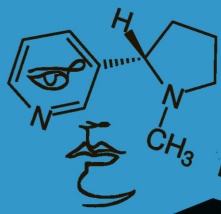


КУРИЛКА ГУТЕНБЕРГА

Наука делается здесь!

Денис Смирнов

КРИПТОВАЛЮТА

Аванта

Денис Сергеевич Смирнов
Криптовалюта
Серия «Курилка Гутенберга»

Текст предоставлен издательством
http://www.litres.ru/pages/biblio_book/?art=69216187
Криптовалюта: АСТ; Москва; 2023
ISBN 978-5-17-151869-1

Аннотация

Блокчейн – на протяжении последнего десятилетия это магическое слово приходится слышать все чаще. Почти каждый сейчас уже знает, что благодаря системе блокчейн в мире появились криптовалюты. Однако в чем же заключается уникальность этой технологии, которой эксперты пророчат роль универсального помощника для бизнеса? Что такое система децентрализованных финансов и, наконец, волнующая всех криптовалюта? Обо всем этом, а еще о том, при чем здесь шифры и математика, расскажет специалист в области криптоиндустрии Денис Смирнов.

Для широкого круга читателей.

В формате a4.pdf сохранен издательский макет.

Содержание

Денис Смирнов
Криптовалюта

Начало

Эта книга будет полезна тем, кто интересуется историей технологии блокчейн, тем, кто хочет узнать, как и где эта технология может быть применима и, наконец, тем, кто жаждет разобраться в том, как блокчейн и криптовалюты уже сегодня меняют формат человеческих взаимоотношений, а также какие перспективы они открывают перед человечеством.

Как автор, я стремлюсь не только донести до своих читателей поток информации, но и научить вас пользоваться теми достижениями, которые несут нам децентрализованные технологии. Возможно именно благодаря этой книге, дорогие читатели, у вас загорятся глаза так же, как это произошло со мной несколько лет назад, и вы захотите связать свою жизнь с децентрализованными технологиями.

Глава I. Введение

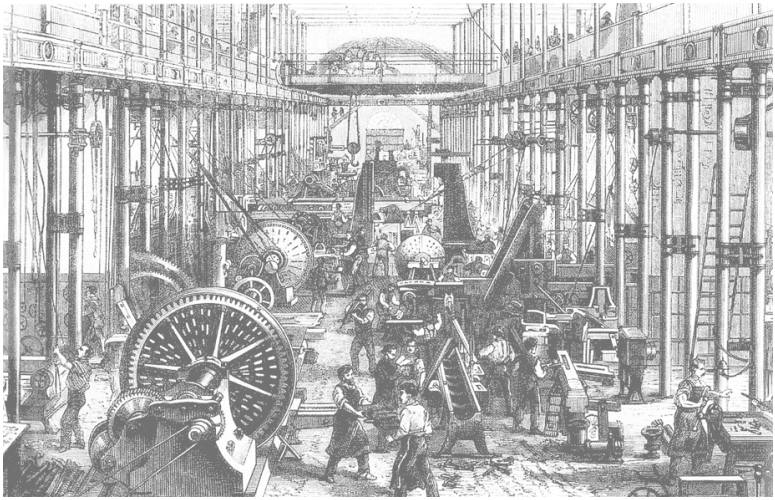
Это вступительная часть, в которой мы познакомимся с индустрией децентрализованных финансов и узнаем, почему, на мой взгляд, это направление является наиболее перспективным на сегодняшний день.

Четвертая промышленная революция

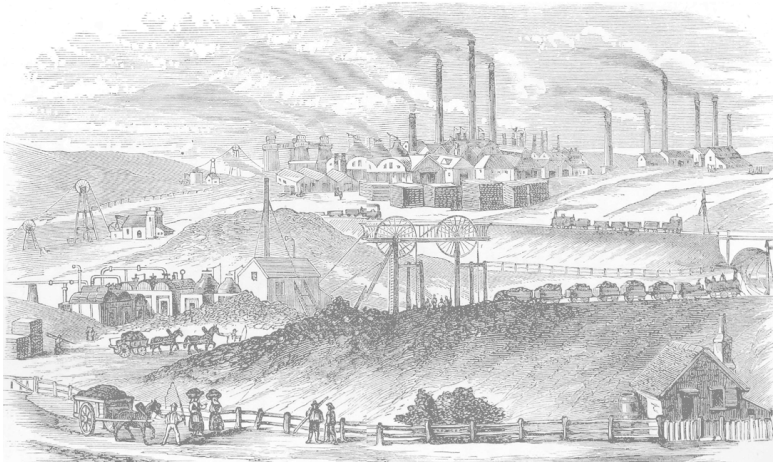
Мы живем в удивительное время! Нам повезло оказаться в самом начале очередной промышленной революции и собственными глазами лицезреть те грандиозные изменения, которые будут происходить в самых разных аспектах нашей жизни!

Еще совсем недавно, на рубеже XVIII–XIX веков, **человечество представляло собой в** основном аграрное общество с низким уровнем грамотности, низкой производительностью труда и низким уровнем жизни. Но изобретение парового двигателя позволило механизировать производство и подстегнуть общество к переходу на новый уровень. Этот период называют **первой промышленной революцией**. Тогда появление и внедрение новых технологий повлияло не только на сами процессы производства. Изменениям, так или иначе, подверглись практически все области жизни, обеспечив обществу переход от аграрного состояния к индустриальному. Резко выросла необходимость в образовании, люди стали перебираться в города, начался рост промышленности, – вслед за ним стал расти и уровень жизни.

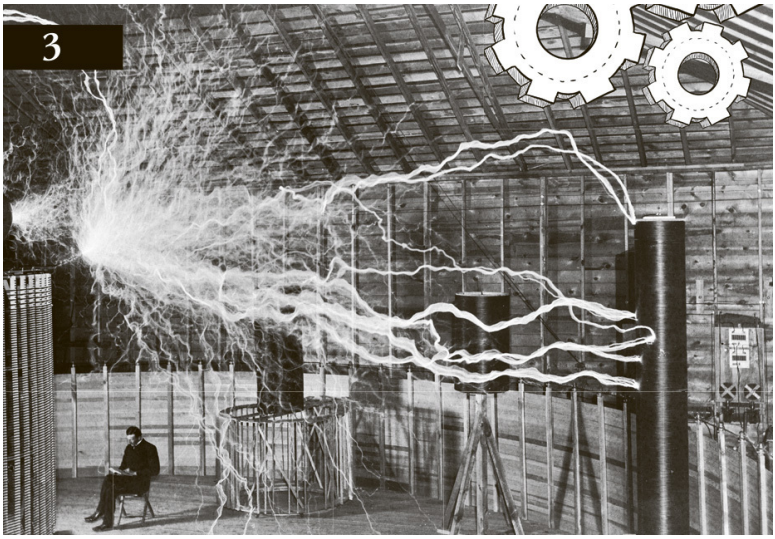
А совсем скоро, во второй половине XIX века, произошла **вторая промышленная революция**, когда развитие науки, открытие электричества и появление новых технологий позволило вывести производство на новый уровень, сделав его массовым. Это привело к дальнейшему развитию, росту урбанизации и повышению уровня жизни.



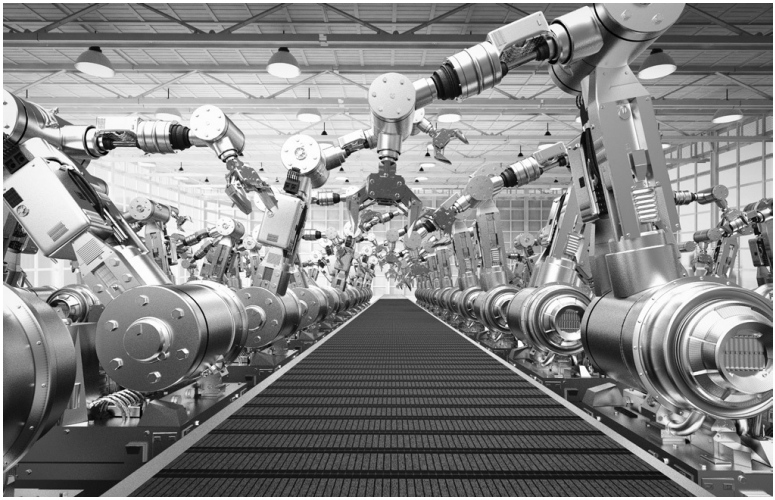
Первая промышленная революция

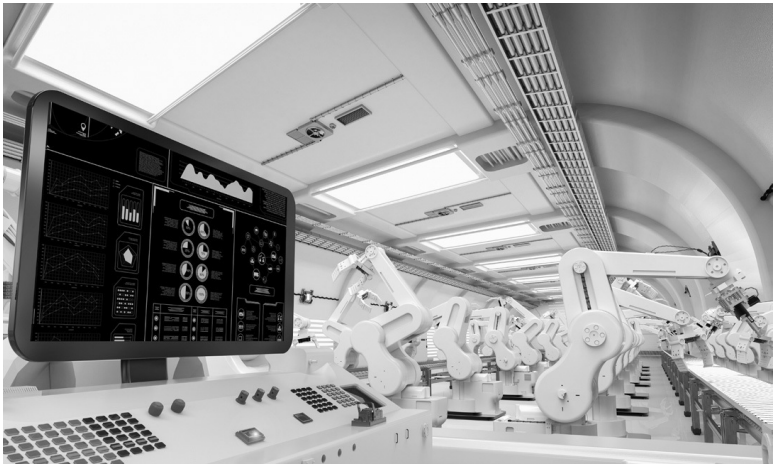


Вторая промышленная революция



Открытие электричества





Третья промышленная революция

Третья (или, как еще ее называют, циф-ровая) революция началась в середине XX века и продолжается по сей день. Ее основными движущими силами стали изобретение транзисторов и микропроцессоров, и широкое распространение вычислительной техники, прежде всего – персональных компьютеров, а также развитие Интернета и массовое применение персональных портативных устройств. Основа третьей промышленной революции – информационные технологии, позволившие автоматизировать производство.

При этом каждая революция сопровождалась резким увеличением производительности труда, ростом урбанизации, быстрым экономическим ростом (хотя до этого экономический рост был заметен лишь в масштабах столетий) и повышением жизненного уровня населения. Все вместе это приводило к существенным изменениям во всех аспектах жизни общества.

Сегодня мы стоим на пороге следующей, **четвертой промышленной революции**, или, как еще ее называют, **«Индустрии 4.0»**. Этому термину мы обязаны прошедшей в 2011 году промышленной выставке в Ганновере, где немецкие бизнесмены попытались представить, как будет выглядеть промышленность будущего.

В первую очередь для Индустрии 4.0 характерна **еще**

большая автоматизация производства. И хотя поначалу может показаться, что все это лишь продолжение цифровой революции, есть несколько факторов, которые позволяют считать эти изменения полноценной следующей промышленной революцией.

Во-первых, это **темпы развития**. Благодаря все ускоряющемуся техническому прогрессу эта промышленная революция, в отличие от предыдущих, развивается не линейными, а экспоненциальными темпами. Если между **первой** и **второй** революцией прошло почти 100 лет, то между **второй** и **третьей** – около 50, а разрыв между **третьей** и **четвертой** и вовсе исчисляется десятилетиями.

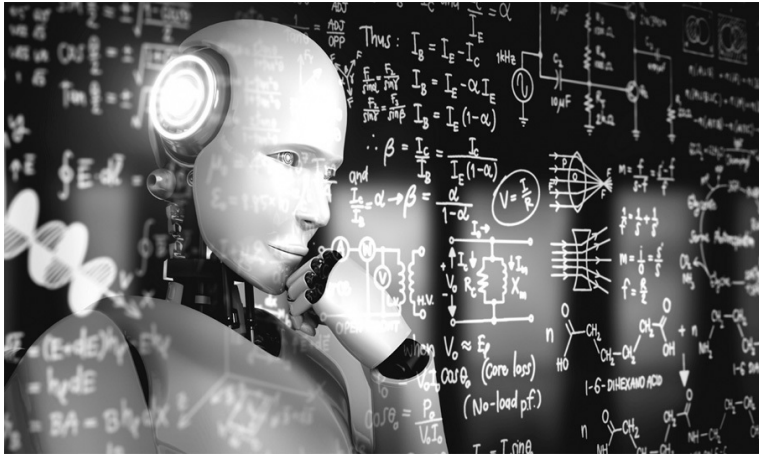
Во-вторых, это **широта и глубина проникновения технологий**. Сегодня научные прорывы не ограничиваются одной областью применения, а влияют и на смежные, приводя к взрывному росту инноваций во всех областях сразу. Так, например, удешевление систем хранения данных и развитие беспроводных сетей дали жизнь различным гаджетам, позволяющим постоянно отслеживать медицинские показатели пользователей и помогать врачам быстрее ставить диагнозы. Уже сегодня есть несколько примеров того, как носимые устройства для измерения сердечного ритма спасали жизнь людям, заметив отклонения еще до того, как человек почув-

ствовал недомогание.

В-третьих, это **системность воздействия**. Сочетание разнообразных технологий приводит к беспрецедентным изменениям сразу во многих областях: бизнесе, социуме и жизни, в целом. Меняются профессии, меняются варианты взаимодействия между людьми. Четвертая промышленная революция изменяет не только то, «что» и «как» мы делаем, но и то, «кем» мы являемся.

Вот основные тенденции, определяющие Индустрию 4.0.

Развитие искусственного интеллекта. Автоматизация многих процессов и услуг. Развитие робото-техники.



Возможность хранения и анализа больших данных.

Сегодня каждое устройство, имеющее доступ к интернету, от умного холодильника до датчиков, следящих за состоянием посевов на полях, становится участником глобального обмена информацией. И самое главное, что этот обмен может осуществляться вообще без участия человека – холодильник может сам узнать о недостатке компонентов для праздничного пирога и заказать их в магазине, а датчик отдаст команду дрону, если растениям необходим полив или удобрение. Сегодня можно говорить уже о таком понятии, как ***IoT – Internet of Things*** (интернет вещей), когда основными пользователями интернета становятся устройства, а человек – всего лишь гостем.

Децентрализация и удешевление производства продуктов и ресурсов, гораздо более гибкое управление масштабом производства с целью снижения издержек. Появление массовых возможностей для 3D-печати и дальнейшее удешевление технологии.

Развитие **«одноранговой экономики»**, где участники взаимодействуют друг с другом напрямую, без посредников. Расширение «пассивного предпринимательства» и sharing economy (экономики совместного потребления), когда выгоднее платить за временный доступ к продукту, чем владеть этим продуктом.

Повсеместное создание институтов и инфраструктуры **дополненной реальности** и протоколов ее общения с «умными» вещами. Таким образом, часть человеческих действий может быть перенесена на цифровой уровень.

Сегодня мы находимся **лишь в самом начале этих изменений** и, по мнению многих экспертов, ожидать серьезного присутствия основных атрибутов новой революции можно не ранее, чем в 2025 году, а наступления господства Индустрии 4.0 и превращения ее в мейнстрим – не ранее 2030-х.

Тем не менее уже сегодня мы можем наблюдать **первые результаты новой революции** , например, с помощью **3D-принтеров** печатаются как новые дома, так и медицинские

протезы. Благодаря **достижениям «горизонтальной экономики»** мы сдаем неиспользуемые комнаты в аренду через приложения или пользуемся автомобилями по модели каршеринга. А в сельском хозяйстве используются беспилотные летательные аппараты, которые позволяют наблюдать за состоянием посевов, отслеживать вредителей и распылять необходимые химикаты. Использование меток и датчиков позволяет увеличить урожайность и следить за здоровьем крупного рогатого скота.

Говоря о синергии между технологическими прорывами, можно привести в пример то, как удешевление систем хранения информации и производства различных датчиков, а также их миниатюризация позволяют нам говорить о потенциальной возможности объединить любые товары в единый «интернет вещей», где каждый предмет сможет собирать и анализировать данные о собственном состоянии и использовании и на основе этого принимать решения. Таким образом, машины смогут самостоятельно оптимизировать свою работу, следить за собственной исправностью и, если они нуждаются в ремонте, заказывать комплектующие. При этом точные сведения о необходимости тех или иных ресурсов позволят более грамотно планировать производство, что в свою очередь приведет к снижению издержек.

Новые проблемы современности

Однако новые технологии, естественно, несут и новые проблемы. Огромные объемы информации, которые генерирует человечество, заставляют нас все чаще задумываться над **вопросом проверки и верификации данных**. Все мы знаем про фейк-ньюс и про то, как пагубно они могут влиять на жизни людей.

Проблема защиты персональных данных также становится все более острой. Корпорации владеют все большим объемом данных о человеке и не стесняются торговать ими. Защищать информацию становится все сложнее, и есть риск, что в будущем это может стать одной из основных проблем человечества.

Одной из таких проблем также является **проблема доверия**. Есть множество областей, где участники не могут, да и не должны, доверять друг другу. Например, при денежных переводах, – нельзя просто так взять и перевести деньги кому-нибудь. Необходимо, чтобы кто-то третий (обычно в этой роли выступает банк) подтвердил, что у одного участника есть необходимая сумма и он может ей распоряжаться, а второй участник может ее получить. И лишь после того, как банк даст разрешение, перевод может быть осуществлен.

Нельзя продать квартиру без участия нотариуса, нельзя получить диплом без комиссии, и т. д.

При этом **наличие посредников делает всю систему уязвимой** из-за того, что посредники централизованы, и на них можно осуществить атаку. Банк можно взломать, подпись нотариуса – подделать, документы, лежащие в централизованном хранилище, можно изъять или заменить. Наличие посредников также значительно замедляет и удорожает любые взаимодействия. Электронное письмо мгновенно доставляется в любую точку земного шара, в то время как банковский перевод по реквизитам может выполняться несколько дней даже в пределах одной страны. При этом одним посредником дело не ограничивается, к примеру, если вы захотите отправить своей тетушке в Бразилию 10 000 $, то для этого потребуется помощь сразу четырех (!) банков: вашего локального банка, банка, осуществляющего трансграничные переводы в вашей стране, аналогичного банка в Бразилии и, наконец, банка, в котором у тетушки открыт счет. Все это займет несколько дней и будет стоить вам комиссии в несколько процентов от суммы перевода. Более того, после того, как вы отправите перевод, и до тех пор, пока тетушка не получит деньги на свой счет, вы даже не сможете узнать, где ваши деньги в определенный момент находятся!

Блокчейн помогает вынести вопрос доверия между

участниками «за скобки» и полностью исключить третью сторону из подобных взаимоотношений, что позволяет существенно снизить издержки и повысить скорость взаимодействий! По своей сути блокчейн, или технология распределенного реестра, – это децентрализованная база данных с гарантией прозрачности и целостности информации.

Но при всей кажущейся сложности такого определения **блокчейн** – это на самом деле очень просто. Это **знакомая всем амбарная книга** – множество строк с записями о чем-либо, объединенных постранично в большую книгу. При этом каждая страница содержит уникальный идентификатор, рассчитываемый из данных предыдущей страницы. А еще книга эта электронная и хранится сразу у нескольких человек, причем в открытом доступе, и каждый при желании может в нее заглянуть. Таким образом, чтобы тайно внести в такую книгу изменения, нужно будет не только исправить данные на конкретной странице, но и на всех страницах, которые были добавлены после нее (т. к. изменятся их контрольные суммы). А еще нужно будет одновременно подменить эту страницу сразу у всех владельцев, иначе обман раскроется, и данные будут сразу же исправлены на верные. Так и достигается упомянутая выше гарантия неизменности информации.

Благодаря именно этому свойству блокчейн может выступать вместо третьей стороны при совершении различных операций. **Доверие между участниками больше не зависит от авторитета** организаций, а строится на принципах математики и криптографии, делая посредников просто ненужными! Эта технология не является «Священным Граалем», но те области, в которых она применима: финансовые взаимоотношения, системы нотариата, учет авторских прав, отслеживание цепей поставок, и т. д., и т. п. – все эти области могут существенно выиграть от использования блокчейна.

Откуда же взялась эта технология? Более десяти лет назад, в 2008 году, произошел крупнейший в новейшей истории финансовый кризис. Помимо очевидных последствий,

он еще больше подорвал доверие к традиционной финансовой системе и подстегнул многих энтузиастов, десятилетиями искавших способ создания новой экономики, к поиску инновационных решений. В самом конце 2008 года в одной из групп рассылок, посвященных тематике электронных платежных средств, особо никому не известный участник, скрывавшийся под именем **Сатоши Накамото**, опубликовал небольшой документ, озаглавленный: «**Биткоин: система цифровой пиринговой наличности**». В этом документе содержались общие принципы той технологии, что мы сегодня знаем под именем блокчейн, а также описание базирующейся на ней платежной системы, построенной на принципах криптографии, а не доверия, и позволяющей любым двум участникам осуществлять перевод средств напрямую, без участия посредников.

Bitcoin: A Peer-to-Peer Electronic Cash System

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

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

Добавление новой информации в блокчейн требовало определенных вычислительных затрат от участников, но также позволяло защитить данные в системе, – так как отмена любой транзакции в сети требовала бы невероятно большой вычислительной мощности, которой ни один из участников системы просто не мог обладать. Таким образом, до тех пор, пока под совокупным контролем честных участников находится больше вычислительной мощности, чем под контролем группы действующих совместно злоумышленников, система является полностью защищенной. Этот прин-

цип получил название «**схемы доказательства работы**», которая используется до сих пор, позволяя особым участникам сети – майнерам – добавлять новые блоки в систему, получая за это вознаграждение, а также комиссии за включенные в блок транзакции. Изначально вознаграждение за майнинг составляло 50 биткоинов за «добытый» блок, но со временем, примерно каждые два года, оно стало уменьшаться в два раза. Следуя этому принципу, он называется «халвинг» (от английского halving – «уполовинивание»), сумма вознаграждения продолжит уменьшаться, пока, наконец, все биткоины из изначально запланированной эмиссии в 21 000 000 не будут добыты. По оценке экспертов, это произойдет не ранее 2140 года.

Биткоин не появился из ниоткуда, он был основан на множестве разработок других людей, криптографов и экономистов, пытавшихся создать новые электронные деньги еще с середины 90-х годов. Но до Сатоши никому не удавалось описать систему, которая была бы одновременно удобной, анонимной и защищенной.

3 января 2009 сеть была запущена! Постепенно вокруг нового проекта начало образовываться сообщество энтузиастов, которое поддерживает и развивает его и по сей день. Сам же Сатоши продолжал анонимно работать над проектом до 2010 года, а затем бесследно исчез. На сегодняшний день

никто достоверно так и не знает, кто же скрывается под этим именем. Но кем бы он ни был, его детище дало начало новой, непрерывно растущей индустрии, которая прямо сейчас меняет облик человеческих взаимо-отношений!

При этом не стоит забывать, что помимо преимуществ у любой технологии есть и свои минусы. Для блокчейна это, в первую очередь, **проблема масштабируемости,** или роста блокчейна, так как необходимость сохранять информацию обо всех транзакциях у каждого участника системы требует огромного количества места на диске. Размер блокчейна биткоина на сегодняшний день уже превосходит 250 Гб, и в будущем он будет только расти.

Также механизм доказательства работы, используемый биткоином, требует существенных вычислительных и, как следствие, энергетических затрат. По оценкам исследователей из Кембриджского университета, сейчас на добычу биткоина приходится около **0,25 % всей потребляемой электроэнергии в мире** – это больше энергии, чем тратят, например, Швейцария, Греция или Израиль!

Еще одной существенной проблемой криптовалютной индустрии остается **инерционность традиционной экономической системы,** а также проблема интеграции криптовалют в легальное правовое поле. Дело в том, что банки не горят желанием терять свои позиции и не хотят рисковать возможностью постоянного получения прибыли. При этом банки обладают довольно серьезным влиянием на правительства и законодательные органы. Тем не менее многие государства начали осознавать потенциал и преимущества криптовалютной экономики и уже начинают легализовывать криптовалюты.

Так или иначе, все эти проблемы вполне разрешимы, – разработчики активно работают над устранением технических проблем. Многие из них на сегодняшний день стоят

уже не так остро, либо уже решены. Также и государства сегодня видят в криптовалютах не однозначную угрозу существующему порядку, а новую динамично развивающуюся индустрию, выиграть от использования которой могут все участники рынка. Сегодня уже ни у кого нет сомнений в том, что **блокчейн и криптовалюты с нами «всерьез и надолго»,**

Конец ознакомительного фрагмента.