**MINISTERUL EDUCAŢIEI AL REPUBLICII MOLDOVA UNIVERSITATEA DE STAT „ALECU RUSSO” DIN BĂLŢI FACULTATEA DE ŞTIINŢE REALE, ECONOMICE ȘI ALE MEDIULUI CATEDRA DE MATEMATICĂ ȘI INFORMATICĂ**

**ТЕХНОЛОГИЯ БЛОКЧЕЙН, и ее применение**

**РЕФЕРАТ ПО ДИСЦИПЛИНЕ „INFORMATICA GENERALĂ”**

**Автор:**

Студент группы IS11Z

**Гаврилицэ Дорин**

**Научный руководитель:** Олеся СКУТНИЦКИ магистр, асист. унив.

**BĂLȚI, 2022**

ОГЛАВЛЕНИЕ

[ВВЕДЕНИЕ 3](#_Toc104209568)

[1. Технология блокчейн 4](#_Toc104209569)

[1.1. История 4](#_Toc104209570)

[1.2. Общая информация 4](#_Toc104209571)

[1.3. Принцип работы блокчейн 5](#_Toc104209572)

[1.4. Блоки 6](#_Toc104209573)

[1.5. Умные контракты (smart contracts) 6](#_Toc104209574)

[1.6. Особенности задачи, решаемой технологией блокчей 7](#_Toc104209575)

[2. Механизмы достижения консенсуса 8](#_Toc104209576)

[3. Общий круг задач, решаемых блокчейн 10](#_Toc104209577)

[4. Границы применимости технологии blockchain 11](#_Toc104209578)

[1.. ВЫВОД 13](#_Toc104209579)

[БИБЛИОГРАФИЯ 14](#_Toc104209580)

# ВВЕДЕНИЕ

В наши дни всю большую популярность набирает разработка нового класса программного обеспечения, носящего название «децентрализованные приложения». Его основы были заложены технологиями Bitcoin и BitTorrent, успех которых вызвал интерес разработчиков к методам их реализации. Последние несколько лет весь мир был взбудоражен резко возросшей популярностью криптовалют, благодаря чему в центре внимания оказалась технология блокчейн. Как выяснилось при более тщательном анализе, сфера её применения не ограничивается только лишь созданием электронных денежных средств и платформ для обмена ими. Одним из перспективных направлений внедрения технологии блокчейн является ее использование в банковском секторе для повышения уровня безопасности операций и сокращения издержек.

В дословном переводе блокчейн — это непрерывная цепочка блоков. В ней содержатся все записи о сделках — хоть с луковицами тюльпанов в ботаническом саду. В отличие от обычных баз данных, изменить или удалить эти записи нельзя, можно только добавить новые. Блокчейн еще называют технологией распределенных реестров, потому что всю цепочку сделок и актуальный список владельцев хранят на своих компьютерах множество независимых пользователей. Даже если один или несколько компьютеров дадут сбой, информация не пропадет.

## Технология блокчейн

### История

Впервые технология блокчейн (англ. blockchain) была описана группой исследователей в 1991 году [1]. Однако в то время основная масса пользователей не обладала скоростным доступом в Интернет и накопителями достаточной емкости, позволяющими реализовать идеи, заложенные в блокчейн.

Практическую реализацию технология блокчейн получила только в 2008 году, когда неизвестный пользователь под псевдонимом Сатоши Накамото (англ. Satoshi Nakamoto) опубликовал техническое описание своего протокола криптовалюты и создал первую версию программного обеспечения, в котором этот протокол был реализован [2]. 3 января 2009 года в новой сети, получившей название Биткойн (англ. Bitcoin), были сгенерированы первые блоки. Данная сеть позволяла пользователям осуществлять переводы биткойнов друг другу без участия стороннего посредника, при этом само слово «биткойн» стало употребляться не только как название самой системы, но и как название денежной единицы. На сегодняшний день именно криптовалюты являются наиболее известным, значимым и распространенным примером использования блокчейн-технологии [3, 4].

### Общая информация

Блокчейн – это распределенная децентрализованная защищенная шифром база данных, в которой каждая совершенная транзакция записывается и становится известна всем участникам сети. Данные о совершенных транзакциях сохраняются в определенном порядке и формируют неизменную последовательность связанных блоков. После этого информация, содержащаяся в блоке, тиражируется и копируется на каждый узел, находящийся в сети. Этот алгоритм обеспечивает устойчивость данной технологии к изменению данных.

Блокчейн обычно управляется при помощи одноранговой (peer-to-peer) сети. После записи, данные в любом блоке не могут быть изменены без полного изменения всех последующих блоков, что требует согласия большинства участников сети.

М. Свон в своей книге «Блокчейн: Схема новой экономики» [5] выделает три вида блокчейн:

а) Блокчейн 1.0 – это криптовалюта. Примерами могут служить Bitcoin, Ethereum, Litecoin и т.д.

б) Блокчейн 2.0 – это умные контракты (smart contracts). Это широкий класс финансовых приложений, реализующих работу с акциями, облигациями, фьючерсами, закладными и многими другими финансовыми активами. Именно этот вид Блокчейн будет рассмотрен в нашей работе.

в) Блокчейн 3.0 – все остальные приложения, основанные на данной технологии и выходящие за рамки финансовой сферы.

### Принцип работы блокчейн

Несмотря на то, что Блокчейн – распределенная система, и каждый участник может проводить транзакцию, не все они равноправны. Участники системы делятся на операторов (майнер/валидатор), проводящих транзакцию, регуляторов сети, отвечающих за регистрацию, и обыкновенных пользователей.

Выделяют несколько основных этапов формирования блоков.

а) Первый шаг – определение транзакции. Отправитель создает транзакцию, в которой содержится информация об адресе получателя, предмете транзакции (сумма средств, товар и т.д.) и криптографическая цифровая подпись, подтверждающая достоверность транзакции и ее правомерность. Узлы сети оповещаются о транзакции и проверяют её достоверность путем дешифрования электронной подписи. Если транзакция проходит проверку, то она встает в режим ожидания на включение в блок.

б) Создание блока. Блоки, содержащие информацию о транзакциях, связываются криптографически и хронологически в «цепочку» с помощью сложных математических алгоритмов. Новые блоки всегда добавляются строго в конец цепочки. Один из узлов сети один раз за определенный интервал времени собирает находящиеся в режиме ожидания транзакции, формирует из них блок и отправляет на подтверждение другим участникам сети на предмет проверки и присоединения к цепочке.

в) Валидация блока. Узлы, ответственные за валидацию блоков, получают просьбу проверить созданный блок. Они запускают повторяющийся процесс, который требует одобрения от других узлов-операторов для того, чтобы признать блок действительным. Процесс шифрования, известный как хеширование, выполняется большим количеством разных компьютеров, работающих в одной сети. Если в результате их расчетов все они получают одинаковый результат, то блоку присваивается уникальная цифровая сигнатура (подпись).

г) Присоединения блока к цепочке. Когда все транзакции в блоке одобряются, новый блок становится присоединенным к общей цепочке. Как только реестр будет обновлён и образован новый блок, он уже больше не может быть изменён. Таким образом подделать его невозможно. К нему можно только добавлять новые записи. Важно учесть то, что реестр обновляется на всех компьютерах в сети одновременно.

### Блоки

Внутренняя структура блока такова: блок включает в себя список транзакций и заголовок (header), который содержит собственный хеш, хеш предыдущего блока, хеш транзакций и дополнительную информацию. Связь между блоками за счет наличия в каждом (за исключением первого) хеша предыдущего означает, что невозможно внести изменения в блок, не изменив всю цепочку с первого блока – нельзя удалить какую-то транзакцию или вставить ее между уже совершенных.

Эти блоки образуют линейную последовательность во времени, и именно отсюда происходит слово «блокчейн». Блоки добавляются в цепочку равномерно – для Эфириума каждые 17 секунд, для Bitcoin – каждые 10 минут.

### Умные контракты (smart contracts)

Когда речь касается финансовых вопросов, современному человеку достаточно тяжело обойтись без посредников в их решении, будь то покупка дома, страхование имущества или приобретение ценной бумаги. Значительно упростить и удешевить эту процедуру могут помочь умные контракты.

Умный контракт – это программный алгоритм, способный выполнять функции бумажного документа. Когда происходит некоторое событие, умный контракт выполняет предопределённые пункты договора, прописанные в нём. Важной особенностью умных контрактов является то, что они находятся не на сервере, а непосредственно в цепочке блоков, а следовательно, имеют надёжную криптографическую защиту.

Умные контракты стали второй ступенью в развитии технологий блокчейн. После успеха Bitcoin появилось множество альтернативных криптовалют, которые в общих чертах копировали его код, но при этом вносили ряд дополнительных возможностей, привлекающих пользователей. Одной из таких функций как раз стали умные контракты. Ярким примером криптовалютного проекта, реализующего эту особенность, может служить Ethereum, созданный нашим соотечественником Виталием Бутериным. На сайте Ethereum подчёркивается, что платформа может быть использована для «кодификации, децентрализации, обеспечения безопасности и торговли практически всем: доменными именами, финансовыми активами, краудфандинга, управления компаниями и интеллектуальной собственностью». У Ethereum есть ряд конкурентов, таких как NEM, Hyperledger Fabric, но «золотым стандартом» в мире смарт-контрактов на сегодняшний день является он.

У умных контрактов есть ряд преимуществ и недостатков.

К плюсам данного изобретения можно отнести надёжность, неизменность, ускорение обмена активами, сокращение издержек за счёт отсутствия третьих лиц при совершении сделок, удобство.

Однако умные контракты имеют определённые риски. Первый из них – возможность ошибки программиста, которая приведёт к неверному выполнению условий договора. Помимо этого, умные контракты запускаются при наступлении определённых событий, и их действие нельзя отменить в случае непредвиденных ситуаций, следовательно, они не обладают достаточной гибкостью. Другим недостатком смарт-контрактов является непонимание их принципов работы широкими массами, что существенно ограничивает круг применимости.

### Особенности задачи, решаемой технологией блокчей

Основная задача, для решения которой применима технология блокчейн – согласование действий участников системы, объединенных одной целью, но лишенных доверия друг к другу.

Среди криптологов уже давно стала классической «задача византийских генералов», которая имеет следующую формулировку: «Византийская армия осаждает город. Генералам необходимо выработать единую стратегию действий, которая приведет к победе, даже если среди них будут предатели, намеренно искажающие информацию о численности своих отрядов и времени наступления». Блокчейн решает эту задачу при помощи механизмов достижения консенсуса.

Данная технология имеет огромный потенциал для тех систем, между участниками которых отсутствует взаимное доверие, т.к. она обеспечивает надёжное хранение персональных данных, делая недоступными изменения в них в целях мошенничества. Более того, блокчейн позволяет совершать различного рода сделки без посредников, что существенно экономит средства и время. Всё это как раз актуально для банковских систем.

## Механизмы достижения консенсуса

Самое ценное звено в технологии блокчейн – это алгоритмы достижения консенсуса, ведь именно они обеспечивают ей надёжность.

Существуют три основных механизма достижения согласования.

а) Доказательство работы (proof of work) – протокол защиты системы. Любой, желающий записать блок в базу данных, должен выполнить определенную сложно вычислимую задачу, построенную на принципе односторонней функции. Процесс вычисления занимает длительный срок, в то время как принимающая сторона быстро проверяет полученный результат. Перед отправкой сообщения к заголовку добавлялась некоторая отметка,

подтвердить валидность которой можно только полным перебором. Проверка вычислений на принимающей стороне происходит быстро - за счет однократного вычисления SHA-1 с заранее подготовленной меткой.

На данный момент именно алгоритм доказательства работы заслужил наибольший авторитет среди прочих механизмов создания надёжных систем. Всё дело в том, что именно он способен противостоять «атакам Сивиллы», суть которых заключается в том, что злоумышленник создает множество поддельных участников и таким образом склоняет консенсус в свою сторону. Проведение подобной атаки затрудняет алгоритм доказательства выполнения работы, так как для её выполнения мошеннику придётся затратить колоссальную вычислительную мощность. Также большинство Блокчейнов взимают комиссию за участие в консенсусе, следовательно, «атака Сивиллы» станет очень дорогостоящей операцией. Нередко алгоритм proof-of-work подвергается критике из-за чрезмерной энергозатратности, но пока это единственное средство противостояния вмешательствам в систему подобного рода.

б) Proof-of-stake (доказательство доли) – протокол защиты, альтернативный proof-of-work, в котором необходимо в качестве доказательства подтвердить хранение определенной суммы на счете. С более высокой вероятностью при формировании следующего блока система выберет майнера с большим количеством средств на счете, при этом вероятность этого выбора не зависит от мощности его процессоров. Для того, чтобы подорвать надежность системы один из участников должен собрать в своих руках более 50% всех средств системы, что очень затратно.

Proof-of-stake имеет больше преимуществ по сравнению с proof-of-work. Главное – более низкие временные затраты (нет необходимости в длительных вычислениях), однако это не избавляет от возможных проблем. Также нет доказательств эффективности в защите от рисков, возникающий в криптовалютах.

Два существенных плюса этого протокола - атака на систему стоит очень дорого, и если какой-то участник ее все же проведет, то сам существенно от этого пострадает, поскольку нарушит устойчивость системы. Аргументы против – метод дает мотивацию накапливать средства на отдельных счетах, что ставит под вопрос децентрализацию; в случае образование небольшого числа участников, сосредоточивших в своих руках большинство средств, эта группа может навязать свои условия функционирования системы.

в) Delegated-proof-of-stake – усовершенствованная версия протокола защиты proof-of-stake, специфика которой заключается в том, что блоки порождаются предопределенным множеством пользователей системы (101 делегат), которые получают вознаграждение за свою обязанность и наказываются за злонамеренное поведение (такое как участие в двойном расходовании средств). Список пользователей, подходящих для подписания блоков, периодически изменяется в соответствии с определенными правилами; например, в Slasher делегаты избираются исходя из их доли и истории блокчейна. Делегаты могут получать голоса от всех пользователей, сила голоса зависит от доли валюты у голосующего. Delegated-proof-of-stake имеет те же достоинства и недостатки, что и proof-of-stake.

## Общий круг задач, решаемых блокчейн

Снижение издержек, повышение уровня безопасности и более высокая прозрачность транзакций – три сильных стороны блокчейн. Потребность банков и бизнеса в этих аспектах делает блокчейн привлекательным для специалистов, работающих над разработкой программного обеспечения в данных отраслях.

Сегодня привычным для нас стало осуществление платежей через Сеть. Но в этом процессе часто принимают участие неэффективные, устаревшие системы вроде Automated Clearing House (ACH), в которых все операции выполняются централизованно, что негативно сказывается на скорости работы. Но компьютеры постоянно взаимодействуют и не должны сутками ждать, пока пройдёт платёж, поэтому следующий уровень эволюции электронных денег как раз и открывает для нас блокчейн. Огромным плюсом этой технологии является тот факт, что блокчейн не зависит от централизованной компьютерной архитектуры, что приводит к тому, что выпадение отдельных узлов на нарушит работу всей системы.

Среди современных специалистов, анализирующих возможности применения Блокчейн в банковском секторе, бытует мнение о том, что эта технология способна полностью трансформировать структуру банков, и в скором времени она станет кардинально отличаться от того, с чем мы привыкли иметь дело сегодня. Возможность избежать посредничества третьих лиц в различного рода сделках способна сделать бесполезным огромный пласт банковских услуг. Однако реализация этой задумки далеко не беспрепятственна и имеет огромное количество тонкостей.

## Границы применимости технологии blockchain

Блокчейн, безусловно, привлекательная и очень перспективная технология, но подойдёт не для каждой системы. Существует ряд предпосылок, которые указывают на возможность внедрения блокчейн:

а) использование базы данных с общим доступом;

б) между участниками отсутствует доверие;

в) необходимость в отсутствии посредников;

г) взаимозависимость операций, потребность в создании цепочек.

Однако стоит учитывать, что даже для тех систем, где применима технология блокчейн, её внедрение имеет ряд препятствий, вызываемых самой структурой и принципами технологии. Рассмотрим некоторые из них.

а) Вопросы безопасности и privacy. Несмотря на существование решений в области безопасности с использованием сложных алгоритмов шифрования, проблемы кибербезопасности остаются одними из самых обсуждаемых. Любое программное обеспечение написано человеком, а поэтому несовершенно. Чем больше оно усложняется, тем стремительнее растёт количество уязвимостей. Вдобавок, целостность программного обеспечения и сети фундаментально важны для превращения блокчейна в инфраструктурную технологию. Если блокчейн переплетется со всеми главными финансовыми системами мира, то мощные атаки на него могут привести к катастрофическим последствиям.

б) Вопросы внедрения и интеграции. Когда организация внедряет технологию для модернизации своих бизнес-процессов, она сталкивается с проблемой переноса своих старых данных в новый формат. В данной ситуации внедрение блокчейна ничем не проще других подобных задач, а значит вопрос планирования перехода от текущих систем к блокчейну остается открытым. Сокращение издержек, которые обещает внедрение блокчейна, воодушевляет, однако внедрение потребует высоких первоначальных затрат, которые нельзя не принимать во внимание.

в) Понимание технологии. Один из наибольших операционных рисков заключается в том, что относительно небольшое число людей понимает, как он работает. Если планируется внедрять блокчейн в систему, пользователями которой являются широкие слои населения, то это может привести к неприятным последствиям. Всё дело в том, что блокчейн не защищает от самого популярного вида мошенничества – фишинга, суть которого заключается в краже конфиденциальных данных пользователей. Компрометация ключа может привести к постоянной потере средств, защищенных криптографией. К сожалению, на сегодняшний день далеко не каждый простой пользователь может похвастаться знанием элементарных правил защиты личных данных. Существует возможное решение проблемы кражи личной информации: связать открытые ключи с физической личностью или юридическим лицом, но данный механизм потребует дополнительных затрат.

г) Вопрос скорости выполнения операций. В целях защиты от атаки 51% (когда один участник сети завладевает более чем половиной вычислительной мощности системы) размер блока (на примере Биткоин) остается не более 1 мегабайта, что позволяет поддерживать децентрализацию, но значительно ограничивает скорость транзакций – 3,3 в секунду, в то время как та же Visa проводит 22 тысячи в секунду. Расширение пропускной способности хотя бы до 10 транзакций в секунду потребовало бы увеличение размера блока до 1,6 гигабайт, что, во-первых, вызвало бы проблемы у маломощных майнеров, а, во-вторых, затруднило бы распространение блоков по узлам. Уже сегодня цепочка блоков Bitcoin весит около 38 Гбайт памяти. Если впоследствии появятся Блокчейн системы, которые будут хранить не только информацию о транзакциях, но и другие, более объёмные данные, то их с высокой вероятностью ждёт неудача, так как вынуждая майнеров хранить чужие данные бесплатно, разработчик лишает их стимула поддерживать работу сети, поскольку затраты майнеров станут превышать доходы.

### ВЫВОД

Технология блокчейн открывает нам огромный спектр возможностей, начиная с денежных переводов и платежей и заканчивая смарт-контрактами и сверкой документов. Её сильные стороны, такие как снижение издержек, повышение уровня безопасности и прозрачность транзакций, привлекли к себе внимание банковского сектора. Но далеко не все операции, которые до появления технологии распределённой базы данных осуществлялись при помощи посредников и третьих лиц, можно упростить с помощью блокчейн. У технологии имеется ряд тонкостей, связанных и с недостаточной изученностью, и с пониманием технической реализации, и с гибкостью.

На сегодняшний день, по мнению международных аналитиков, технология блокчейн является финансовым инструментом.Уже зарегистрированы случаи крупных международных транзакций, где данная технология позволила значительно сократить срок проведения сделок (до нескольких часов). В обычном случае на проведение одной из подобных международных транзакций ушло бы не меньше недели.

Подобно уменьшению сроков проведения крупных денежных транзакций, технология блокчейн содержит в себе потенциал для сокращения времени на обработку документов. Административные расходы любой компании на создание, проверку, обработку и перемещение документации очень высоки. Кроме того, традиционные методы доставки бумажных документов являются уязвимыми для задержек и мошенничества. Технология блокчейн, примененная в качестве цифрового распределенного реестра, могла бы значительно сократить затраты и сроки на документооборот.

Все это говорит о том, что блокчейн имеет большие перспективы внедрения в работу крупных корпораций различных секторов экономики, в том числе на транспорте.

Приживется ли эта технология надолго и будет ли она процветать? Сложный вопрос. Блокчейн до сих пор не изучен до конца, имеет много «острых сторон» относительно легальности в мировой экономике. Из-за новизны данного продукта возможны непредвиденные ситуации, касающиеся технической стороны, и, в конечном счете, она может оказаться недостаточно сильным конкурентом существующим технологиям.

# БИБЛИОГРАФИЯ

1. Haber S., Stornetta W.S. How to time-stamp a digital document // Journal of Cryptology. – January 1991, Volume 3, Issue 2, P. 99-111.
2. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System [Электронный ресурс] // 2008. – Режим доступа: https://bitcoin.org/bitcoin.pdf (дата обращения 06.05.2022).
3. Винья П., Кейси М. Эпоха криптовалют. Как биткоин и блокчейн меняют мировой экономический порядок. – М.: Издательство «Манн, Иванов и Фербер», 2017. – 432 с.
4. Дрешер Д. Основы блокчейна: вводный курс для начинающих в 25 небольших главах. – М.: ДМК Пресс, 2018. – 312 с.
5. Мелани Свон. Блокчейн. Схема новой экономики, Олимп- Бизнес, 2017, 240с.
6. Равал С. Децентрализованные приложения. Технология Blockchain в действии, Питер, 2017, 192с