**MINISTERUL EDUCAȚIEI ȘI CERCETĂRII**

**UNIVERSITATEA DE STAT „ALECU RUSSO” DIN BĂLŢI**

**FACULTATEA DE ŞTIINŢE REALE, ECONOMICE ȘI ALE MEDIULUI**

**CATEDRA DE MATEMATICĂ ȘI INFORMATICĂ**

**BLOCKCHAIN**

**РЕФЕРАТ**

**ПО ДИСЦИПЛИНЕ «INFORMATICA GENERALĂ»**

**Autor:**

Studentul grupei IS11Z

**Nicolai Russu**

**\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Conducător știintific:**

**Olesea SKUTNIȚKI**

magistru, asist. univ.

\_\_\_\_\_\_\_\_\_\_\_\_\_

**BĂLȚI, 2022**

[ВВЕДЕНИЕ 3](#_Toc103521230)

[1.Blockchain 4](#_Toc103521231)

[1.1.Что такое Blockchain ? 4](#_Toc103521232)

[1.2.История BlockChain. 5](#_Toc103521233)

[2.Реализация в системе Биткойн. 6](#_Toc103521234)

[2.1.Блок транзакций. 6](#_Toc103521235)

[2.2.Цепочка блоков. 7](#_Toc103521236)

[2.3.Подтверждение транзакций. 9](#_Toc103521237)

[2.4.Двойное расходование. 9](#_Toc103521238)

[2.5.Сложность. 10](#_Toc103521239)

[2.5.1. Unix-время 10](#_Toc103521240)

[3.Проблемы и возможные пути их решения. 12](#_Toc103521241)

[3.1.Публичные блокчейны. 12](#_Toc103521242)

[3.2.Частные блокчейны. 13](#_Toc103521243)

[3.3. Консорциумные блокчейны. 13](#_Toc103521244)

[4.Применение вне сферы криптовалют. 14](#_Toc103521245)

[4.1. Банковское дело. 14](#_Toc103521246)

[4.2. Кибербезопасность. 14](#_Toc103521247)

[4.3. Удостоверения личности. 15](#_Toc103521248)

[Выводы 16](#_Toc103521249)

[библиография 17](#_Toc103521250)

ВВЕДЕНИЕ

Блокчейн — это распределенная база данных, которая содержит информацию обо всех транзакциях, проведенных участниками системы. Информация хранится в виде цепочки блоков. В каждом из них записано определенное число транзакций.[3]

Впервые термин появился как название полностью реплицированной распределённой базы данных, реализованной в системе «Биткойн», из-за чего блокчейн часто отождествляют с реестром транзакций в различных криптовалютах. Однако технология цепочек блоков может быть распространена на любые взаимосвязанные информационные блоки. Появившаяся в октябре 2008 года система Биткойн стала первым применением технологии блокчейн.

Блокчейн просто известен как список записей, который часто обновляется. Блокчейн не позволяет изменять данные. Растущий список записей называется блоками, и каждый блок содержит адрес или хэш предыдущего блока, который имеет временную метку и информацию о транзакционных данных. Блокчейн представляет собой открытую, децентрализованную, распределенную и цифровую книгу, которая используется для записи транзакций в системах без каких-либо изменений данных.[2]

Существуют различные типы блокчейнов, которые являются публичными, частными и консорциумными. Публичный блокчейн не имеет ограничений доступа. С помощью Интернета любой может отправить транзакцию и подтвердить ее. Публичный блокчейн - это биткойн. Закрытая блокчейн - это разрешение, это означает, что однажды может присоединиться, когда сетевой администратор предоставит приглашение для доступа. Этот блокчейн рассмотрен для компаний, которые заинтересованы в этой технологии и хотят использовать ее без предоставления своих данных в общедоступную сеть. Блокчейн консорциума называется полу-децентрализованным. Это также разрешение, но в этом случае многие компании используют одну и ту же сеть и получают доступ к выделенному для них узлу.

Технология блокчейн использует ряд технологий, таких как P2P-сети, криптография с закрытым ключом и программ. Он широко используется и показывает большой успех в области распространения и регистрации информации. Он используется в криптовалюте. Это обеспечивает безопасность и уменьшает проблему несанкционированных расходов.[2]

1. Blockchain

1.1. Что такое Blockchain

Блокчейн — цепь из блоков выстроенная по определённым правилам непрерывная последовательная цепочка блоков (связный список), содержащих информацию. Связь между блоками обеспечивается не только нумерацией, но и тем, что каждый блок содержит свою собственную хеш-сумму и хеш-сумму предыдущего блока. Изменение любой информации в блоке изменит его хеш-сумму. Чтобы соответствовать правилам построения цепочки, изменения хеш-суммы нужно будет записать в следующий блок, что вызовет изменения уже его собственной хеш-суммы. При этом предыдущие блоки не затрагиваются. Если изменяемый блок последний в цепочке, то внесение изменений может не потребовать существенных усилий. Но если после изменяемого блока уже сформировано продолжение, то изменение может оказаться крайне трудоёмким процессом. Дело в том, что обычно копии цепочек блоков хранятся на множестве разных компьютеров независимо друг от друга.[1]

Главное преимущество блокчейна в его прозрачности, потому что каждый может ознакомиться с информацией внутри блоков, но никто не в силах ее изменить или уничтожить.

Аналогия с блокчейном — ожерелье. Каждая бусина –– это «блок» или запись действия. Это ожерелье — или «chain» (цепь) — не может быть уничтожено или разрушено. Таким образом, блокчейн — это нерушимая цифровая запись действий. Надежность этой системы позволила использовать ее для повышения эффективности денежных операций и обмена информацией среди частных лиц, корпораций и даже госсектора.[2]



Рис.1.Как работает блокчейн.

1.2. История BlockChain

Официально история блоков и цепей начинается 31 октября 2008 года, когда некто под псевдонимом Сатоши Накамото упомянул блокчейн в white paper (базовом документе) про сеть первой криптовалюты — биткоина. Основополагающие принципы применения децентрализации и неизменности для учета документов были заложены еще в 1960-1970 годах, но ближе всего к ним можно отнести работы ученых Стюарта Хабера и У. Скотта Сторнетта, которые в 1991 году описали схему последовательного создания блоков, в которых находится хеш. Технология была даже запатентована, но стала для своего времени вертолетом Да Винчи — технической возможности для реализации идеи не было, и интерес к ней пропал. Срок патента истек в 2004 году, всего за четыре года до появления Сатоши и его white paper.[1]

За последние годы было много версий того, кто мог быть автором этого манифеста. Убедительны некоторые доказательства в пользу его русскоязычного происхождения. Первый блок был сгенерирован в 2009 году, а на сегодня только криптоинструментов на базе разных модификаций блокчейна в мире циркулирует свыше 2 тыс. видов.

2. Реализация в системе Биткойн

2.1. Блок транзакций

Блок транзакций — специальная структура для записи группы транзакций в системе Биткойн и аналогичных ей. (Рис.2) Транзакция считается завершённой и достоверной , когда проверены её формат и подписи, и когда сама транзакция объединена в группу с несколькими другими и записана в специальную структуру — блок. Содержимое блоков может быть проверено, так как каждый блок содержит информацию о предыдущем блоке. Все блоки выстроены в одну цепочку, которая содержит информацию обо всех совершённых когда-либо операциях в базе. Самый первый блок в цепочке первичный блок рассматривается как отдельный случай, так как у него отсутствует родительский блок.[1]

Блок состоит из заголовка и списка транзакций. Заголовок блока включает в себя свой хеш, хеш предыдущего блока, хеши транзакций и дополнительную служебную информацию. В системе Биткойн первой транзакцией в блоке всегда указывается получение комиссии, которая станет наградой майнеру за созданный блок. Далее идёт список транзакций, сформированный из очереди транзакций, ещё не записанных в предыдущие блоки. Критерий отбора из очереди задаёт майнер самостоятельно. Это не обязательно должна быть хронология по времени. Например, могут включаться только операции с высокой комиссией или с участием заданного списка адресов. Для транзакций в блоке используется древовидное хеширование, аналогичное формированию хеш-суммы для файла в протоколе BitTorrent. Транзакции, кроме начисления комиссии за создание блока, содержат внутри параметра input ссылку на транзакцию с предыдущим состоянием данных (в системе Биткойн, например, даётся ссылка на ту транзакцию, по которой были получены расходуемые биткойны). Операции по передаче майнеру комиссии за создание блока не имеют «входных» транзакций, поэтому в данном параметре может указываться любая информация.

Созданный блок будет принят остальными пользователями, если числовое значение хеша заголовка равно или меньше определённого целевого числа, величина которого периодически корректируется. Так как результат хеширования функции SHA-256 считается необратимым, на данный момент нет алгоритма получения желаемого результата, кроме случайного перебора. Если хеш не удовлетворяет условию, то в заголовке изменяется параметр nonce и хеш пересчитывается. Обычно (статистически) требуется большое количество пересчётов. Когда вариант найден, узел рассылает полученный блок другим подключенным узлам, которые проверяют блок. Если ошибок нет, то блок считается добавленным в цепочку и следующий блок должен включить в себя его хеш.

Величина целевого числа, с которым сравнивается хеш, в системе Биткойн корректируется через каждые 2016 блоков. Запланировано, что вся сеть системы Биткойн должна тратить на генерацию одного блока примерно 10 минут, на 2016 блоков — около двух недель. Если 2016 блоков сформированы быстрее, то целевое число немного уменьшается и получить удовлетворяющий ему хеш подбором параметра nonce становится труднее, в противном случае целевое число увеличивается. Изменение сложности вычислений не влияет на надёжность сети Биткойн и требуется лишь для того, чтобы система генерировала блоки почти с постоянной скоростью, не зависящей от вычислительной мощности участников сети.[1]

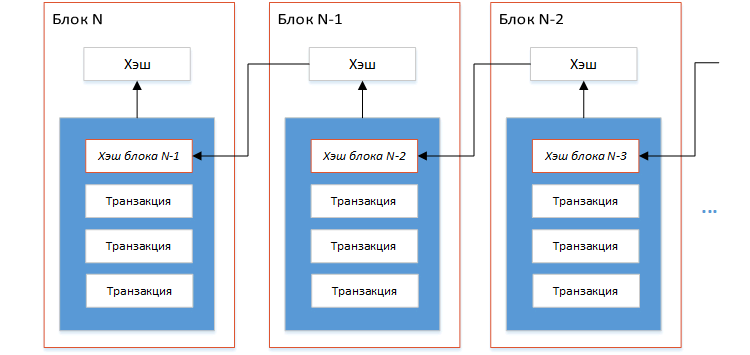


Рис.2. Блоки транзакций

2.2.Цепочка блоков.

Блоки одновременно формируются множеством «майнеров». (Рис.3) Удовлетворяющие критериям блоки отправляются в сеть, включаясь во все репликации распределённой базы блоков. Регулярно возникают ситуации, когда несколько новых блоков в разных частях распределённой сети называют предыдущим один и тот же блок, то есть цепочка блоков может ветвиться. Специально или случайно можно ограничить ретрансляцию информации о новых блоках (например, одна из цепочек может развиваться в рамках локальной сети). В этом случае возможно параллельное наращивание различных ветвей. В каждом из новых блоков могут встречаться как одинаковые транзакции, так и разные, вошедшие только в один из них. Когда ретрансляция блоков возобновляется, майнеры начинают считать главной цепочку с учётом уровня сложности хеша и длины цепочки. При равенстве сложности и длины предпочтение отдаётся той цепочке, конечный блок которой появился раньше. Транзакции, вошедшие только в отвергнутую ветку (в том числе по выплате вознаграждения), теряют статус подтверждённых. Если это транзакция по передаче биткойнов, то она будет поставлена в очередь и затем включена в очередной блок. Транзакции получения вознаграждения за создание отсечённых блоков не дублируются в другой ветке, то есть «лишние» биткойны, выплаченные за формирование отсечённых блоков, не получают дальнейших подтверждений и «утрачиваются».

Таким образом, цепочка блоков содержит историю владения, с которой можно ознакомиться, например, на специализированных сайтах.

Блокчейн формируется как непрерывно растущая цепочка блоков с записями обо всех транзакциях. Копии базы или её части одновременно хранятся на множестве компьютеров и синхронизируются согласно формальным правилам построения цепочки блоков. Информация в блоках не шифрована и доступна в открытом виде, но отсутствие изменений удостоверяется криптографически через хеш-цепочки (элемент цифровой подписи).

База публично хранит в незашифрованном виде информацию о всех транзакциях, подписываемых с помощью асимметричного шифрования. Для предотвращения многократной траты одной и той же суммы используются метки времени, реализованные путём разбиения БД на цепочку специальных блоков, каждый из которых, в числе прочего, содержит в себе хеш предыдущего блока и свой порядковый номер. Каждый новый блок осуществляет подтверждение транзакций, информацию о которых содержит и дополнительное подтверждение транзакций во всех предыдущих блоках цепочки. Изменять информацию в блоке, который находится в цепи, не практично, так как в таком случае пришлось бы редактировать информацию во всех последующих блоках. Благодаря этому успешная double-spending атака (повторная трата ранее израсходованных средств) на практике крайне маловероятна.

Для более наглядного объяснения механизма работы платёжной системы Сатоси Накамото ввёл понятие «цифровая монета», определив его как цепочку цифровых подписей. В отличие от стандартизированных номиналов обычных монет, каждая «цифровая монета» имеет свой собственный номинал. Каждому биткойн-адресу может сопоставляться любое количество «цифровых монет». При помощи транзакций их можно делить и объединять, при этом сохраняется общая сумма их номиналов за вычетом комиссии.[1]

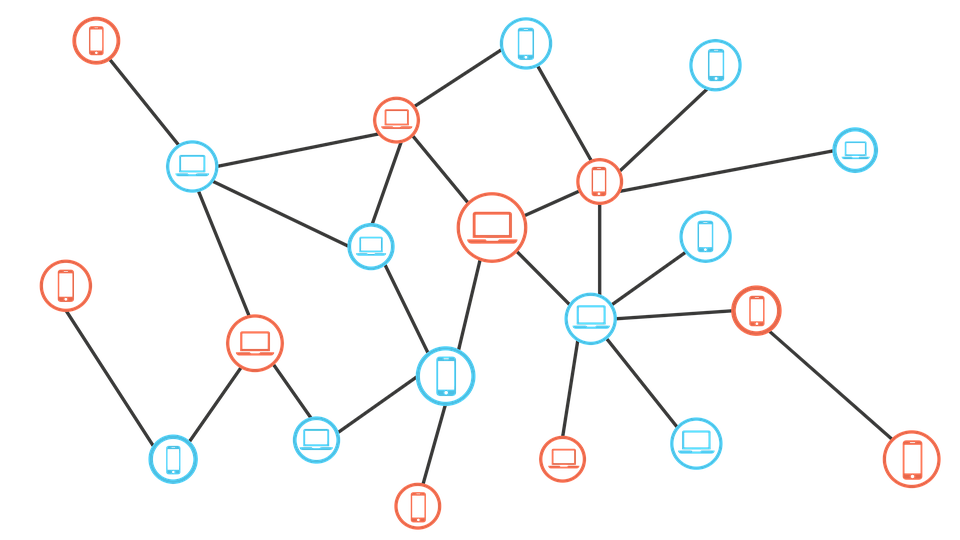


Рис.3. Цепочка блоков

2.3. Подтверждение транзакций

Пока транзакция не включена в блок, система считает, что количество биткойнов на некоем адресе остаётся неизменным. В это время есть техническая возможность оформить несколько разных транзакций по передаче с одного адреса одних и тех же биткойнов разным получателям[[16]](https://ru.wikipedia.org/wiki/%D0%91%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B9%D0%BD#cite_note-CNNMoney-16). Но как только одна из подобных транзакций будет включена в блок, остальные транзакции с этими же биткойнами система будет уже игнорировать. Например, если в блок будет включена более поздняя транзакция, то более ранняя будет считаться ошибочной. Есть небольшая вероятность, что при ветвлении две подобные транзакции попадут в блоки разных ветвей. Каждая из них будет считаться правильной, лишь при отмирании ветви одна из транзакций станет считаться ошибочной. При этом не будет иметь значения время совершения операции.

Таким образом, попадание транзакции в блок является подтверждением её достоверности вне зависимости от наличия других транзакций с теми же биткойнами. Каждый новый блок считается дополнительным «подтверждением» транзакций из предыдущих блоков. Если в цепочке 3 блока, то транзакции из последнего блока будут подтверждены 1 раз, а помещённые в первый блок будут иметь 3 подтверждения.(Рис. 4) Достаточно дождаться нескольких подтверждений, чтобы вероятность отмены транзакции стала очень низкой.

Для уменьшения влияния подобных ситуаций на сеть существуют ограничения на распоряжение только что полученными биткойнами.[1]

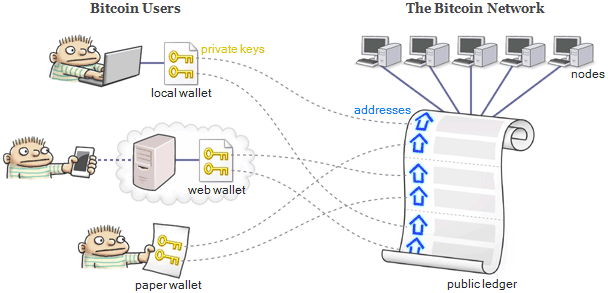


Рис.4.Транзакций

2.4. Двойное расходование

Если контролировать более 50 % суммарной вычислительной мощности сети, то существует теоретическая возможность при любом пороге подтверждений одни и те же биткойны передать два раза разным получателям — одна из транзакций будет публичной и подтверждаться в общем порядке, а вторая не будет афишироваться, её подтверждения будут происходить блоками скрытой параллельной ветви. Лишь через некоторое время сеть получит сведения о второй транзакции, она станет подтверждённой, а первая утратит подтверждения и будет игнорироваться. В результате не произойдёт удвоения биткойнов, но изменится их текущий владелец, при этом первый получатель утратит биткойны без каких-либо компенсаций.

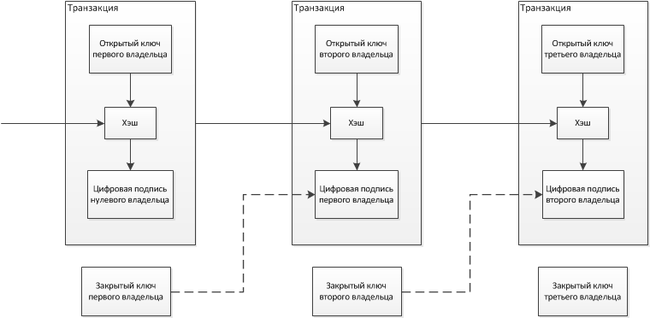
Открытость цепочки блоков позволяет внести в произвольный блок изменения. Но тогда потребуется пересчёт хеша не только изменённого блока, но и всех последующих. Фактически, для такой операции потребуется мощность не меньше той, которая была использована для создания изменённого и последующих блоков (то есть всей текущей мощности), что делает такую возможность крайне маловероятной.

Рис. 5

2.5. Сложность

А требование к хешам блоков отвечает специальный параметр, называемый «сложность». Так как вычислительные мощности сети непостоянны, этот параметр пересчитывается клиентами сети через каждые 2016 блоков таким образом, чтобы поддерживать среднюю скорость формирования блокчейна на уровне 2016 блоков в две недели. Таким образом, 1 блок должен создаваться примерно раз в десять минут. На практике, когда вычислительная мощность сети растёт — соответствующие временные промежутки короче, а когда снижается — длиннее. Перерасчёт сложности с привязкой ко времени возможен благодаря наличию в заголовках блоков времени их создания. Оно записывается в Unix-формате[4] по системным часам автора блока (если блок создается в пуле, то по системным часам сервера этого пула).

2.5.1. Unix-время

Unix-время (англ. Unix time, также POSIX-время) — система описания моментов во времени, принятая в Unix и других POSIX-совместимых операционных системах. Определяется как количество секунд, прошедших с полуночи (00:00:00 UTC) 1 января 1970 года (четверг); этот момент называют «эпохой Unix» (англ. Unix Epoch).[4]

3.Проблемы и возможные пути их решения

Являясь технологией построения массово-распределённых баз данных, блокчейн испытывает ряд специфических проблем, которые затрудняют его использование. Среди этих проблем можно назвать следующие:

* Постоянный рост размера файлов блокчейна.
* Ограничения пропускной способности каналов связи между узлами сети и сложности синхронизации отдельных реплик, связанные с этим ограничением.
* Общее ограничение производительности блокчейна, связанное со спецификой работы алгоритмов консенсуса.

Разработка новых видов блокчейна зачастую связана с преодолением или обходом этих проблем и ограничений. При этом есть ряд функций, без которых не может обойтись ни одна система блокчейна:

* Данные сохраняются в структуре из цепочки блоков, в которой каждый блок связан с предыдущим. Изменение информации в блоке невозможно без внесения изменений во все последующие блоки.
* У каждого участника сети есть копия всех данных (всей цепочки блоков). Участники взаимодействуют между собой в одноранговом формате (peer-to-peer).
* Установлен механизм консенсуса — определённое взаимодействие узлов, обеспечивающее достижение согласия о правильности информации, записываемой в очередной блок цепочки и выбора включаемого в цепочку блока из нескольких возможных альтернатив.[1]

3.1. Публичные блокчейны

Публичные блокчейны общедоступны. Любой может читать блоки, отправлять в них информацию и участвовать в механизме консенсуса. При этом пользователи могут оставаться анонимными. Такие блокчейны обычно полностью децентрализованы, то есть не имеют администраторов или центров доверия. Неизменность и целостность информации обеспечивают экономические стимулы и криптографические проверки с использованием таких механизмов, как доказательство выполнения работы или доказательство доли владения. Публичные блокчейны обычно имеют существенные ограничения в объёме и скорости размещения данных в блоках.[1]

3.2. Частные блокчейны

В частных блокчейнах правом записи информации обладает только один участник или узлы, уполномоченные этим единственным администратором. Это централизованные персонифицированные системы, поскольку существует иерархия полномочий. Сбои можно быстро исправить вручную. Нет смысла применять доказательство выполнения работы или доказательство доли владения — информация без задержки попадает в блоки, формируемые по мере необходимости, и не требует дополнительного подтверждения, что максимизирует скорость работы сети и минимизирует стоимость транзакций. Однако сохраняется распределённый характер хранения данных, при котором узлы содержат полные копии в формате взаимосвязанных цепочек блоков. Доступ к информации может быть общим или иметь произвольные ограничения. Чаще всего речь идёт о системе передачи информации внутри одной компании, что не требует общего доступа ко всей информации, но может предусматривать общедоступную возможность аудита.

Несмотря на внутреннюю персонализацию, ограничения доступа к информации могут обеспечить в частных блокчейнах более высокий уровень конфиденциальности.[1]

3.3. Консорциумные блокчейны

В консорциумных блокчейнах процесс согласования обеспечивается несколькими заранее оговоренными равноправными узлами. Например, консорциум из 15 банков договаривается считать действительным блок с мультиподписью не менее 10 участников консорциума. Скорость появления новых блоков может быть весьма высокой. При этом участники концерна доступ к информации из блокчейна могут сделать как общедоступным, так и ограничить избранным кругом или ввести иные количественные, содержательные или временны́е ограничения. Эти блокчейны можно считать «частично децентрализованными».

Ограниченное количество доверенных узлов позволяет модернизировать систему гораздо проще, чем при публичном блокчейне. Но работа такой сети возможна только при условии, что основная часть узлов работает добросовестно.[1]

4.Применение вне сферы криптовалют

4.1. Банковское дело

Блокчейн позволяет сделать все процессы в банковской индустрии безопаснее, надежнее и прозрачнее. Денежные переводы, расчеты при сделках с ценными бумагами, аккредитивы, KYC-комплаенс, рутинная работа бэк-офисов банков — все эти операции теперь проходят с внедрением этой технологии.[3]

Блокчейн может сократить затраты банков до 50%. Об этом заявляли еще в 2017 г. аналитики Morgan Stanley. По их мнению, блокчейн мог бы оптимизировать инфраструктуру, радикально сократить затраты и обеспечить необходимое повышение RoE (доходности собственного капитала) банков. Многим банкам, несмотря на присущую им консервативность, опасно было бы недооценивать потенциал этой технологии. Повсеместное ее внедрение может привести к ликвидации некоторых участников мировой финансовой системы.[3]

4.2. Кибербезопасность

Рис. 6

На каждом узле блокчейн-системы хранятся копии всей базы данных в целом, и они сверяются между собой. Это придает системе жизнеспособность даже в случае успешных хакерских атак на ее одиночные узлы. Несмотря на то, что приложения на блокчейне предлагают анонимность, технология может использоваться, чтобы прикреплять реальные идентификационные данные к криптографическим в базе данных.[3]

4.3. Удостоверения личности

Такие ID представляют собой перевод персональных данных о человеке на блокчейн, создание его цифрового профиля. Есть большой перечень госуслуг, доступ к которым может быть осуществлен посредством блокчейна, и есть статистика передовых блокчейн-стран (Эстония, некоторые эмираты ОАЭ). Использование блокчейна и блокчейн-ID активным гражданином может стать обычным паттерном поведения уже при жизни современного поколения.[3]



Рис. 7

Выводы

BlockChain это сложный механизм который с каждым годом становятся все лучше и лушче можно констатировать, что концепция блокчейна оказалась насыщенной точками появления новых решений, будь то вопросы защиты, расположения и доступа к блокчейну, его топологии и структуры, взаимодействия с другими блокчейнами, свойств блоков, типов транзакций и т.д. Уникальные свойства блокчейна способствовали тому, что поиском таких решений занялось огромное число специалистов всех стран. В результате идея блокчейна уже стала и, по всей видимости, еще долго будет оставаться мощнейшим источником инноваций в технической, экономической, финансовой, правовой и других областях общественной жизни людей во всем мире.

библиография

1. *Информация про Блокчейн.* [online]. [посещен 15.05.2022] Доступен в интернете по ссылке:

<https://ru.wikipedia.org/wiki/%D0%91%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B9%D0%BD>

1. *Что такое блокчейн.* [online]. [посещен 14.05.2022] Доступен в интернете по ссылке:

<https://www.forbes.ru/mneniya/456381-cto-takoe-blokcejn-vse-cto-nuzno-znat-o-tehnologii>

1. *Применение вне сферы криптовалют.* [online]. [посещен 14.05.2022] Доступен в интернете по ссылке:

<https://trends.rbc.ru/trends/industry/5f05c0a79a7947aac5c7577a#card_5f05c0a79a7947aac5c7577a_3>

1. *Unix-время*. [online]. [посещен 14.05.2022] Доступен в интернете по ссылке:

<https://ru.wikipedia.org/wiki/Unix-%D0%B2%D1%80%D0%B5%D0%BC%D1%8F>