Городское Бюджетное Образовательное Учреждение Средняя Общеобразовательная Школа 558 с углублённым изучением математики Выборгского района

Криптовалюта в современном мире

Работу выполнили
Ученики 11Б класса:
Вотинов Егор
Линевич Дмитрий
Николаев Дамир
Руководитель проекта:
Кольцова С.Г.

Санкт-Петербург
2018

Содержание

Введение

- Мы выбрали эту тему потому, что криптовалюта в современном мире начинают повсеместно развиваться и оказывают сильное влияние на экономику во всех странах

Цели и задачи

Цели : Рассказать о том , что такое криптовалюта ,

её влиянии на экономику , что ждет её в будущем.

Задачи : Собрать материал, подготовить тему представить эту тему перед аудиторией.

Теоритическая часть

С чего всё началось.

- История использования криптовалюты начинается в 2010 году, в Джексонвилле, штат Флорида. Программист по имени Laszlo Hanyecz , к своему счастливому удивлению, уговарил кого-то принять 10 000 Биткоинов в обмен на две пиццы от Пиццерии ,, Папа Джонс,, Путем причисления мистер Hanyecz, получил две свои пиццы за $30. Эта была самая первая в мире сделка с использованием криптовалюты.

Что такое Блокчейн простыми словами. Хэш и хэширование.

- Коля решил вести дневник. Для этого он завёл тетрадку и начал писать там строчки вроде таких:
- 1. Купил хлеба2. Позвонил Геннадию…132. Дал Васе в долг 100 рублей133. Ужинал134. Лег спать
- Он очень старался вести дневник честно, и если у него с кем-то возникал спор о чём-то, что произошло раньше, он доставал его и тыкал всем носом в свои записи. Однажды Коля сильно поспорил с Васей на тему того, давал ли он Васе в долг 100 рублей или нет. В момент спора у Коли не было с собой дневника, но он обещал завтра же принести и всё показать Васе.
- Вася решил не искушать судьбу, пробрался к Коле в дом, нашёл дневник, долистал до строчки 132 и заменил её на «Купил яйца». На следующий день Коля достал дневник, долго искал в нём запись про долг Васе, не нашёл и пришел извиняться.

- Прошёл год, Васю замучила совесть, и он признался во всём Коле. Коля простил друга, но решил на будущее использовать какую-нибудь более надёжную систему записи, которую нельзя было бы так просто подделывать.
- Придумал он следующее. У себя в операционной системе «Линупс» он нашёл программу md5sum, которая брала любой текст и превращала его в хеш — 32 непонятные цифры. Как именно она это делала, Коля не понимал, но в целом казалось, что она выдавала полную белиберду. Например, если в программу ввести слово «привет», она в ответ выдаёт «8b4609d7e974702ff1451220c7ededcf». А если ввести, казалось бы, почти то же самое, но с лишним пробелом, то уже «69ab827825fdb876e709abd3d783dbb6».

- Почесав тыковку, Коля придумал способ усложнить будущим Васям замену записей следующим образом: после каждой записи он вставлял хеш, который получался, если скормить программе текст записи и прошлый хеш. Новый дневник получался таким:
- 0000 (начальный хеш, ограничимся для простоты четырьмя знаками)1. Купил хлеба4178 (хеш от 0000 и «Купил хлеба»)2. Позвонил Геннадию4234 (хеш от 4178 и «Позвонил Геннадию»)…4492132. Дал Васе в долг 100 рублей1010133. Завтракал8204 (хеш от 1010 и «Завтракал»)

- Если теперь какой-нибудь Вася захочет изменить строчку 132, изменится и хеш этой строчки (он будет не 1010, а чем-то другим). Это, в свою очередь, повлияет на хеш строчки «133.Затракал» (он будет не 8204, а чем-то другим), и так далее до конца дневника. Теперь ради одной записи Васе придётся подменить весь дневник после неё, что сложно.
- Прошло время, Коля открыл банк. Он всё так же писал в дневничок записи «дал в долг» и «взял в кредит», снабжая их хешами. Банк разросся, и однажды он дал в долг (уже новому) Васе миллион. Следующей ночью десять нанятых Васей за полмиллиона работников пробрались в комнату Коле, заменили запись «143313. Дал в долг Новому Васе 1000000» на «143313. Дал в долг Новому Васе 10» и по-быстрому пересчитали все хеши вплоть до конца дневника.

- Чудом Коля обнаружил подмену и, раз такое дело, решил усложнить способ подделки дневника: «Теперь, — решил Коля, — я буду в конце каждой записи в скобочках добавлять какое–нибудь число („нонс“), а подбирать его буду так, чтобы каждый хеш заканчивался на два нуля». Единственный способ это сделать — тупо перебирать числа, пока не получится нужный хеш:
- 0000 (начальный хеш, ограничимся для простоты четырьмя знаками)1. Купил хлеба (22)4100 (хеш от 0000 и «Купил хлеба (22)», 22 было подобрано, чтобы хеш кончался на 00)2. Позвонил Геннадию (14)3100 (хеш от 4100 и «Позвонил Геннадию (14)»)…1300132. Дал Васе в долг 100 рублей (67)9900133. Завтракал (81)8200 (хеш от 9900 и «Завтракал (81)»)

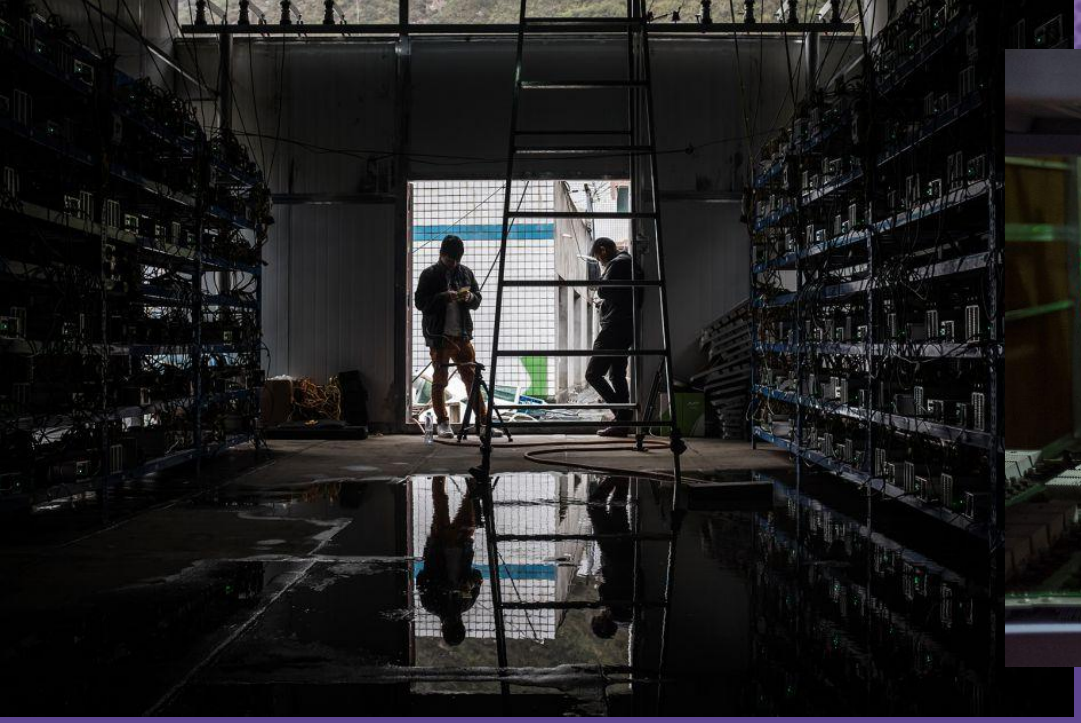
- Для создания каждой записи Коле теперь в среднем нужно будет перебрать порядка 50 чисел, что трудозатратно. Соответственно, если запись кто-то подменит, подделка её и всех последующих будет тоже в 50 раз сложнее, а это значит, что теперь Васе даже с работниками не справиться.
- Через какое–то время Коля взял себе партнёра и они стали оба вести дневничок. Для каждой новой записи оба одновременно начинали подбирать нонс и тот, кому первому удавалось найти подходящий, вносил запись. Так как вдвоём подбирать нонсы быстрее, Коля усложнил задачу и требовал, чтобы все хеши кончались уже на три нуля, а не на два.
- Этот окончательный Колин дневничок по сути и есть настоящий блокчейн, только Колю с другом надо заменить на кучу соединённых по сети компьютеров, а вычисления хешей усложнить, чтобы даже компьютерам было тяжко.

Самая известная потеря биткоинов

- Джеймс Хауэлс купил 7500 биткоинов в 2009 году, когда их стоимость была равна почти нулю. А к 2013 году один биткоин оценивался в 613 фунтов стерлингов. Таким образом, ценные бумаги Хауэлса стали стоить 4,5 миллиона фунтов стерлингов.
- Проблема была только в том, что Хауэлс оставил жёсткий диск с данными в ящике стола и забыл об этом, а затем выбросил с ненужными бумагами. После осознания ужасного он попробовал разыскать диск, но ему сказали, что он уже на свалке. Восстановить утерянные данные оказалось невозможно.

Майнинг биткоинов

- Пользуясь дешевой и обильной энергией ГЭС, которую требует армия компьютеров, майнинг распространяется в отдаленных районах китайской провинции Сычуань. В темных и изолированных складах, bitcoin громко гудят в унисон машины решающие уравнений для получения высокой цены криптовалюты.
- В 2016 году китайский фотограф Лю газеты провели время в Китае биткоин-шахтах и с шахтерами, которые контролируют огромные коридоры со станки для производства криптовалют для разных клиентов. По словам Лю, шахтеры, как правило, живут в общежитиях компаниями на несколько дней лишь иногда путешествуя десятки километров до ближайшего города.
- Несмотря на увеличение государственного надзора за китайской торговлей bitcoin, страна остается важным игроком в добыче bitcoin, благодаря дешевой электроэнергии и вычислительной. Китайские клиенты, которые платят за добычу bitcoin от их имени могут удаленно контролировать прогресс с помощью приложения на своих мобильных телефонах.



Что можно купить за криптовалюту

- В современном мире за биткоин можно купить все что тебе угодно, начиная пиццей и заканчивая билетами в космос, огромными территориями.
- То, что будут продавать за биткоины зависит только от общества и людей которые принимают их в оплату. Мы сами решаем, что будем покупать за криптовалюту.

Практическая часть

График изменений курса 1 биткоина к российскому рублю

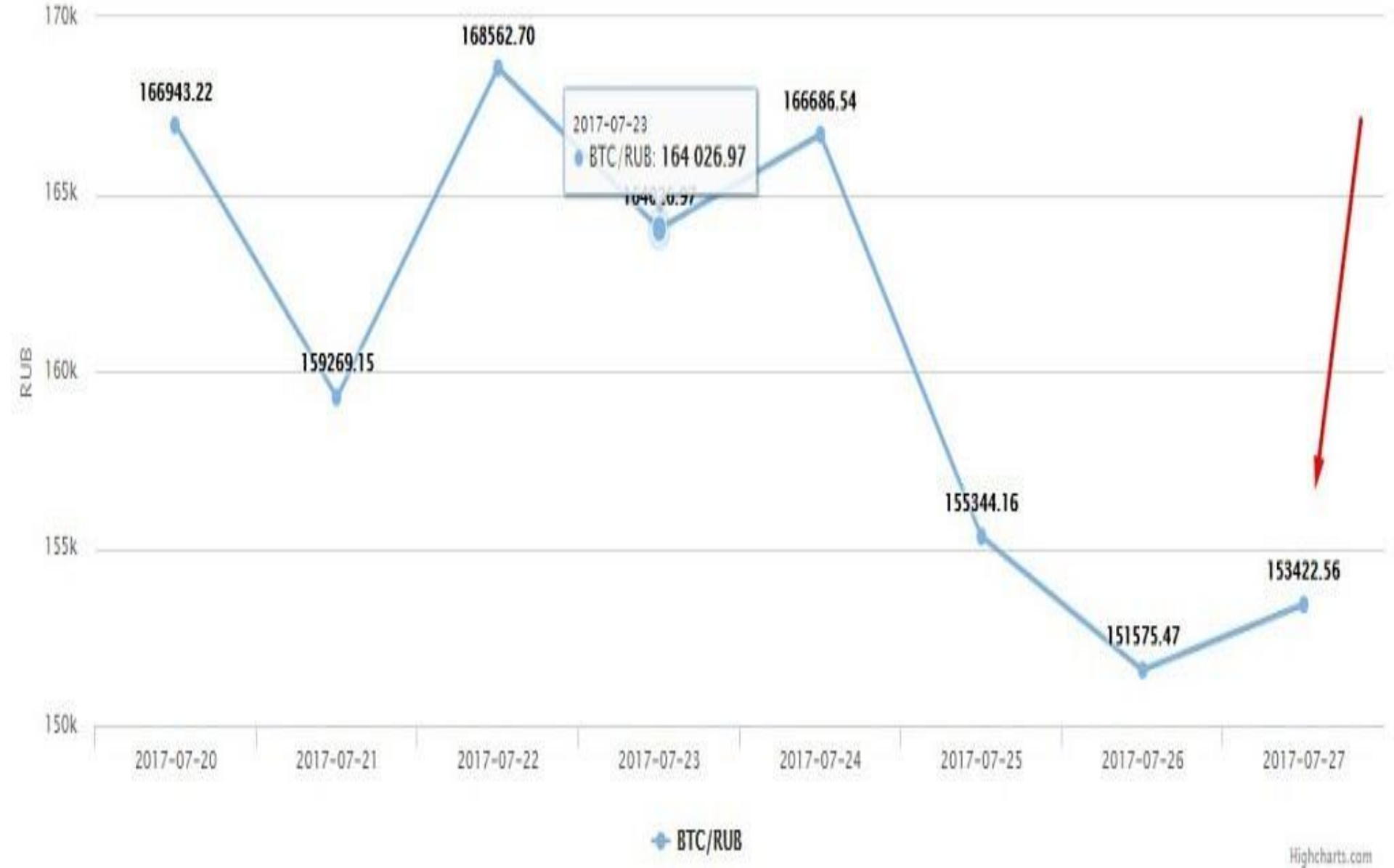
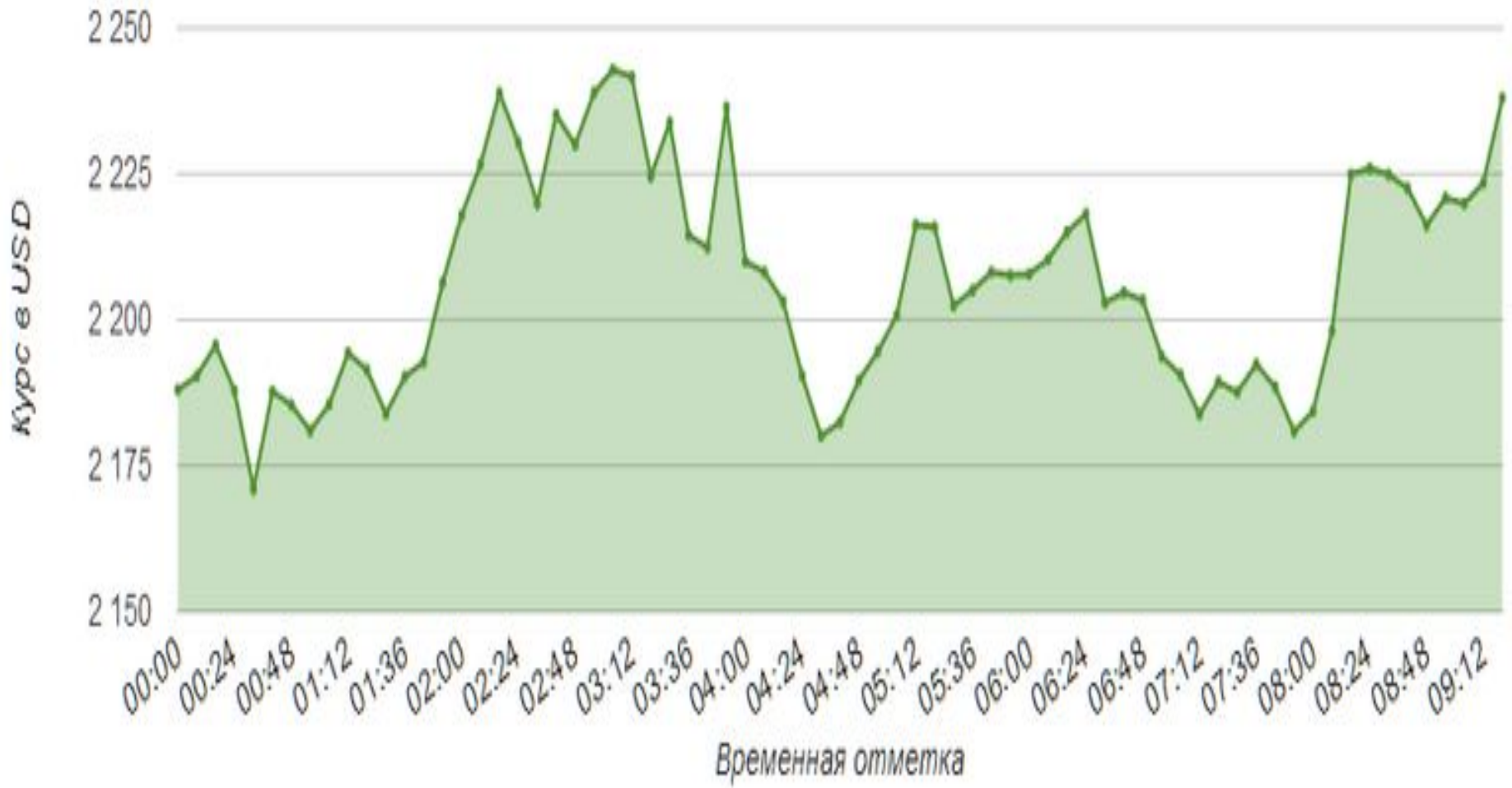
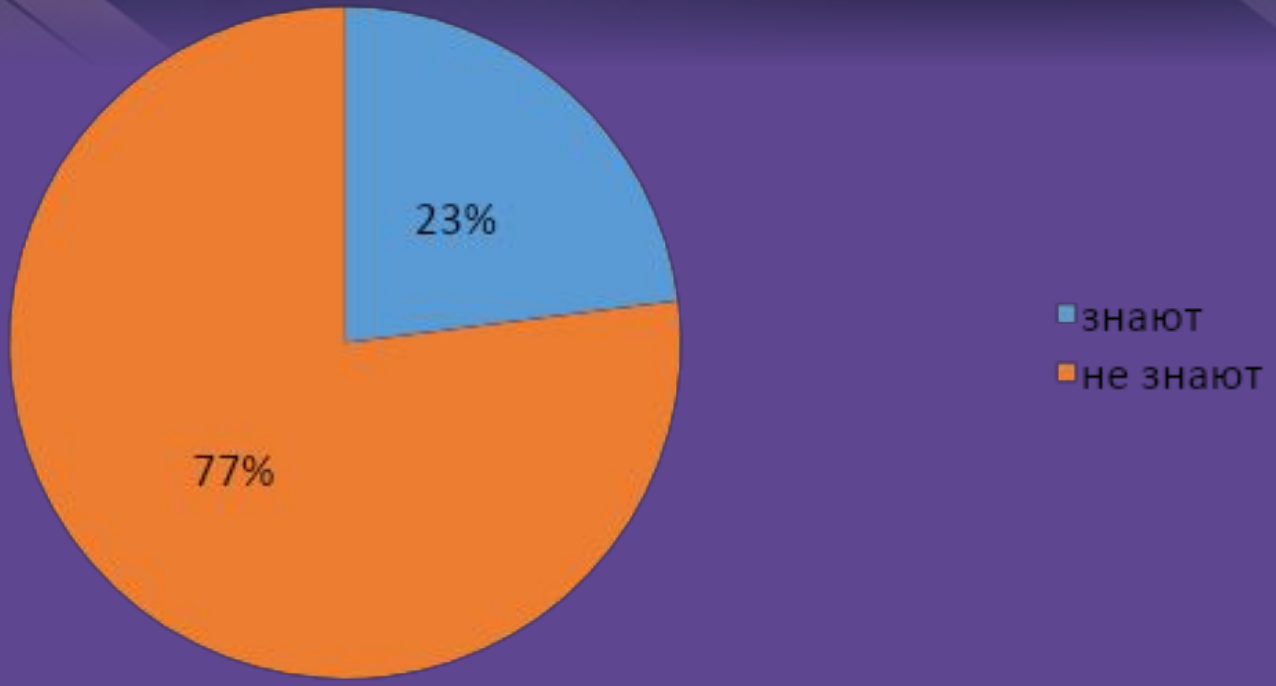


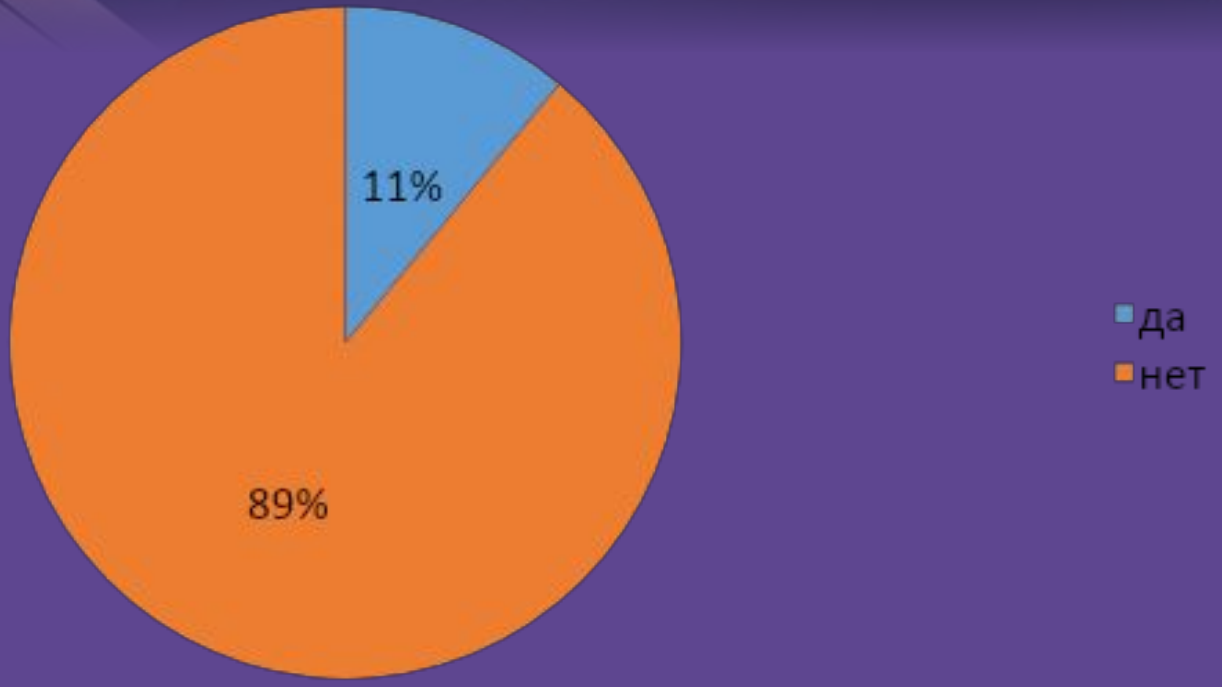
График изменения курса Биткоина сегодня



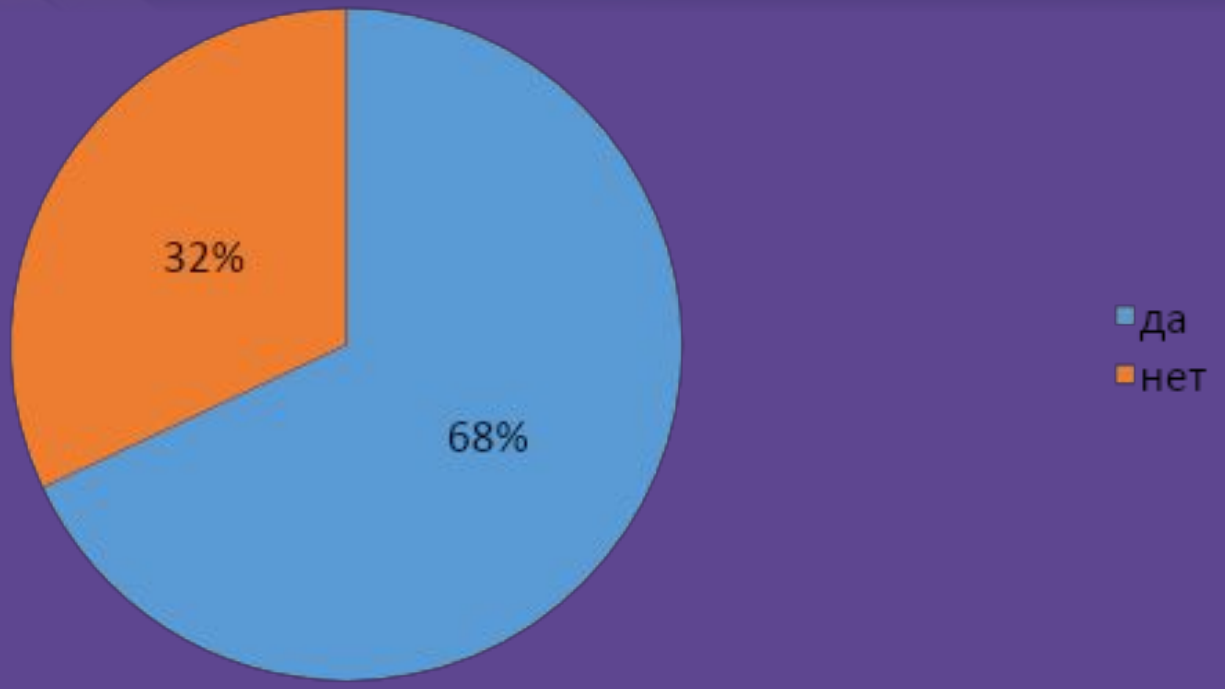
Знание что такое криптовалюта



Использование криптовалюты



хотели бы узнать



Заключение

- Криптовалюты- весьма перспективный экономический проект, направленный на повышение свободы экономических действий, но пока еще, в большинстве стран данная система недоступна широким массам ввиду ее сложности и необычности

Литература

- https://bits.blogs.nytimes.com/2013/12/22/disruptions-betting-on-bitcoin/
- https://tjournal.ru/41306-samoe-ponyatnoe-obyasnenie-principa-raboty-blokcheyna
- https://www.factroom.ru/life/10-losers
- https://qz.com/1026605/photos-chinas-bitcoin-mines-and-miners/
- https://yandex.ru/images/search?text=график%20изменения%20курса%20биткоина