

МИНОБРНАУКИ РОССИИ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ  
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ  
«Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»  
им. В.И. Ульянова (Ленина)»

Эссе

по дисциплине: "Экономика"

Тема: Принцип функционирования электронных денег и криптовалют

Студент гр. 1323 \_\_\_\_\_ В.В. Скопцов

Преподаватель \_\_\_\_\_ Т.Н. Лебедева

Санкт-Петербург 2022

# Содержание

<b>1</b>	<b>Введение</b>	<b>3</b>
<b>2</b>	<b>Определение электронных денег</b>	<b>3</b>
<b>3</b>	<b>Типы электронных денег</b>	<b>4</b>
<b>4</b>	<b>Теория, обеспечивающая работу электронных денег</b>	<b>5</b>
4.1	Метод слепой цифровой подписи . . . . .	5
4.2	Протокол RSA . . . . .	5
<b>5</b>	<b>Особенности криптовалют</b>	<b>5</b>
5.1	Недостатки криптовалют . . . . .	5
<b>6</b>	<b>Заключение</b>	<b>7</b>

A specter is haunting the modern world,  
the specter of crypto anarchy.

---

*The Crypto Anarchist Manifesto (1988)*  
Timothy C. May

## 1 Введение

Появление интернета помогло распространению электронных денег в качестве очень практичного и удобного средства оплаты. Быстрота транзакций, защищённость посредством разных криптографических средств и другие достоинства дают огромные преимущества по сравнению с обычными деньгами. Но, в тоже время, на полечи посреднических организаций, которые непосредственно регулируют транзакции, ложится огромная ответственность, которая с дальнейшим развитием и увеличением объёмов цифровых денежных переводов будет только возрастать. Так, например, в распоряжении частных лиц будет находиться всё больше информации о клиентах, что может ставить под угрозу их личную безопасность в случае утечки этих данных. Одним из решений этой проблемы стали криптовалюты, появившиеся относительно совсем недавно. При использовании криптовалют отпадает не только необходимость в стороне осуществляющей транзакцию, но и в государственных эмитентах, из-за чего сама идея децентрализованных платёжных систем подвергается большой критики, в особенности от сторонников государственного контроля за финансами. Но даже если игнорировать политическую сторону вопроса, то остаётся техническая и экономическая, где ещё больше людей найдут недочёты.

## 2 Определение электронных денег

Перед тем, как рассмотреть принципы функционирования электронных денег необходимо дать чёткое определение этому достаточно расплывчатому понятию. Для этого можно обратиться к законодательству Российской Федерации.

Федеральный закон «О национальной платёжной системе» от 27.06.2011 N 161-ФЗ содержит следующее определение электронных денег:

это денежные средства, которые предварительно предоставлены одним лицом (лицом, предоставившим денежные средства) другому лицу, учитывающему информацию о размере предоставленных денежных средств без открытия банковского счёта (обязанному лицу), для исполнения денежных обязательств лица, предоставившего денежные средства, перед третьими лицами и в отношении которых лицо, предоставившее денежные средства, имеет право передавать распоряжения исключительно с использованием электронных средств платежа.

В свою очередь, электронное средство платежа:

это средство и (или) способ, позволяющие клиенту оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платёжных карт, а также иных технических устройств.

### 3 Типы электронных денег

В первую очередь, электронные деньги делятся по принципу физической реализации, а именно, они могут быть либо основаны на *базе смарт-карт*, либо на *базе сетей*.

Смарт-карты в большинстве случаев представляют из себя пластиковые карты со встроенной микросхемой и операционной системой. Обычные дебетовые или кредитные карты, являются всего лишь средством доступа к счёту, и не могут быть носителями средств, в то время как, смарт-карты непосредственно хранят записи о сумме, которая заложена в них, а так же могут осуществлять криптографические вычисления. Самой известной подобной картой является Visa Cash, разработанная в 1995 году.

Работоспособность электронных денег на базе сетей обеспечивается за счёт некоторой программы, или распределённой сети. Самые известные в России сервисы, работающие по такому принципу являются Яндекс.Деньги и QIWI.

Далее, электронные деньги делятся по принципу государственного регулирования, а именно, на *фиатные* и *нефиатные*.

Фиатные электронные деньги — это деньги, выраженные в государственной валюте, эмиссия которых происходит по правилам центрального банка. В качестве примера отлично подходит Яндекс.Деньги.

Нефиатные, в свою очередь, эмитируются частными организациями, и не являются горонтированным средством платежа, в отличии от фиатных денег. Самый яркий пример — платёжный сервис QIWI.

Данное разделение не зависит от технической реализации денег, поэтому деньги могут быть как фиатными, так и нефиатными, вне зависимости от того, какая у них база: сетевая или на основе смарт-карт.

Так же существует разделение на *персонифицированные* и *неперсонифицированные* электронные платёжные средства, которые подразумевают необходимость идентификации и возможность анонимности соответственно.



Рис. 1: Разделение типов электронных денег.

## 4 Теория, обеспечивающая работу электронных денег

### 4.1 Метод слепой цифровой подписи

В 1982 году вышла работа американского исследователя Дэвида Чаума, где были представлены криптографические методы, которые в последствии легли в основу всех видов электронных платежных систем. Одной из самых важных идей, которые изложил Чаум, была идея слепой цифровой подписи, обеспечивающее следующие возможности, которых не было в стандартных деньгах:

- Возможность фиксации факта осуществления транзакции.
- Невозможность установления личности получателя третьей стороной.
- Возможность становки транзакции.

### 4.2 Протокол RSA

Надёжность транзакций обеспечивается протоколом RSA, который совместно разработали в 1977 году специалисты по информатике Рональд Ривест, Ади Шамир и Леонард Макс Адельман. Устойчивость за счёт фундаментальных криптографических методов позволяет обеспечить анонимность передачи сообщений, из-за чего система RSA стала использоваться во многих сферах в жизни, но особенно важную роль она играет в банковской сфере работая в совокупности с идеей слепой цифровой печати.

## 5 Особенности криптовалют

Обычные электронные деньги, реализованные на принципах не предполагающих децентрализованное регулирование могут быть уязвимыми за счёт существования третьей доверительной стороны, которая не смотря на использование метода цифровой слепой печати, всё равно полагается на финансовые учреждения. Для решения этой проблемы были созданы определённые методы, в частности, принцип **доказательство выполнения работы** (англ. proof-of-work), обеспечивающие автономную работу регулирования электронной валюты. Впервые данные методы были использованы в первой криптовалюте Bitcoin, выпущенной в 2009 году в виде открытого программного обеспечения.

Криптовалюта представляет из себя распределённую базу данных, в которой хранятся общедоступные данные об совершенных транзакциях за весь период её функционирования. За счёт криптографического принципа доказательства выполнения работы система предотвращает слишком частые внесения изменений в базу данных, что предотвращает возможность взлома. Эмиссия происходит во время подтверждений транзакций, обладающих особыми качествами. Со временем, из-за притока новых пользователей сложность проверки историй транзакций в базе данных возрастает и эмиссия становится более дорогой.

### 5.1 Недостатки криптовалют

Криптовалюты предоставляют возможность анонимных транзакций, что усложняет возможность государственного регулирования денежных потоков. В частности, анонимность криптовалют позволяет избегать уплаты налогов, осуществлять оборот нелегальных товаров.

В рыночной среде часто поднимается вопрос об факте завышения текущих цен криптовалют в сравнении с их гипотетической стоимостью, что основывается на отсутствии внутренней ценности. В частности, лауреат Нобелевской премии по экономике Джеймс Хекман сравнил ожиотаж вокруг биткойна с тюльпаноманией в Голландии в 17 веке. Рынок криптовалют действительно напоминает спекулятивный пузырь, к примеру, цена криптовалют может стремительно возрасти за короткий промежуток времени, а потом падать на несколько десятков процентов.

В особенности криптовалюты критикуют за их очень нестабильный курс, характерный практически для всех криптовалют, курс которых не привязан к какой-либо национальной валюте. Исследователь Марк Т. Уильямс в своей статье в 2014 году заявил, что волатильность биткойна в семь раз выше чем у золота, и в 18 раз выше чем у доллара США. Это, в частности, хорошо иллюстрирует крах рынка криптовалют в 2022 году, когда на фоне предупреждений об инфляции биткойн, Ethereum, потеряли 20% и 26% своей стоимости, а фондовый индекс FTSE 100 упал на 3.6%.

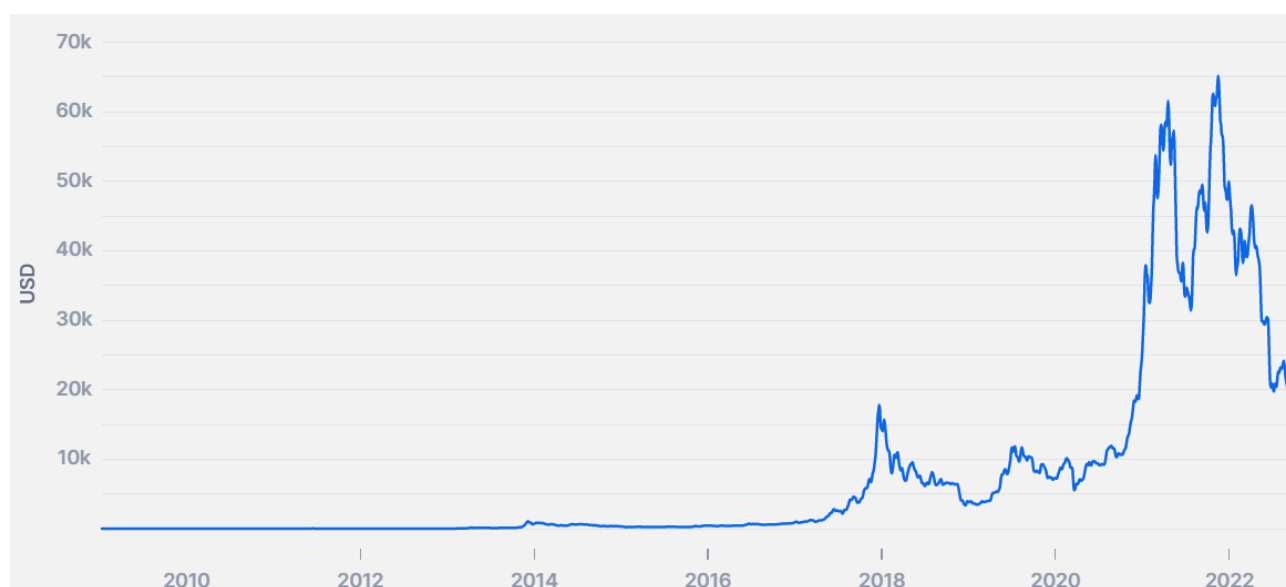


Рис. 2:

Также у всех криптовалют присуща медлительность транзакций из-за сложные криптографические вычисления, обеспечивающих их работу. Так, биткойн осуществляет 7 транзакций в секунду, в то время как максимальная производительность платежной системы Visa составляет около 54 тысячи транзакций в секунду. В среднем транзакция в том же биткойне длится порядка 20-30 минут. Этот факт делает криптовалюты крайне неудобными для оплаты физических товаров.

Ещё одной проблемой является неразумное использование электроэнергии при эмитировании криптовалют, в особенности тех, в основе которых лежит принцип доказательства выполнения работы. Согласно результатам исследования Кембриджского центра по организации дополнительного финансирования, на биткойн уходит порядка 100 ТВтч в год, что соответствует величине, которую потребляет Египет.

## 6 Заключение

Электронные деньги в целом занимают в нашей жизни уверенную позицию. Однако, например, криптовалюты часто становятся в центре споров и скандалов, что делает их крайне противоречивым средством расчёта