

# Криптовалюты: революция в электронных платежах



**Павел Кравченко**

# О себе



- 8 лет в IT
- PhD по специальности “Системы защиты информации”
- Делаю курс лекций для университетов, создаю исследовательскую лабораторию

# План

Что такое Bitcoin?

Чем отличается Bitcoin от WebMoney и других?

Почему Bitcoin приобрел популярность?

Как формируется ценность Bitcoin?

Как осуществляется эмиссия?

На каких принципах построен Bitcoin?

Какие недостатки биткойна?

Как это работает?

# Что такое Bitcoin?



Редкость

Делимость

Сложность добычи

Невозможность  
скопировать

Не контролируется

# В чем отличие Bitcoin?

Валюта а не платежная система

Не может быть напечатан кем-либо

Не может быть уничтожен атакой на сервер

Не поддаются регуляции

Не привязан к национальным валютам

*Это электронная наличность, а не  
обязательства эмитента*

# Почему приобрел популярность?

Не подвержен инфляции

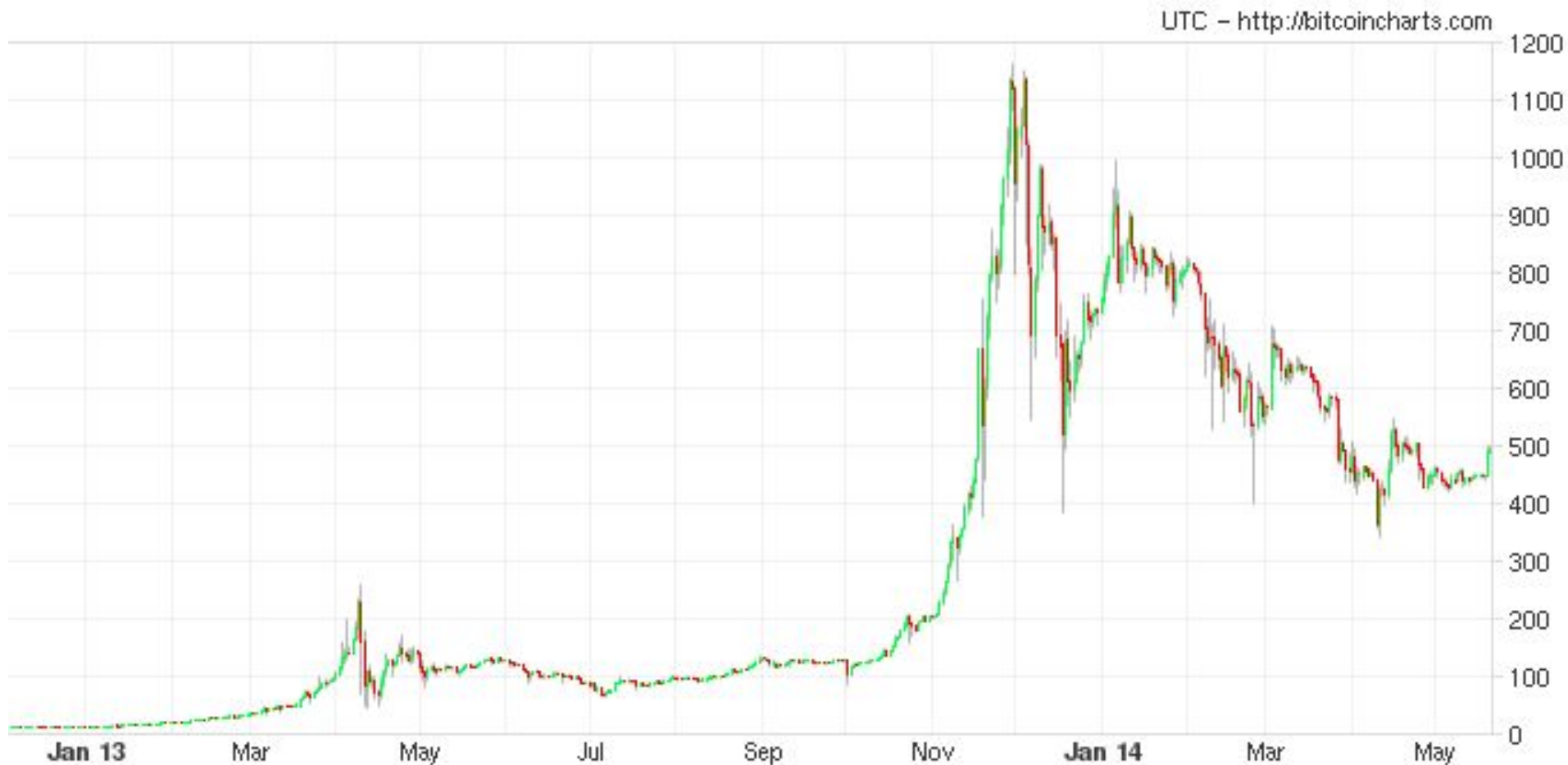
Децентрализованная  
система

Биткоин относительно  
анонимен

Вы можете платить кому  
угодно, где угодно и за  
что угодно



# Как формируется цена Bitcoin?



# Цифры

> 1000000 пользователей

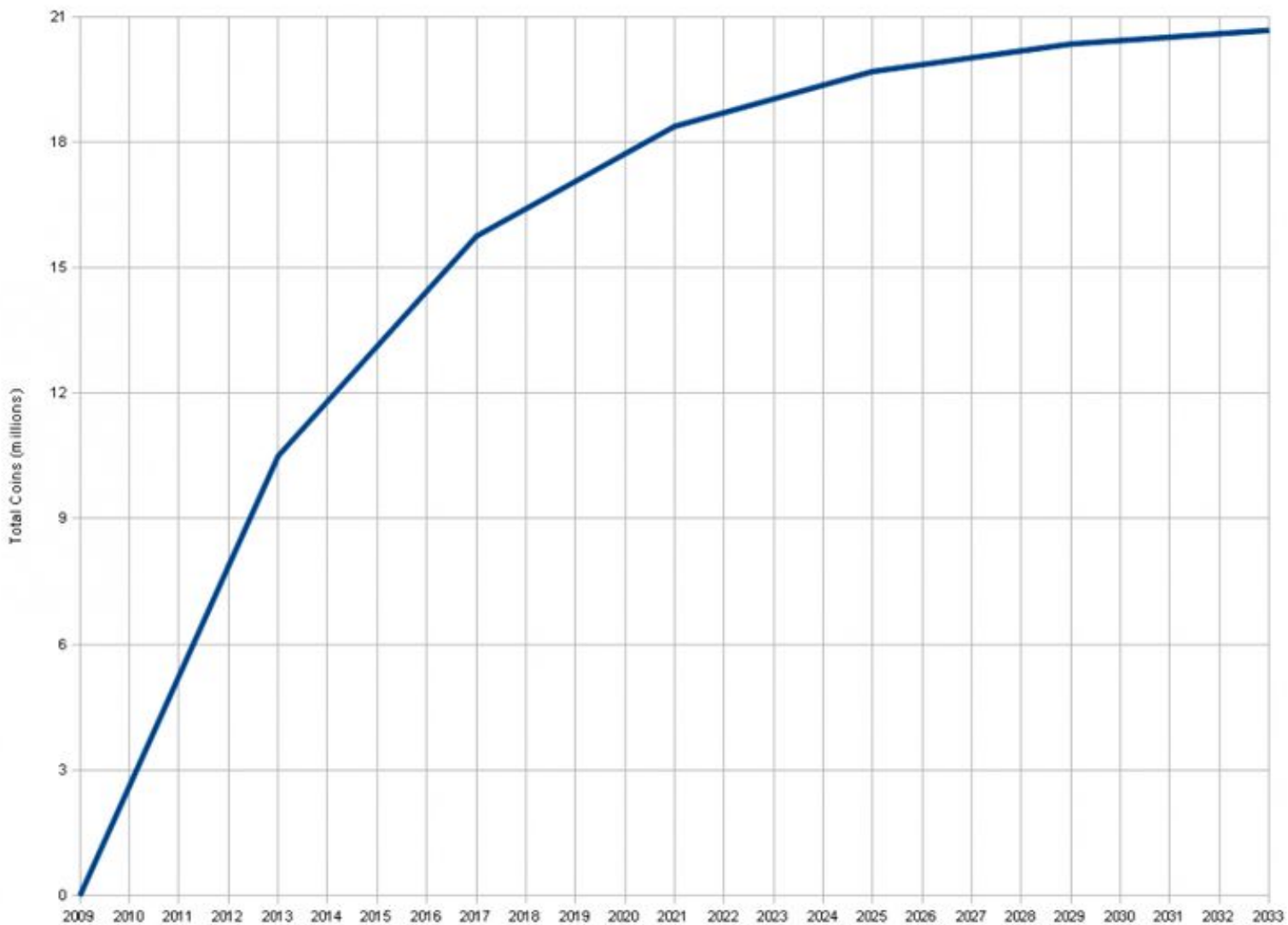
~100000 бизнесов

10-100 миллионов \$ дневной оборот

> 5 миллиардов стоимость всех биткоинов



# Как осуществляется эмиссия?



# Принципы в основе

Хранение информации обо всех транзакциях у каждого участника системы

Последовательность транзакций неизменна

Верификацию транзакций делает каждый, конкурируя за право быть первым, чтобы получить вознаграждение

Только владелец ключа может потратить деньги


Консенсус - простое большинство участников системы принимают решения

# Как работает Bitcoin? Шаг 1

Расписка.

Я, Свибунцов Александр Григорьевич, для нужд  
избирательной кампании 2006 г. получил от Киселева В.А.  
300.000 (Триста тысяч) долларов США

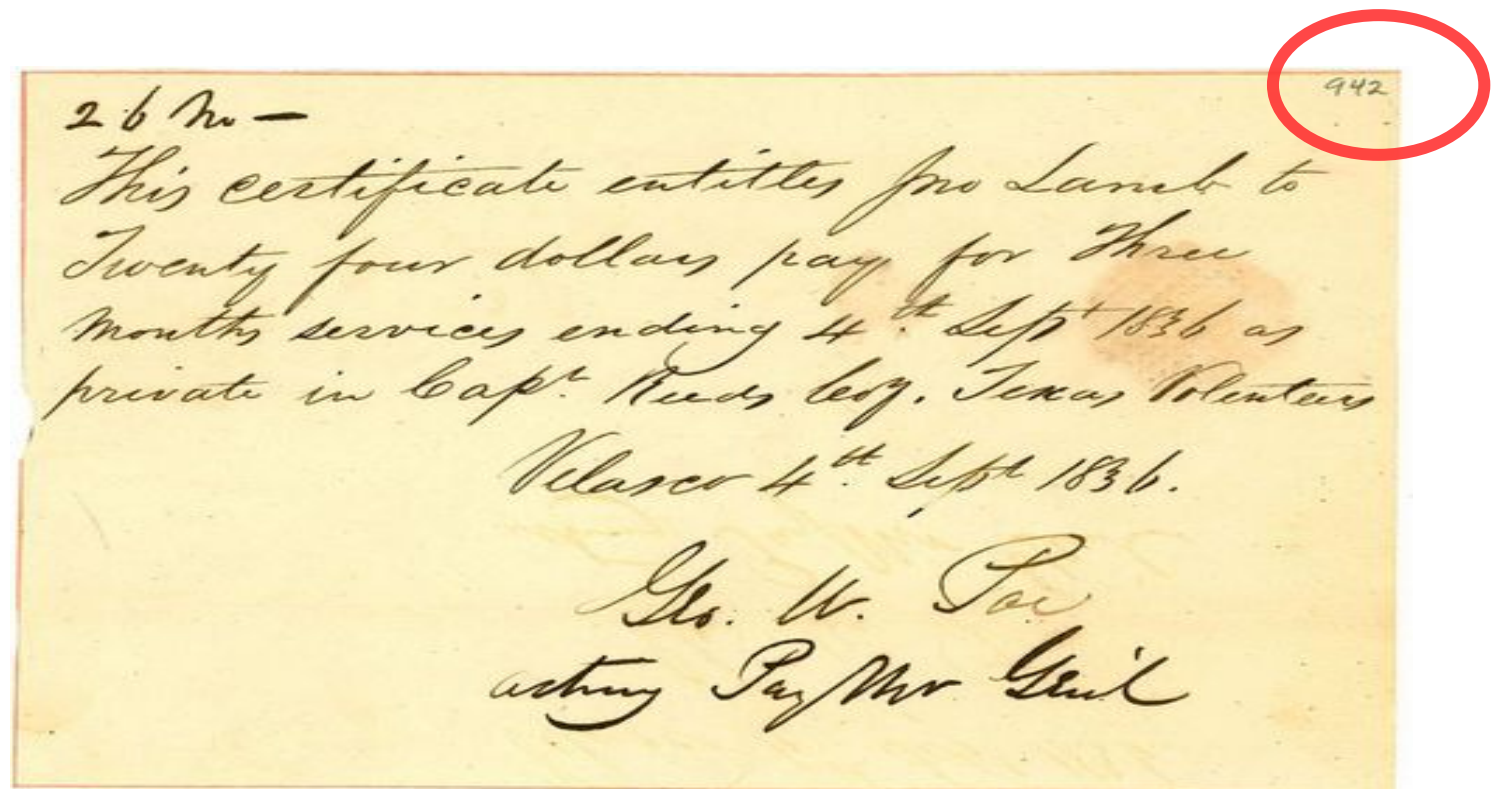
22.03.2006 г.

 (Свибунцов А.Г.)

Цифровая расписка, подписанная личным  
КЛЮЧОМ ПОЛЬЗОВАТЕЛЯ

# Как работает Bitcoin? Шаг 2

Для отличия одной расписки от другой вводится  
*уникальный идентификатор расписки*



# Как работает Bitcoin? Шаг 3

Каждый может проверить идентификатор по своей копии базы данных (Blockchain)



# Как работает Bitcoin? Шаг 4

Каждый выражает свое мнение по поводу транзакции

Транзакции объединяются в блоки

Блоки подтверждаются ~каждые 10 минут



# Как работает Bitcoin? Шаг 5

Чтобы проголосовать, надо предоставить доказательство работы

Только первый голос учитывается

Первому выдается вознаграждение



# Как работает Bitcoin? Шаг 6

Вероятность стать первым  
равна проценту  
вычислительных ресурсов

Контролировать сеть может  
только тот, кто контролирует  
51% вычислительных  
ресурсов

Система надежна пока честные пользователи  
контролируют 51% вычислительной мощности





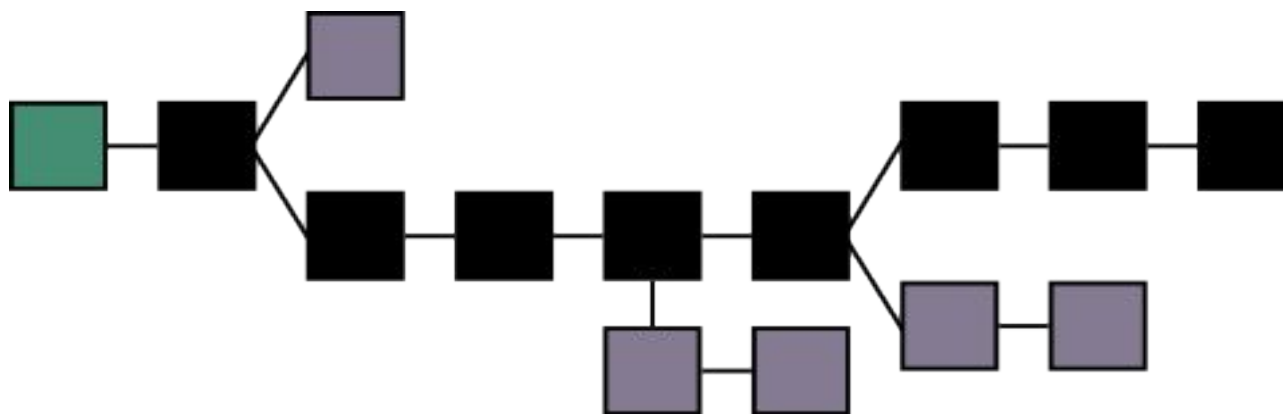
# Как работает Bitcoin? Шаг 7

Каждый блок содержит указатель на предыдущий

Если вдруг случается вилка, сохраняются обе цепочки

Дальнейшая работа ведется над длиннейшей цепочкой

Транзакция подтверждена если она находится в самой длинной цепочке и за ней следует 5 блоков



# Недостатки

Ограничения по скорости работы

Большой объем данных для хранения

Возможность проследить всю цепочку транзакций

Высокое потребление электроэнергии



# Вопросы?



kravchenkopo@gmail.com



ideateam\_macuser



ua.linkedin.com/in/pkravchenko/