Microsoft

Microsoft Developer School

30 листопада 2017 року, Київ

https://aka.ms/msdevschoolnov

#msdevschool

BLOCKCHAIN

індустрії, сценарії і технології. Розгортаємо Blockchain інфраструктуру в хмарі Azure

Самое простое обьъяснение принципа работы blockchain

Жил был Коля

Коля решил вести дневник. Для этого он завёл тетрадку и начал писать там строчки вроде таких:

Дневник Коли
1. Купил хлеба
2. Позвонил Геннадию...
...
132. Дал Васе в долг 100 гривен
133. Встретился с Людой
134. Пел

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 «Гулял с Олей».

Дневник Коли
1. Купил хлеба
2. Позвонил Геннадию...
...
132. Гулял с Олей
133. Встретился с Людой
134. Пел

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

0000 (начальный хеш, ограничимся для простоты четырьмя знаками)
1. Купил хлеба 4178 (хеш от 0000 и «Купил хлеба»)
2. Позвонил Геннадию 4234 (хеш от 4178 и «Позвонил Геннадию»)
...
132. Дал Васе в долг 100 рублей 1010
133. Встретился с Людой 8204 (хеш от 1010 и «Встретился с Людой»)

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 таджиков 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)»)

...

132. Дал Васе в долг 100 рублей (67) 9900
133. Встретился с Людой (81) 8200 (хеш от 9900 и «Встретился с Людой (81)»)

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.

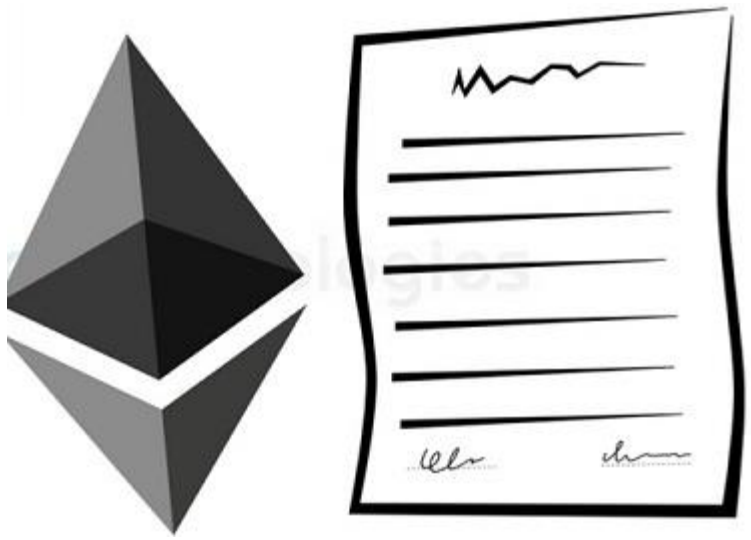
Что же такое blockchain?

Блокчейн — это не более чем дневничок записей, который можно записывать совместно, и в котором де-факто невозможно подделать старые записи.

Биткоин — это дневничок, где каждая запись имеет вид «Передать столько-то денег с кошелька X на кошелёк У». Так как дневничок нельзя подделать и в нём хранится вся история переводов, в любой момент из него можно вычислить количество денег на каждом кошельке. Ну а чтобы в системе вообще были какие-то деньги, биткоин сделан так, что каждая запись в дневничке заканчивается словами «Произвести Z монет и перевести мне», где «мне» — это тот пользователь, кто первым «угадает» нонс, который обеспечит хеш с нужным количеством нулей в конце.

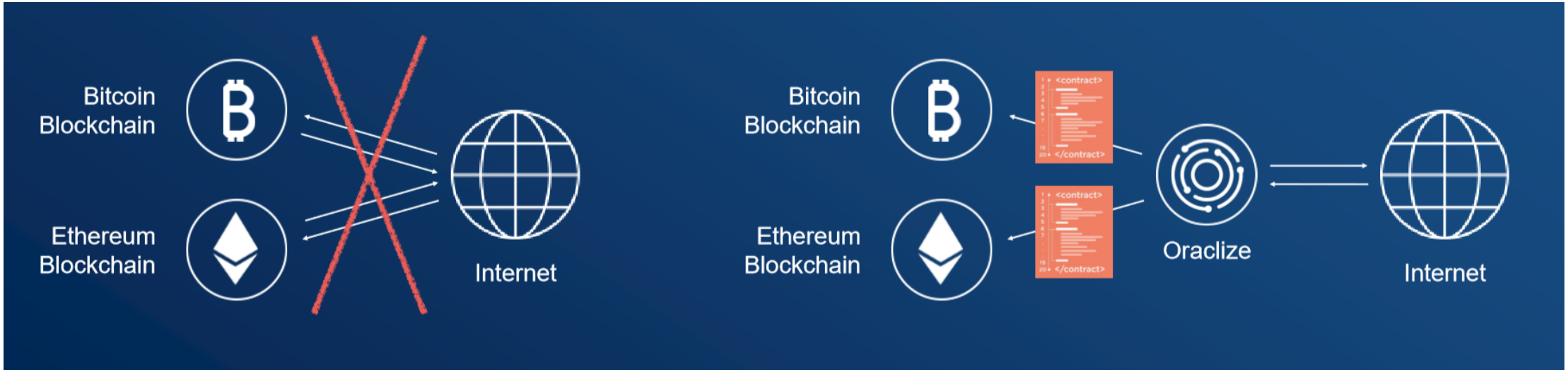
Smart-контракты

Поверх дневничка с некоторым количеством криптографии можно строить другие интересные системы. Например, можно делать записи в духе «Кто решит уравнение f(x) = 14, тот получает 10 монеток». Соответственно, первая запись в дневничке, где будет предоставлено решение, может автоматически считаться получателем монеток. Вокруг этой и схожих идей строятся так называемые «контракты».



Как работает smart-контракт

Использование внешних данных



Solidity - статически типизированный JavaScript-подобный язык программирования, созданный для разработки самовыполняющихся контрактов, исполняющихся на виртуальной машине Ethereum (EVM)

```
contract MyToken {
    /* This creates an array with all balances */
    mapping (address => uint256) public balanceOf;

    /* Initializes contract with initial supply tokens to the creator of the contract */
    function MyToken(
        uint256 initialSupply
        ) {
        balanceOf[msg.sender] = initialSupply;              // Give the creator all initial tokens
    }

    /* Send coins */
    function transfer(address _to, uint256 _value) {
        require(balanceOf[msg.sender] >= _value);               // Check if the sender has enough
        require(balanceOf[_to] + _value >= balanceOf[_to]);     // Check for overflows
        balanceOf[msg.sender] -= _value;                        // Subtract from the sender
        balanceOf[_to] += _value;                               // Add the same to the recipient
    }
}
```

More

Сферы применения

Выборы

Благодаря умным контрактам
и распределенному
хранению можно пол
исключить возможно
внешнего вмешательс
систему голосования.

Логистика и снабжение

«UPS может исполнять контракты, в которых будет
сказано: “Если мы получим оплату за доставку товара, то
его производитель, который в це
на много звеньев выше, немедле
новый такой товар, поскольку это
назначению”».

Автомобили

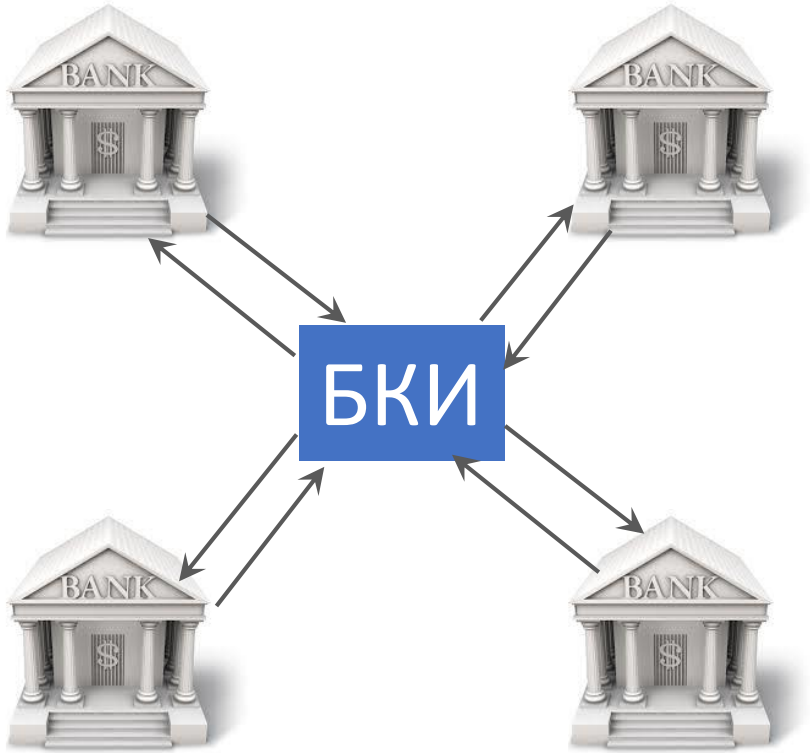
Задумайтесь о будущем, где все
будет автоматизировано.
Google уже строит его, создав
умные телефоны, умные очки
даже умные автомобили. И
здесь на помощь придут умны
контракты.

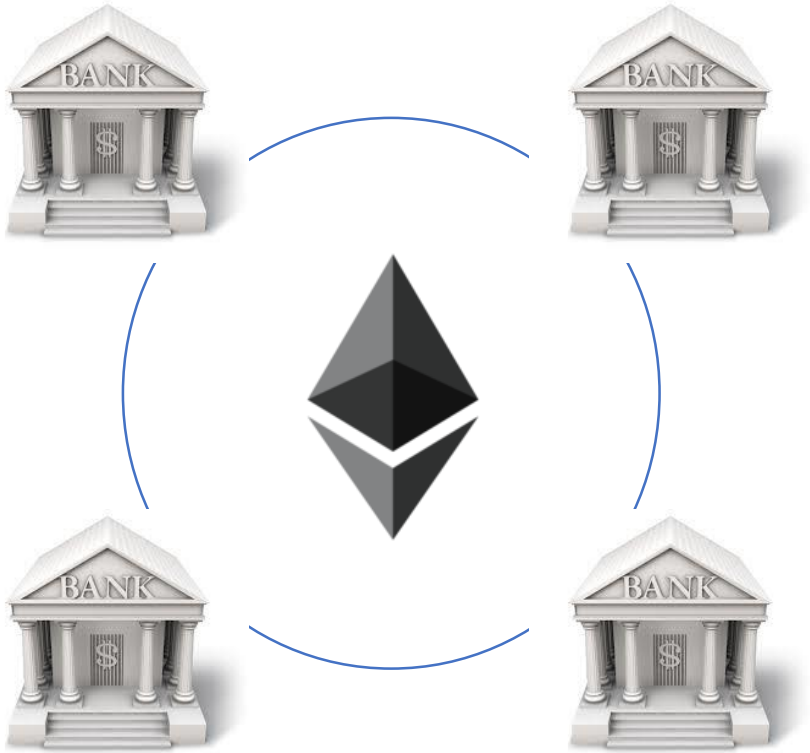
Другие сферы

Другие индустрии, такие как эквайринг, кредитование и бухгалтерский учет, тоже будут использовать умные контракты — например, для оценки рисков и аудита в режиме реального времени. Юристы смогут перейти от составления традиционных контрактов к созданию типовых образцов умных контрактов.

Сервис гарантированных покупок

Бюро кредитных истрий

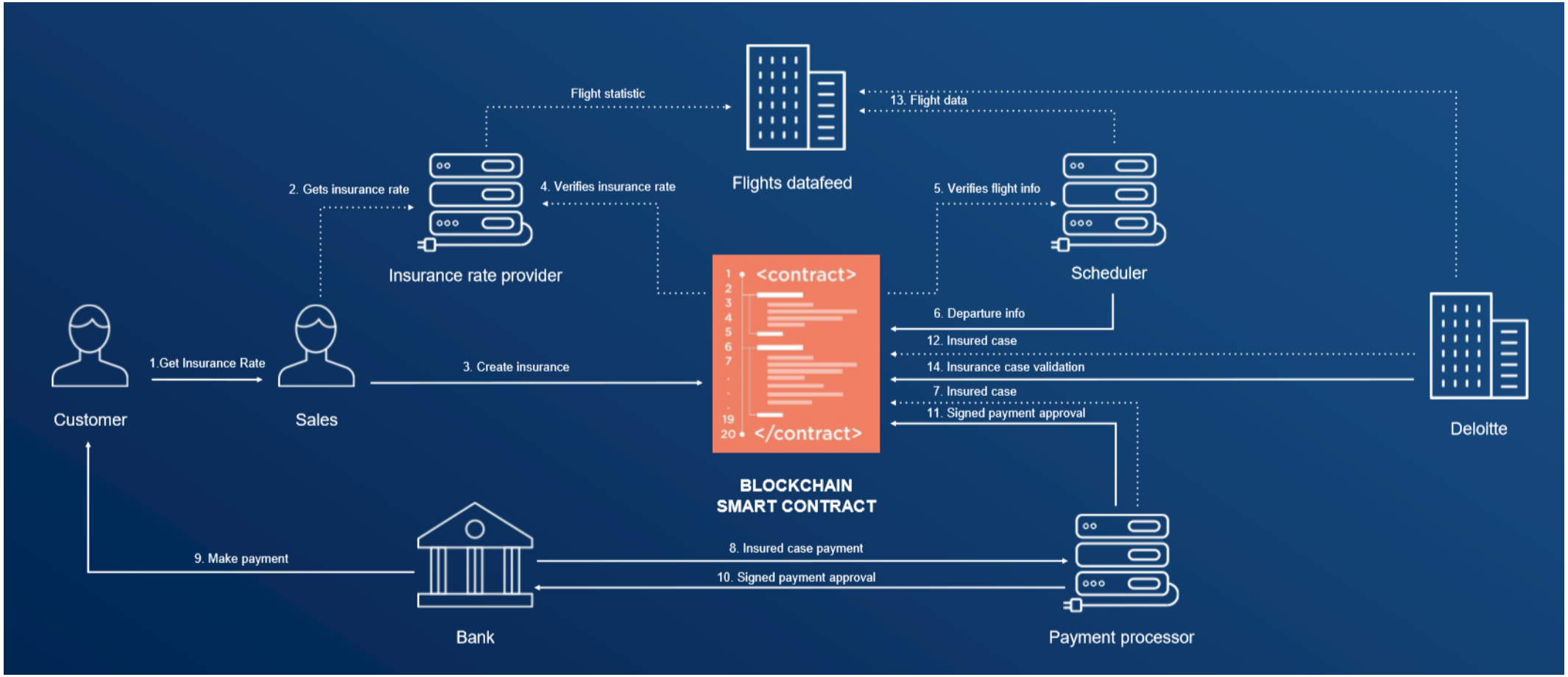




Продажа недвижимости

Buydentity: Борьба с контрафактом

Страхование от задержки вылета самолета



Плюсы умных контрактов

1

Независимость

Не нужно искать специалиста, чтобы заключить сделку.

2

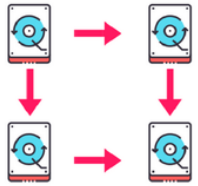
Безопасность

Контракт хранится в зашифрованном виде в распределенном реестре.

3

Надежность

Все документы многократно продублированы в блокчейне.



4

Экономия

Нет необходимости оплачивать услуги посредников.

5

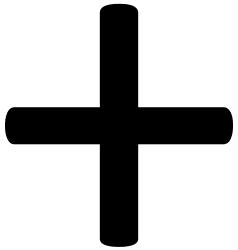
Точность

Не нужно заполнять вручную множество форм с риском допустить ошибки.

Минусы умных контрактов

- Умные контракты далеки от совершенства. Что если в код попадут ошибки? (TheDAO - украдено $50 миллионов)
- Как должно регулировать эти контракты государство? И как оно будет взимать налоги с таких транзакций?
- Список возможных проблем этим не ограничивается. Специалисты пытаются решить все вопросы, но подобные трудности отталкивают многих возможных пользователей.

Demo: развертывание Ethereum в Azure



ethereum