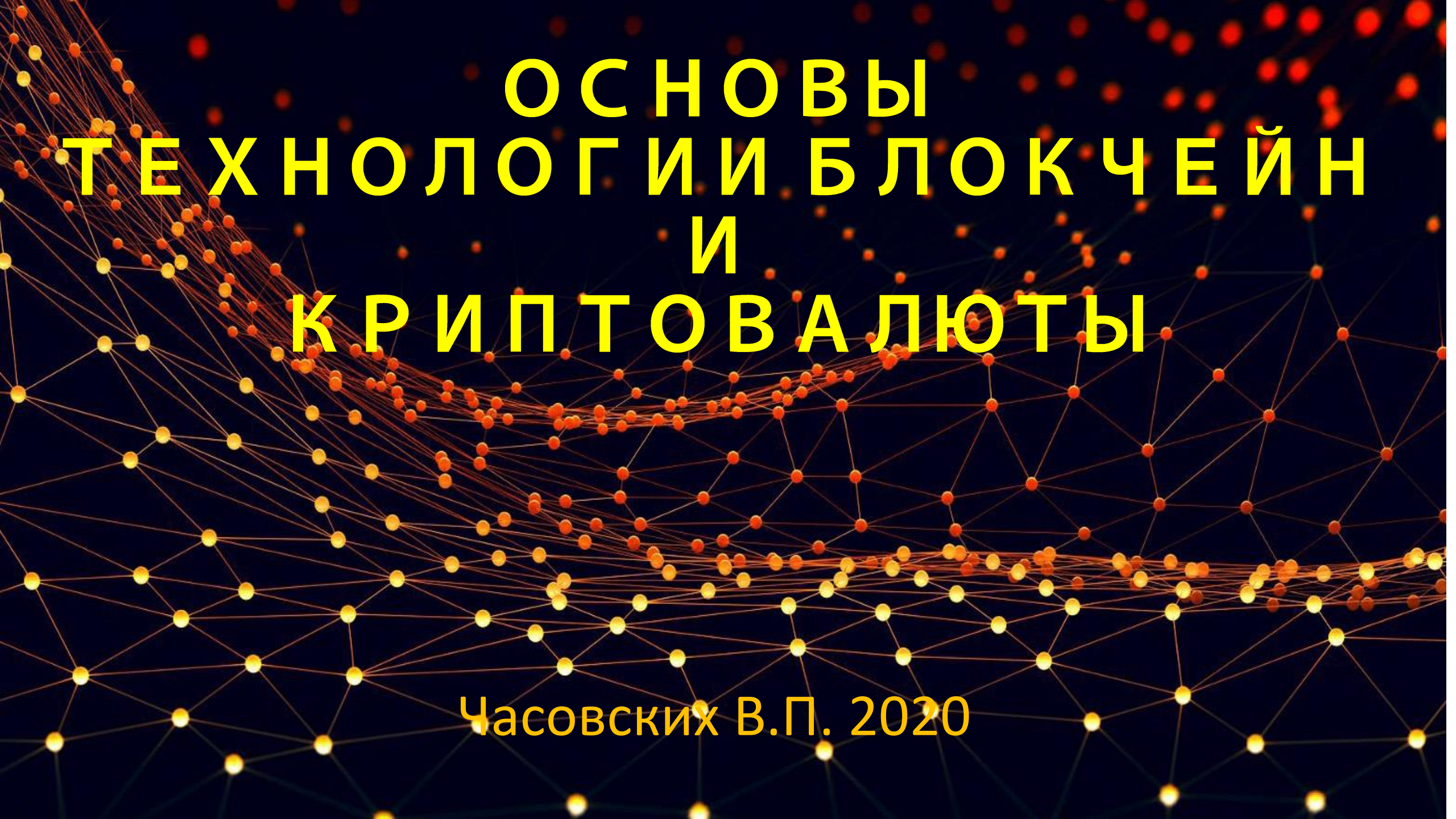




# ОСНОВЫ ТЕХНОЛОГИИ БЛОКЧЕЙН И КРИПТОВАЛЮТЫ

Часовских В.П. 2020

# Децентрализованные приложения

Почти все современные интернет-приложения являются централизованными, есть сервер к которому подключены компьютеры клиентов. **Функции сервера:** хранения данных и кода программы. **Функции клиента:** обработка данных происходит исключительно на стороне клиента.

Конечно, основным достоинством данной архитектуры является простота организации.

Проектировщики и разработчики информационных систем находятся в привычных и комфортных условиях Windows. Имеются удобные и развитые средства разработки графического пользовательского интерфейса, простые в использовании средства разработки систем баз данных.

# Децентрализованные приложения

## Достоинства такой архитектуры:

- многопользовательский режим работы с данными;
- удобство централизованного управления доступом;
- низкая стоимость разработки;
- высокая скорость разработки;
- невысокая стоимость обновления и изменения ПО.

## Недостатки:

- проблемы многопользовательской работы с данными: последовательный доступ, отсутствие гарантии целостности;
- низкая производительность (зависит от производительности сети, сервера, клиента);
- плохая возможность подключения новых клиентов;
- ненадежность системы.



# Децентрализованные приложения

Почти все современные интернет-приложения являются централизованными, есть сервер к которому подключены компьютеры клиентов. **Функции сервера:** хранения данных и кода программы. **Функции клиента:** обработка данных происходит исключительно на стороне клиента.

Конечно, основным достоинством данной архитектуры является простота организации.

Проектировщики и разработчики информационных систем находятся в привычных и комфортных условиях Windows. Имеются удобные и развитые средства разработки графического пользовательского интерфейса, простые в использовании средства разработки систем баз данных.

# Децентрализованные приложения

Распределенные приложения работают на множестве серверов одновременно! Это необходимо при наличии большого сетевого трафика и объема данных, особенно, если отказ в обслуживании приложения недопустим. В распределенных приложениях данные реплицируются между разными серверами, чтобы обеспечивать высокую доступность данных. Централизованные приложения могут быть распределенными, а могут и не быть таковыми. Но децентрализованные приложения всегда распределенные. Например, Google, Facebook, Slack, Dropbox и им подобные являются распределенными, а простой сайт нет, пока трафик не слишком большой.

# Децентрализованные приложения

Одним из **основных преимуществ** ДП является гарантия анонимности пользователя.

Но многие приложения нуждаются в проверке личности пользователя перед началом работы. Поскольку центрального органа верификации не существует, подтверждение личности пользователя становится проблемой. Мы должны предоставить приложению цифровой идентификатор, который ДП сможет понять и проверить. Основная проблема сегодня заключается в том, что не каждое ДП работает с цифровой идентификацией, и лишь редкие пользователи знают, как получить цифровой идентификатор.

# Децентрализованные приложения

Существуют различные формы цифровых идентификаторов. На сегодняшний день наиболее популярной и рекомендованной формой является цифровой сертификат, который также называют сертификатом открытого ключа или удостоверением личности. Это электронный документ устанавливающий право собственности на открытый ключ. В общем случае пользователь имеет закрытый ключ, открытый ключ и цифровой сертификат. Пользователь хранит закрытый ключ в тайне и никому его не показывает. Открытый ключ может быть показан кому угодно. Цифровой сертификат содержит публичный ключ и информацию о том, кто владелец ключа.

# Внутренняя валюта приложений

Чтобы централизованное приложение сохраняло работоспособность в течение длительного времени, его владельцу нужно как-то извлекать прибыль. У ДП нет владельца, но все равно узлы ДП нуждаются в оборудовании и сетевых ресурсах для поддержания работы. То есть узлы ДП должны приносить какую-то выгоду в обмен на усилия по поддержанию их работоспособности. Именно здесь вступает в игру внутренняя валюта. Большинство ДП имеют встроенную внутреннюю валюту. Точнее, большинство успешных ДП имеют встроенную внутреннюю валюту.



# Внутренняя валюта приложений

Лишь те узлы, которые способствуют поддержанию и управлению ДП, **зарабатывают валюту**. Узлы, которые только считывают данные, не получают ничего. Например, в Bitcoin только майнеры зарабатывают биткойны за успешно добытые блоки.

Самый важный вопрос о цифровой валюте — почему ее вообще кто-то ценит? Согласно экономической теории, все, что имеет достаточный спрос и недостаточное количество, **имеет ценность**.

Заставляя пользователей расплачиваться внутренней валютой приложения, мы решаем проблему **спроса**. Чем больше пользователей используют ДП, тем больше спрос на валюту и тем выше она ценится.

Установление фиксированного объема выпускаемой валюты приводит к ее нехватке и повышает стоимость. Обычно валюта вводится в оборот постепенно, чтобы вновь подключившиеся узлы тоже имели возможность заработать.

# Недостатки внутренней валюты приложений

Единственным недостатком внутренней валюты является то, что ДП не могут быть бесплатными для всех. Это как раз тот случай, когда централизованные приложения берут верх, потому что они могут быть монетизированы за счет рекламы, предоставления премиальных API для сторонних приложений и т. п. Поэтому они могут быть бесплатными для обычных пользователей. Мы не можем интегрировать рекламу в ДП, потому что некому проверять рекламу на соответствие стандартам. Клиенты могут не отображать рекламу, потому что не имеют выгоды от показ объявлений.

# Приложения с контролируемым доступом

ДЕЦЕНТРАЛИЗОВАННЫЕ приложения (ДП) полностью открыты и не контролируют доступ. Это значит, что любой желающий может подключиться к одноранговой сети без идентификации личности.

С другой стороны, контролируемые ДП (КДП) не распахнуты настежь для все желающих. КДП наследуют все качества открытых ДП, за исключением того, что требуется разрешение для подключения к сети.

# Приложения с контролируемым доступом

## Понятие регистра

Регистр — это, в общем случае, просто список транзакций.

Регистр отличается от данных. В регистр мы можем только добавить новую транзакцию, тогда как в данных мы можем добавлять, модифицировать и удалять записи о транзакции База данных может быть использована как реализация регистра.

# Приложения с контролируемым доступом

**Транзакция** - группа последовательных операций с базой данных, которая представляет собой логическую единицу работы с данными.

Транзакция может быть выполнена либо целиком и успешно, соблюдая целостность данных и независимо от параллельно идущих других транзакций, либо не выполнена вообще, и тогда она не должна произвести никакого эффекта.

Транзакции обрабатываются транзакционными системами, в процессе работы которых создаётся история транзакций.



# Приложения с контролируемым доступом

**Блокчейн** — это особая структура данных, применяемая для создания децентрализованного регистра.

Блокчейн состоит из блоков (block), особым образом соединенных в цепочку (chain).

Блок содержит набор транзакций, хеш предыдущего блока метку времени (время создания блока) и другую информацию (например: сумму отчисления за блок). Поскольку каждый блок содержит хеш предыдущего блока, они связаны в цепочку.

Каждый узел сети хранит полную копию блокчейна.

# Блокчейн и биткойн

**Биткойны** (монеты) вводятся в оборот путем выплаты вознаграждения майнерам, успешно создавшим новые блоки. В сети Bitcoin блокчейн хранит транзакции Bitcoin.

Майнинг, также добыча (от англ, mining — добыча полезных ископаемых) — деятельность по поддержанию распределенной платформы и созданию новых блоков с возможностью получить вознаграждение в форме новых единиц и комиссионных сборов в различных криптовалютах, в частности в Биткойн. Производимые вычисления требуются для обеспечения защиты от повторного расходования одних и тех же единиц, а вознаграждение стимулирует людей расходовать свои вычислительные мощности и поддерживать работу сетей.

# Блокчейн и биткоин

Суть **майнинга** состоит в том, что в разных уголках Земли, находятся компьютеры, которые решают математические задачи, результатом которых является создание биткоина.

Процесс выпуска (добычи) распределяется по всем участникам системы, что обеспечивает безопасность и не контролируется единым выпускающим центром.

Основным преимуществом блокчейна является автоматизация контроля над **безопасностью транзакций**.

Блокчейн предотвращает мошенничество и злоупотребления и может решить множество других проблем, в зависимости от способа реализации и использования.

# Блокчейн и экономика

**Блокчейн** — это многофункциональная и многоуровневая информационная **технология**, предназначенная для надежного учета различных **активов**.

Потенциально эта технология охватывает все без исключения сферы экономической деятельности и имеет множество областей применения. В их числе: финансы, экономика и денежные расчеты, а также операции с материальными (реальная собственность, недвижимость, автомобили и т. п.) и нематериальными (права голосования, идеи, репутация, намерения, медицинские данные, личная информация и т. п.) активами. Блокчейн создает новые возможности по поиску, организации, оценке и передаче любых дискретных единиц. По сути, это **новая организационная парадигма для координации любого вида человеческой деятельности**.

# Приложения блокчейн вне финансовых рынков

Потенциальные выгоды от применения блокчейн-технологии лежат не только в сфере экономики — они распространяются на политику и гуманитарные, социальные и научные области. Технологические возможности блокчейна уже задействуются для решения реальных общественных задач.

Помимо ситуаций, когда общественные интересы выходят за рамки национальных границ, целые отрасли экономики смогут освободиться от избыточного регулирования и лицензирования, навязанных иерархическими структурами, лоббистами и группами влияния внутри государств. Это позволит создавать новые модели бизнеса, не отягощенные ненужными посредниками.

# Приложения блокчейн

Каждый **актив** в блокчейне кодируется уникальным идентификатором, по которому актив можно отслеживать, контролировать и обменивать, продавать или покупать.

Это означает, что любые виды материальных (дома, автомобили и другие) и цифровых активов можно регистрировать и совершать с ними транзакции на блокчейне.



# БЛОКЧЕЙН 1.0, 2.0 и 3.0

Стало понятно, что благодаря своим экономическим, политическим, гуманитарным и юридическим преимуществам биткойн и блокчейн-технологии превращаются в мощнейшую инновацию, способную коренным образом изменить большинство аспектов жизни общества.

Для упорядочения и удобства разделим различные — существующие и потенциальные — технологические аспекты блокчейн на три категории: блокчейн 1.0, 2.0 и 3.0.

**Блокчейн 1.0** — это валюта. Криптовалюты применяются в различных приложениях, имеющих отношение к деньгам, например системы переводов и цифровых платежей.

# БЛОКЧЕЙН 1.0, 2.0 и 3.0

**Блокчейн 2.0** - это контракты. Целые классы экономических, рыночных и финансовых приложений, в основе которых лежит блокчейн, работают с различными типами финансовых инструментов — с акциями, облигациями, фьючерсами, залладными, правовыми титулами, умными активами и умными контрактами.

**Блокчейн 3.0** — это приложения, область применения которых выходит за рамки денежных расчетов, финансов и рынков. Они распространяются на сферы государственного управления, здравоохранения, науки, образования, культуры и искусства.

# БЛОКЧЕЙН - обучение

Умные контракты на основе блокчейна могут иметь множество применений. Одно из них — умные контракты на **обучение**. MOOK (массовые открытые онлайн-курсы) с использованием биткойна и умные контракты на обучение воплощают идею открытия развивающегося рынка умных контрактов на обучение, доступного всем желающим по всему миру, так же как обычные MOOK предоставили принципиальную возможность дистанционного обучения всем желающим.

# Блокчейн как информационная технология

Наверное, самое главное в блокчейне состоит в том, что это **информационная технология**.

Но много у нее и других аспектов. В качестве средства децентрализации блокчейн являет собой новую революционную парадигму вычислений. У блокчейна есть встроенный экономический уровень, которого у **технологий интернета** никогда **не было**.

Блокчейн — механизм координации, схема отслеживания привязки к единичным записям, кредита, подтверждения и компенсационных вознаграждений для поощрения участия любого интеллектуального агента в любом виде сотрудничества, не использующая доверенных посредников. Блокчейн сам по себе является «децентрализованной сетью доверия»

# Блокчейн как информационная технология

**Блокчейн** — облачная площадка для транснациональных компаний.

**Блокчейн** — это средство предоставления персонализированных децентрализованных служб управления и поддержки образования и экономического развития.

**Блокчейн** является средством доказательства существования и точности содержимого любого документа или другого цифрового актива на определенный момент времени.

**Блокчейн** обеспечивает интеграцию и автоматизацию взаимодействия людей и машин, служит сетью платежей между машинами (machine-to-machine, M2M) в экономике машин и между «вещами» в «интернете вещей». Блокчейн и криптовалюта — основа для механизма платежей и бухучета в M2M-коммуникациях.

# Основные сведения о криптовалюте

Биткойн и другие криптовалюты (альткойны) представляют собой **цифровые деньги**, средство покупки и продажи товаров в интернете.

Чтобы пользоваться ими, нужно создать электронный кошелек — либо заведя новый онлайн-кошелек в браузере, либо загрузив кошелек-приложение для обычного компьютера или смартфона с сайта Bitcoin.org, Blockchain.info или сайтов других разработчиков биткойн-кошельков.

При создании кошелька автоматически генерируется биткойн-адрес, а также открытый и закрытый ключи.

Биткойн-адрес — это, как правило, идентификатор, начинающийся с «1» или «3» и состоящий из 26—34 буквенно-цифровых символов, которые указывают на получателя биткойн-платежа,



# Асимметричная криптография

Когда кошелек инициализируется или создается впервые, автоматически генерируется адрес, а также открытый и закрытый ключи. В основе биткойна лежит механизм **асимметричного шифрования**, в котором открытый ключ распространяется свободно, а закрытый ключ надо держать при себе.

Программа формирует биткойн-адрес, выбирая случайное число и создавая пару «открытый и закрытый ключи». Ключи в паре математически связаны и проверяются в процессе расходования биткойнов. Закрытый ключ генерируется автоматически, но для создания биткойн-адреса нужны дополнительные операции.

# Асимметричная криптография

Вычислить закрытый ключ, соответствующий открытому ключу, невозможно из-за однонаправленности операции хеширования (или природы другого применяемого для вычисления этого значения механизма), а также непомерно высокой стоимости этой операции (нужен колоссальный объем вычислительных ресурсов на время, намного превышающее время подтверждения транзакции). Для получения биткойнов достаточно адреса, а для отправки нужна пара из открытого и закрытого ключей.

## РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

1. Лелу, Лоран. **Блокчейн от А до Я. Все о технологии десятилетия**/Лоран Лелу ; [пер. с фр. А.Н. Степановой]. - Москва : Эксмо, 2018. - 256 с. — (Мир технологий). ISBN 978-5-699-98942-3
2. Свон, Мелани. **Блокчейн: Схема новой экономики** / Мелани Свон : [переводе английского]. — Москва : Издательство Олимп—Бизнес, 2018. — 240 с., ил. ISBN 978-5-9693-0360-7
3. Варнавский, Андрей Владимирович. **Блокчейн на службе государства** : монография / А.В. Варнавский, А.О. Бурякова, Е.В. Себеченко. — Москва : КНОРУС, 2020. — 218 с. ISBN 978-5-406-07599-9
4. Прасти Н. **Блокчейн. Разработка приложений**: Пер. с англ. — СПб.: БХВ-Петербург, 2018, —256 с.: ил. ISBN 978-5-9775-3976-0
5. Дрешер Д. **Основы блокчейна: вводный курс для начинающих в 25 небольших главах** / пер. с англ. А. В. Снастина. - М.: ДМК Пресс, 2018.-312 с.: ил. ISBN 978-5-97060-591-2



## РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

6. Могайар, Уильям. **Блокчейн для бизнеса** / Уильям Могайар ; предисл. Виталика Бутерина ; [пер. с англ. Д. Шалаевой]. - Москва : Издательство «Эксмо», 2018. — 224 с. — (Top Business Awards). ISBN 978-5-699-98499-2
7. Тапскотт, Дон. **Технология блокчейн: то, что движет финансовой революцией сегодня** / Дон Тапскотт, Алекс Тапскотт; [пер. с англ. К. Шашковой, Е. Ряхиной]. — Москва : Эксмо, 2018. — 448 с. — (Top Economics Awards). ISBN 978-5-699-95092-8
8. Лоуренс, Тиана. **Блокчейн для чайников.** : Пер. с англ. - СПб. : ООО “Альфа-книга”, 2018. - 272 с. : ил.- Парал. тит. англ. ISBN 978-5-9500295-6-1 (рус.)
9. Антонопулос А. М. **Осваиваем биткойн** / пер. с англ. А. В. Снастина. - М.: ДМК Пресс, 2018. - 428 с.: ил. ISBN 978-5-94074-965-3
10. Винья, Пол **Эпоха криптовалют. Как биткойн и блокчейн меняют мировой экономический порядок** / Пол Винья, Майкл Кейси; пер. с англ. Э. Кондуковой; [науч. ред. А. Форк]. — М.: Манн, Иванов и Фербер, 2017. -432 с. ISBN 978-5-00100-747-0
11. Шнайер, Брюс. **Прикладная криптография: протоколы, алгоритмы и исходный код на С**, 2-е юбил. изд.: Пер. с англ. — СПб.: ООО “Альфа-книга”, 2017. - 1040 с.: ил. - Парал. тит. англ. ISBN 978-5-9908462-4-1 (рус.)

## РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

12. Генкин А. Блокчейн: Как это работает и что ждет нас завтра / Артем Генкин, Алексей Михеев. — М.: Альпина Паблишер, 2018. - 592 с. ISBN 978-5-9614-6558-7