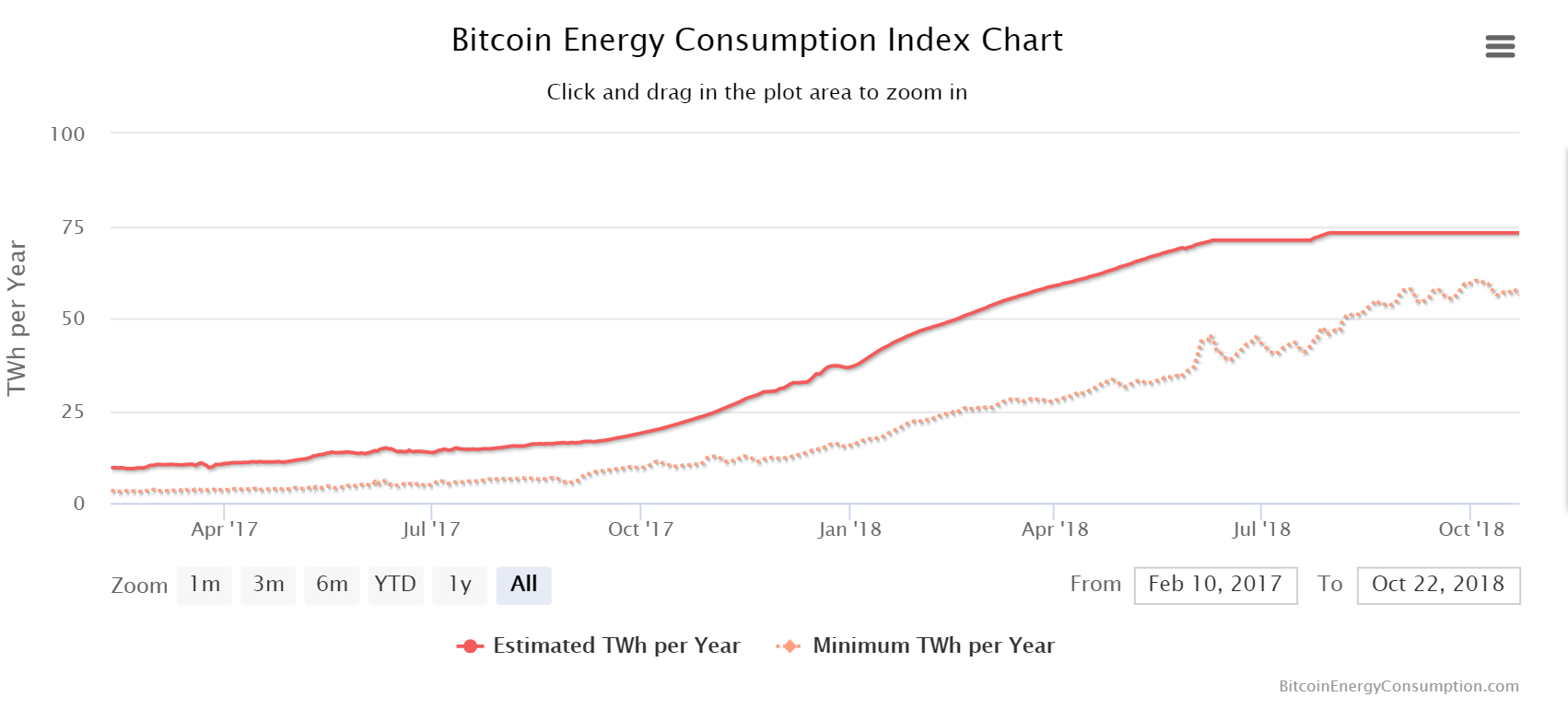


Централизация криптовалюты как таковая не критична. Опасность возникает, когда контроль над финансовой системой в сотни миллиардов долларов получает субъект, цели которого непонятны, а действия непредсказуемы. В этом случае управление рисками блокчейн-системы становится невозможным.

***Рост энергопотребления***

Как известно, для обеспечения безопасности функционирования децентрализованной сети, а также для достижения консенсуса в блокчейне, используются криптографические функции и методы, требующие дорогих и сложных вычислений.

Согласно [статистике Digiconomist](https://digiconomist.net/bitcoin-energy-consumption), за последний месяц энергопотребление сети Bitcoin увеличилось на 25% и в приведении к годовому счислению достигло 35,77 ТВт⋅ч. Это больше, чем годовое энергопотребление Дании (33 ТВт⋅ч), Беларуси (33,8 ТВт⋅ч) или Болгарии (34,9 ТВт⋅ч).

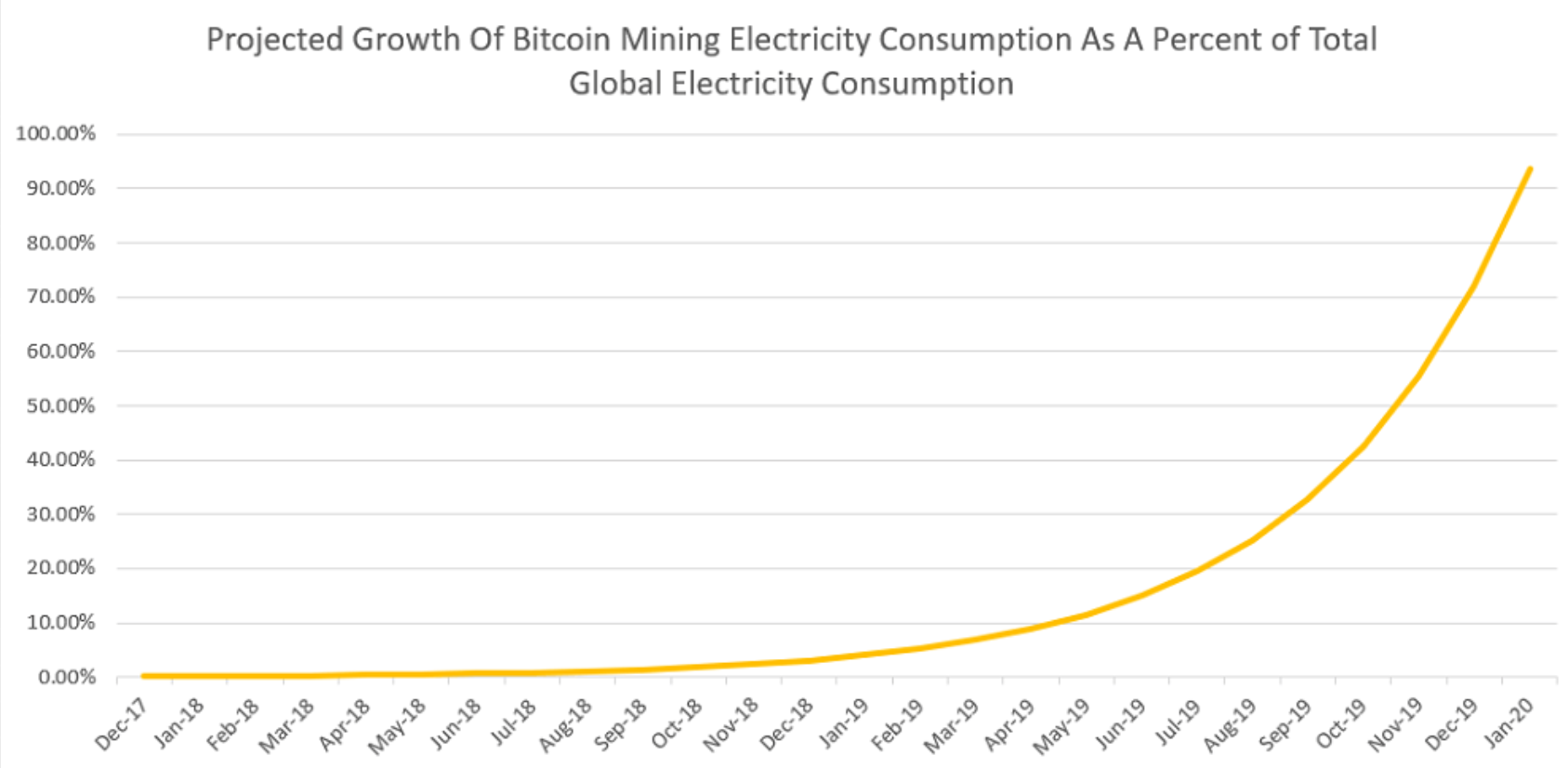


Согласно условной [модели энергопотребления](https://digiconomist.net/bitcoin-energy-consumption#assumptions), затраты на электричество коррелируют со стоимостью добываемых монет в определённой пропорции. Так что потребление электричества высчитывается исходя из рыночной стоимости добываемых монет и стоимости электричества 5 центов за 1 кВт⋅ч. Представители Digiconomist признают все условности и погрешности такой модели.

Если верить в «экономическую модель», то расходы электричества на майнинг будут расти пропорционально росту стоимости биткоина на рынке, с некоторым отстованием. Поэтому неудивительно, что энергопотребление растёт такими темпами: на 25-30% в месяц.

Если тенденция продолжится (рост на 25-30% в месяц), то ничего хорошего нас не ждёт. Например, сотрудники организации ZeroHedge [подсчитали](http://www.zerohedge.com/news/2017-11-24/will-bitcoin-mining-consume-all-worlds-current-electricity-production-feb-2020), что тогда к октябрю 2018 года энергопотребление сети Bitcoin сравняется с Великобританией (309 ТВт⋅ч), в июле 2019 года — с США (3913 ТВт⋅ч), а в феврале 2020 года Bitcoin «будет потреблять всё электричество в мире» (21 776 ТВт⋅ч).

По формуле роста на 25-30% в месяц получаем график.

******

“К 2050 году на майнинг биткоина будет требоваться энергия всей галактики, как кинетическая, так и потенциальная. А стоимость одного биткоина будет равняться стоимости слитка золота размером с Бетельгейзе. Земля победит бедность, потому что все будут невероятно богаты. Мировая медицина, получив мощный поток благотворительных средств от биткоиновых богачей в размере нцати квинтиллионов долларов, продвинется вперед и разработает лекарства от всех болезней в мире кроме простуды. Космические корабли будут бороздить межгалактическое пространство. Отключение воды в мае будет сокращено на один день.” - комментарий [BOM](https://geektimes.ru/users/bom/).

Есть и более оптимистические прогнозы. Например, опрошенные The Washington Post эксперты [считают](https://www.washingtonpost.com/news/energy-environment/wp/2017/12/19/why-the-bitcoin-craze-is-using-up-so-much-energy/?utm_term=.c44ec92e469f), что к 2020 году майнинг криптовалюты будет составлять всего лишь 1% энергопотребления США или 0,14% общемирового потребления. То есть всего лишь как 1−3 ядерных реактора. Конечно, это гораздо более консервативная и реалистичная оценка.

***Проблема производительности***  
 Из-за того, что объем данных блокчейна увеличивается ежеминутно, в ближайшей перспективе остро станет вопрос их хранения и скорости доступа к ним. Принципиально важно получить на него ответ организациям, для которых скорость совершения транзакций является первостепенным фактором.

“Скорость выполнения транзакций — это одна из самых острых технических проблем технологий распределенного реестра, в том числе блокчейна.” - Юрий Ковалев, управляющий партнер компании Performance Lab

**Преждевременное внедрение**  
 Важно понимать, что блокчейн сегодня находится только на стадии разработки и тестирования. Поэтому сама система еще недостаточно надежна. Многие пользователи относятся к критике технологии, так как у них отсутствует уверенность в ее качестве и стабильности услуг.  
  
Учитывая тот факт, что работа децентрализованной сети базируется на вовлеченности большого количества пользователей, ее успех и работоспособность напрямую зависят от уровня доверия к ней.

## **Другие риски и негативные факторы блокчейна**

Хотя многие варианты использования блокчейна призваны обеспечить людям большую свободу и, соответственно, безопасность и защиту личных данных, в определенных ситуациях криптография может сыграть обратную роль.

В 2017 году в Европе был принят закон «О праве на забвение». Этот закон обеспечивает возможность гражданину любой страны Евросоюза при соблюдении определенных условий затребовать удаление личных данных из большинства существующих баз, в первую очередь, общедоступных. Таким образом человек может начать жизнь «с чистого листа».

Однако если данные будут занесены в систему на базе блокчейна, возможность их удаления оказывается под вопросом. Даже при том, что это возможно технически, последствия потери огромного числа других данных из-за «перемотки» делает концепцию нереализуемой.

**“Неизвестности"**

Помимо объективных рисков и недостатков блокчейна, есть весьма спорные теории, которые могут быть рассмотрены как с положительной, так и с отрицательной точки зрения. Например, ряд экспертов считает, что блокчейн, как и другие системы автоматизации процессов, грозит потерей рабочих мест миллионам специалистов. Несмотря на то, что автоматизация выгодна в экономическом плане, с социальной точки зрения она является проблемой.

Другим неоднозначным фактором является неизменность информации. Тот факт, что информацию, уже внесенную в блоки цепи, нельзя изменить или подделать, можно рассмотреть как один из главных ценностей блокчейна. Благодаря этому пользователи могут быть уверены, что их транзакции будут направлены по адресу, баланс на криптокошельках останется неизменным и т. д. Несмотря на то, что иногда случаются досадные исключения, как атаки на DAO и Bitfinex, в общем этот тезис остается справедливым.Однако у такой «монолитной» надежности есть и обратная сторона медали. Например, неопытный пользователь может направить транзакцию на по тому адресу, и деньги будут переведены совсем другому человеку или компании. В этом случае уже не придет на помощь служба поддержки клиентов ЭПС, ведь Биткоин и другие криптовалюты работают по совершенно иному принципу.Также существует риск, что адрес блокчейн-кошелька будет введен некорректно, и транзакция окажется «зависшей» (то есть, деньги и до адресата не дойдут, и вернуть их не будет возможности). В какой-то момент такие транзакции разбираются (например, при форке), однако сколько времени процесс будет находиться в замороженном состоянии – неизвестно.Риск внесения некорректной информации в блокчейн присутствует не только в финансовой сфере. Например, при внедрении блокчейн-медкарт в систему здравоохранения, медработник может допустить ошибку при внесении информации в базу данных. Далее эта ошибочная информация попадает в блок, и дублируется во всех последующих. В итоге это может повлечь за собой назначение неправильного лечения с серьезными последствиями для здоровья, а иногда даже с риском для жизни пациента. Даже если ошибка будет выявлена, придется «отмотать» назад огромные объемы информации, что повлечет за собой риск потери данных и дополнительные затраты ресурсов.

Несмотря на то, что все больше людей начинает доверять блокчейну, многие не понимают даже базовых основ его работы. Эксперты отмечают, что блокчейн исключает посредничество в современных финансовых бизнес-процессах, однако в реальной жизни, банки достаточно успешно решают эту задачу. Неудивительно, что биткоин был создан сразу после финансового кризиса 2008 года, когда уровень недоверия к финансовым институтам достиг своего апогея. Вместе с тем, спустя десять лет подобных событий в истории больше не отмечалось. Поэтому возникает вопрос, готово ли человечество к значительным кардинальным переменам в сфере финансов?

Риски, которые влечет за собой развитие блокчейна в разы оправдываются той пользой, которую несет миру эта технология. Однако знание и трезвая оценка негативных факторов помогут избежать ряда проблем, которые может повлечь за собой необдуманное использование механизма

**9) Использованные источники:**

1.https://ru.wikipedia.org/wiki/Блокчейн

2.https://decenter.org/ru/blokcheyn

3.https://arazuvaev.ru/blokcheyntehnologiya

4.<https://coinnet.ru/problemy-blokchejna/#i-3>

<https://bitexpert.io/wiki/riski-tehnologii-blokchejn/>

<https://www.zerohedge.com/news/2017-11-24/will-bitcoin-mining-consume-all-worlds-current-electricity-production-feb-2020>

<https://bitexpert.io/wiki/vozmozhnosti-blokchejn-tehnologij-o-kotoryh-ty-ne-znal-i-vryad-li-uznaesh/>

https://bitexpert.io/wiki/chto-zhdet-blokchejn-predskazaniya-na-2018-god/

https://www.performance-lab.ru/blog/kak-testirovat-proizvoditelnost-blokchejna

5.Блокчейн. Схема новой экономики (Blockchain: Blueprint for a New Economy)

Мелани Свон, Олимп Бизнес, 2017;

6. Эпоха криптовалют. Как биткойн и блокчейн меняют мировой экономический порядок (The Age of Cryptocurrency: How Bitcoinand the Blockchain Are Challenging the Global Economic Order)

Пол Винья, Майкл Кейси, Манн, Иванов и Фербер, 2017.

7. «Блокчейн-революция. Как технология, стоящая за биткойном, меняет деньги, бизнес и мир» (Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World)

Дон Тапскотт, Алекс Тапскотт, ЭКСМО, 2017.

8. Блокчейн. Как это работает и что ждет нас завтра

Артем Генкин, Алексей Михеев, Альпина Паблишер, 2018.