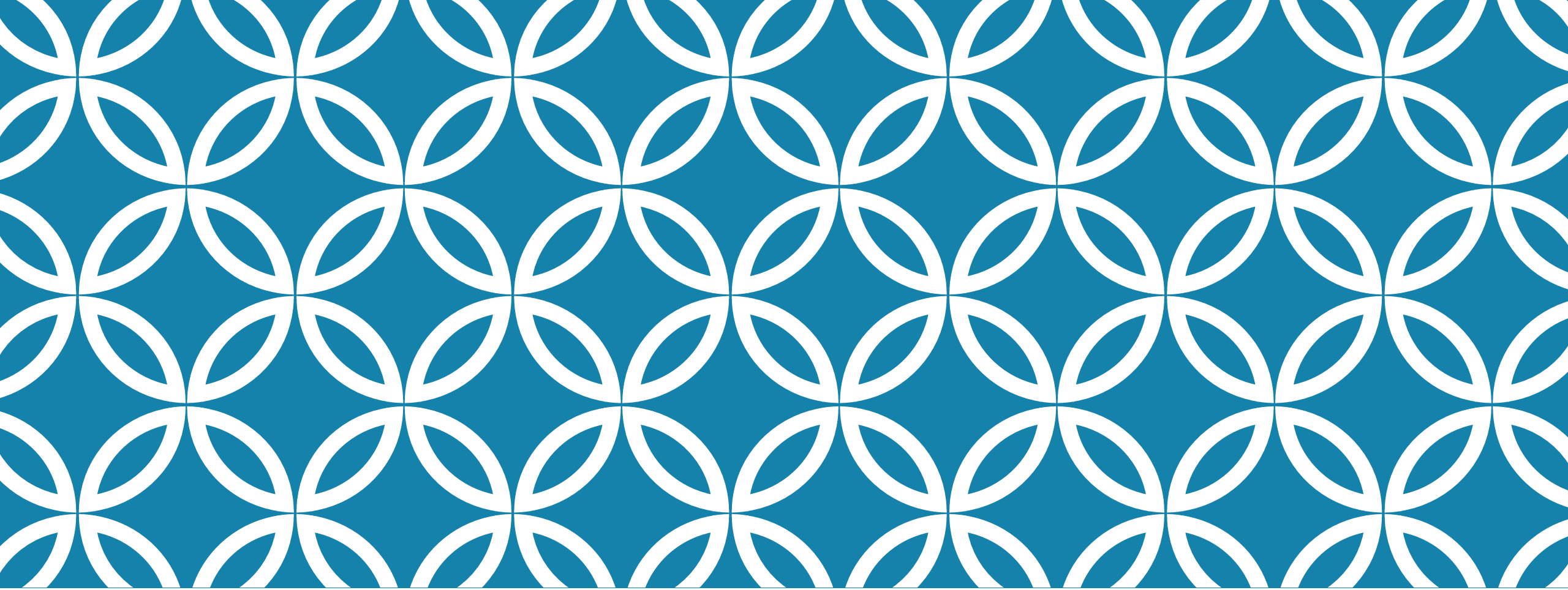


СФЕРЫ ПРИМЕНЕНИЯ BLOCKCHAIN В БИЗНЕСЕ

Ершово, Московская обл.
22 сентября 2017 г.

ЧТО ТАКОЕ БЛОКЧЕЙН?

«Технология blockchain на мой взгляд, — это новый интернет. Это идея такого же уровня, как интернет. И она не успела ещё родиться, как наш центробанк сказал, что криптовалюты нельзя выпускать. Потом они сказали, что их нельзя ещё покупать, а теперь они говорят, что тех, кто попытается их купить, могут посадить в тюрьму. Мы понимаем, что весь прогресс в этом случае уйдёт за пределы России, все наши специалисты в области blockchain будут вынуждены работать в более удобных юрисдикциях»

«Я думаю, пять-десять лет — и мы увидим гигантский сдвиг во всей экономике»

«Меня спрашивают, останется ли Сбербанк после того, как эта технология будет зрелой. Это очень большой вопрос, какой из видов бизнеса вообще останется»

Блокчейн (с англ. - цепочка блоков) – это распределенная децентрализованная база данных

Блокчейн изнутри

Блокчейн – учетная книга записей.

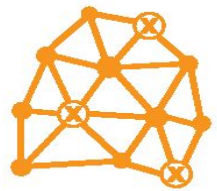
Цепочка страниц в книге = Цепочка блоков в блокчейне.

Аналогия книги и блокчейна

1.
Невозможно незаметно вырвать страницу

2.
Невозможно изменить существующий текст

3.
Содержание книги хранится во множестве экземпляров



1.
Нельзя удалить данные

2.
Нельзя подделать информацию

3.
Информация в сети блокчейн хранится на множестве узлов

Преимущества блокчейна

Неизменяемость

Невозможно скорректировать изменения,
уже внесённые в базу данных,
без согласия большинства участников

Лёгкость аудита

Аудит может быть проведён любым
участником сети, корректность любого изменения
можно легко подтвердить.

Доверие

Архитектура сети позволяет убрать из рассмотрения
вопрос доверия провайдеру инфраструктуры.

Экономия

Устранение посредников и онлайн-аудит
приводят к снижению рисков и издержек на
обработку транзакций.

ГЛАВНОЕ СВОЙСТВО БЛОКЧЕЙНА

Блокчейн устраняет НЕДОВЕРИЕ между людьми, организациями.

Он меняет парадигму человеческих взаимоотношений

НЕМНОГО ИСТОРИИ

Дориан Сатоши Накомото

Крейг Райт

НЕМНОГО ИСТОРИИ

30 октября 2008 г. – обращение Накамото в форуме криптографов

3 января 2009 года появился Ginesis block

2010 году 22 мая – сделка с пиццей

2011- биткоин торгуется на бирже

2012 – первый банкомат на биткоин

Ноябрь 2013 – резкий рост курса

Сейсчас курс – $3870

КАКИЕ ВОПРОСЫ РЕШАЛ САТОШИ ПРИ СОЗДАНИИ BITCOIN

1. Задача византийских генералов.

2. Как создать распределенную и децентрализованную сеть

3. Как замотивировать участников сети поддерживать её, формировать и подтверждать блоки с трансакциями

4. Как прийти к консенсусу

5. Как передавать большие объемы информации

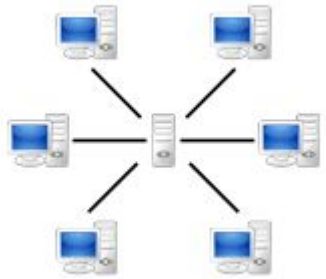
6. Как надежно зашифровать трансакции

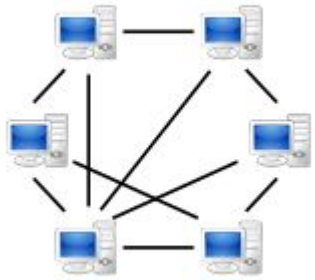
7. Экономика

ЗАДАЧА ВИЗАНТИЙСКИХ ГЕНЕРАЛОВ

КАК СОЗДАТЬ РАСПРЕДЕЛЕННУЮ И ДЕЦЕНТРАЛИЗОВАННУЮ СЕТЬ

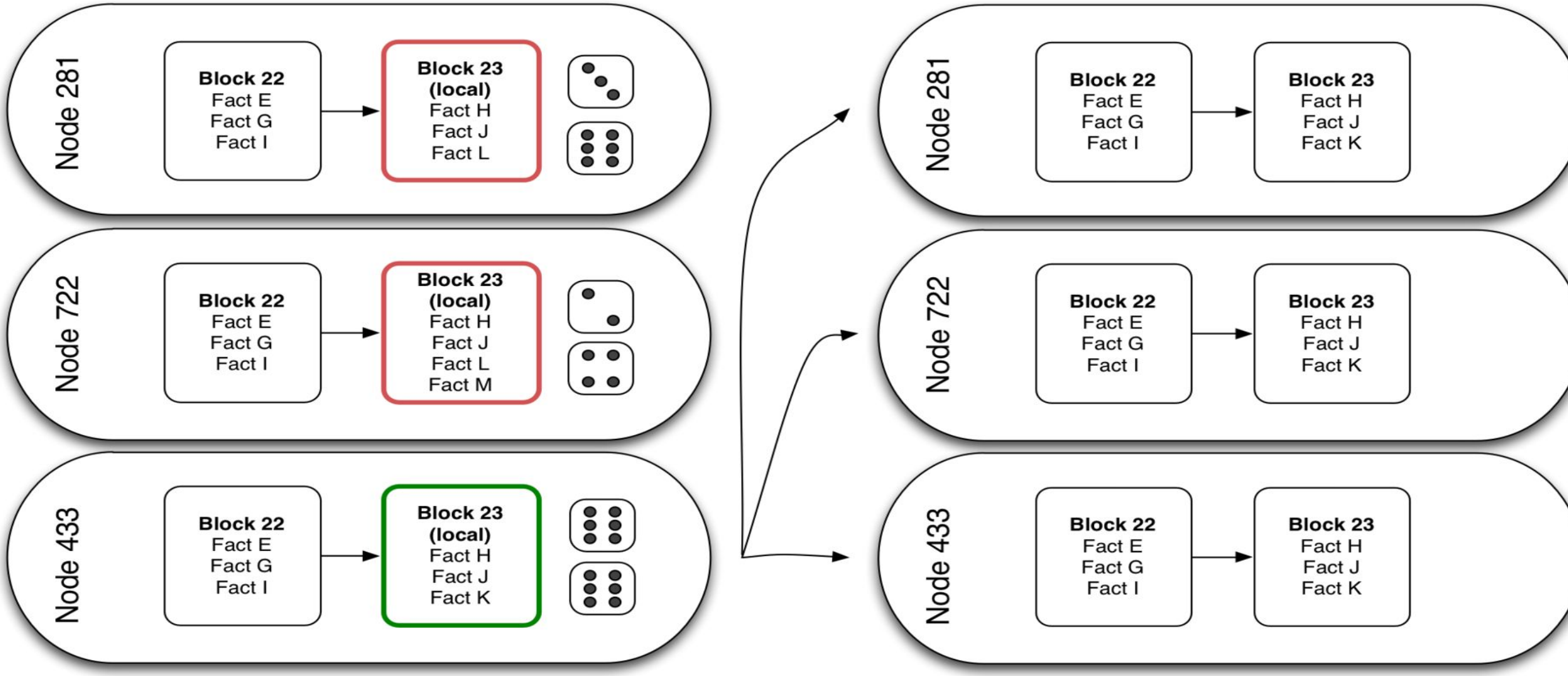
Однора́нговая, децентрализо́ванная, или пи́ринговая (англ. **peer**-to-**peer**, **P2P** — равный к равному) сеть — это компьютерная сеть, основанная на равноправии участников. Часто в такой сети отсутствуют выделенные серверы, а каждый узел (**peer**) является как клиентом, так и выполняет функции сервера.





КАК ЗАМОТИВИРОВАТЬ УЧАСТН

Майнинг, также добыча (от англ. mining — добыча полезных ископаемых) — деятельность по поддержанию распределенной платформы и созданию новых блоков с возможностью получить вознаграждение в форме новых единиц и комиссионных сборов в различных криптовалютах, в частности в Биткойн.



ПРОЦЕСС МАЙНИНГА

КОНСЕНСУС

Проблема двойных трат

Proof-of-work

Proof-of-stake

БОЛЬШИЕ ОБЪЕМЫ ИНФОРМАЦИИ

Хэширование или **хеширование** (англ. hashing) — преобразование массива входных данных произвольной длины в (выходную) битовую строку фиксированной длины, выполняемое определённым алгоритмом.

// проигрышный хэш для Bitcoin
787308540121f4afd2ff5179898934291105772495275df35f00cc5e44db42dd

// выигрышный хэш для Bitcoin, если n=10
00000000009f766c17c736169f79cb0c65dd6e07244e9468bc60cde9538b551e

КАК НАДЕЖНО ЗАШИФРОВАТЬ ИНФОРМАЦИЮ

8(926)343-12-60 = 44=4+4=8 (пример хэширования с алгоритмом сумма)

Хеширование +Ассиметричная система защиты информации

Общедоступный и Частный (Private) ключи

С.Накамото: «Мы считаем, что цифровая монета – это последовательность цифровых подписей. Каждый держатель переводит монету следующему владельцу, поставив свою цифровую подпись и открытый ключ следующего владельца. Получатель может проверить достоверность подписей и убедиться, что данный биткоин действительно переходил от одного владельца к другому».

ЭКОНОМИКА

Криптовалюта – биткоины, эфиры, лайткоины и др. альткоины.

Токен – заменитель денег, внутренние деньги проекта:

Виды токенов:

- токены приложений
- кредитные токены
- токены-акции

Трансформация различных индустрий с применением технологии блокчейн

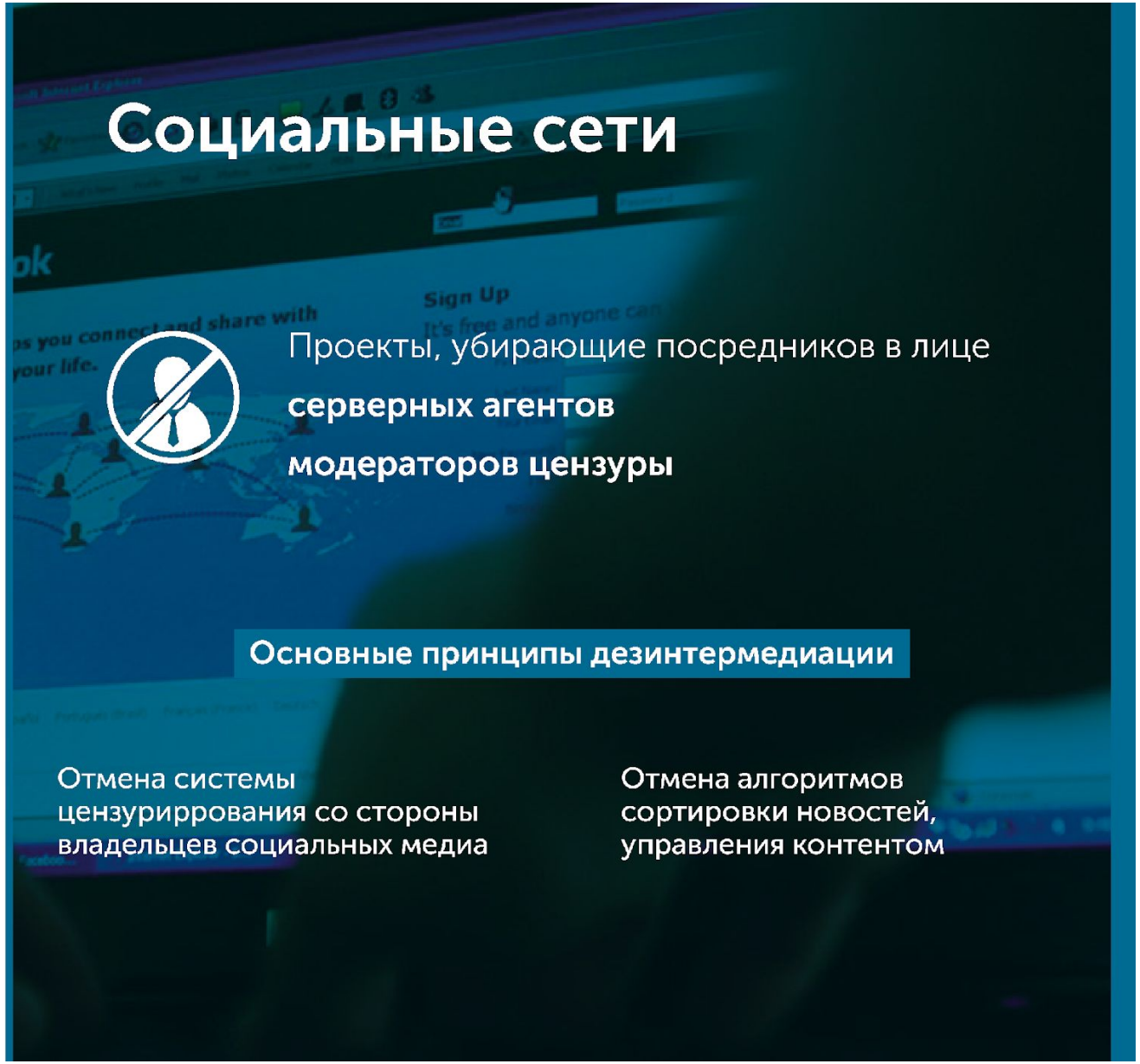
synereo

Штаб-квартира: **Ether, North Carolina**
Год основания: **2014**
Финансирование: **$4.7M Equity Crowdfunding** (October 26, 2016)

Synereo – социальная p2p-платформа, **позволяющая любому приложению существовать без централизованного сервера**, избавляя от необходимости мириться с использованием вашей личной информации тех-компаниями (Google, Apple, и т.д.)

Штаб-квартира: **Tel Aviv**
Год основания: **2014**
Финансирование: **$400k Seed** (January, 2015)

GetGems – мессенджер, который платит. Основанный на софте Telegram, и bitcoin, и GEMZ-кошелек в одном лице, **позволяет любому пользователю переводить деньги без посредников в лице банков**, бирж, трансфер-агентов, экверов



Штаб-квартира: **London, England**
Год основания: **2015**
Финансирование: **$118K Seed** (March, 2015) **Assistance from Mastercard** (2016)

Everledger – система обнаружения мошенничества на основе анализа больших объемов данных от страховщиков и юридических институтов. Блокчейн-книга для сертификации и ведения транзакций бриллиантов, позволяющая внести в реестр данные без привлечения юристов, страховых фирм.

Штаб-квартира: **London, England**
Год основания: **2015**
Финансирование: **$36.85k** (April, 2015) **$16.25k Seed** (July, 2015)

Blockverify – аналогичная платформа для фармацевтики, товаров роскоши, бриллиантов и электроники (в разработке). Обнаруживает контрафактные продукты, ворованные, фильтрует фродные транзакции. Позволяет обходить использование третьих лиц в лице: юристов, IP-специалистов, фрод-мониторинговые системы отдельных институтов

Антиконтрафакт

Проекты, убирающие посредников в лице

юристов

провайдеров страховых услуг

IP специалистов

Основные принципы дезинтермедиации

Сопротивление некачественным подделкам, контра- фактной продукции, за счет контроля производства продукта по supply chain

onename

Штаб-квартира:	New York, US
Год основания:	2013
Финансирование:	$1.33M (July, 2014)
Top Investors:	Y Combinator, Union Square Ventures

Onename – способ использовать свой идентификатор личности, который не требует каждый раз предоставлять личную информацию и позволяет подтверждать принадлежность всех твоих аккаунтов в соцсетях. От компаний типа Apple & Facebook вплоть до вебсайтов мы не знаем как и какие данные используются о нас. Onename позволяет обходить факт использования ID данных третьими серверами сайтов или провайдеров услуг.

ShoCard

Штаб-квартира:	Palo Alto, California
Год основания:	2015
Финансирование:	$1.5M Seed (July, 2015)
Top Investors:	Digital Currency Group, AME Cloud Ventures

Shocard – во многом аналогичная платформа в стадии разработки с акцентом на легкость и скорость применения идентификатора везде, где нужно подтвердить личность Также позволяет снизить риск несанкционированного использования данных, путем использования одного сервера с персонализированными опциями по предоставлению доступа.

Цифровая идентификация

Проекты, убирающие посредников в лице **серверов веб-сайтов**

посредников использующих онлайн-инфо

Основные принципы дезинтермедиации

Прозрачное и безопасное управление данными

Нет централизованного хранилища, базы данных ID профилей

Управляемый доступ и представление определённой инфо сайтам

ascribe®

Штаб-квартира:	Berlin, Germany
Год основания:	2014
Финансирование:	$2M Seed (June, 2015)
Top Investors:	Digital Currency Group, Earlybird Venture Capital, Freelands Ventures

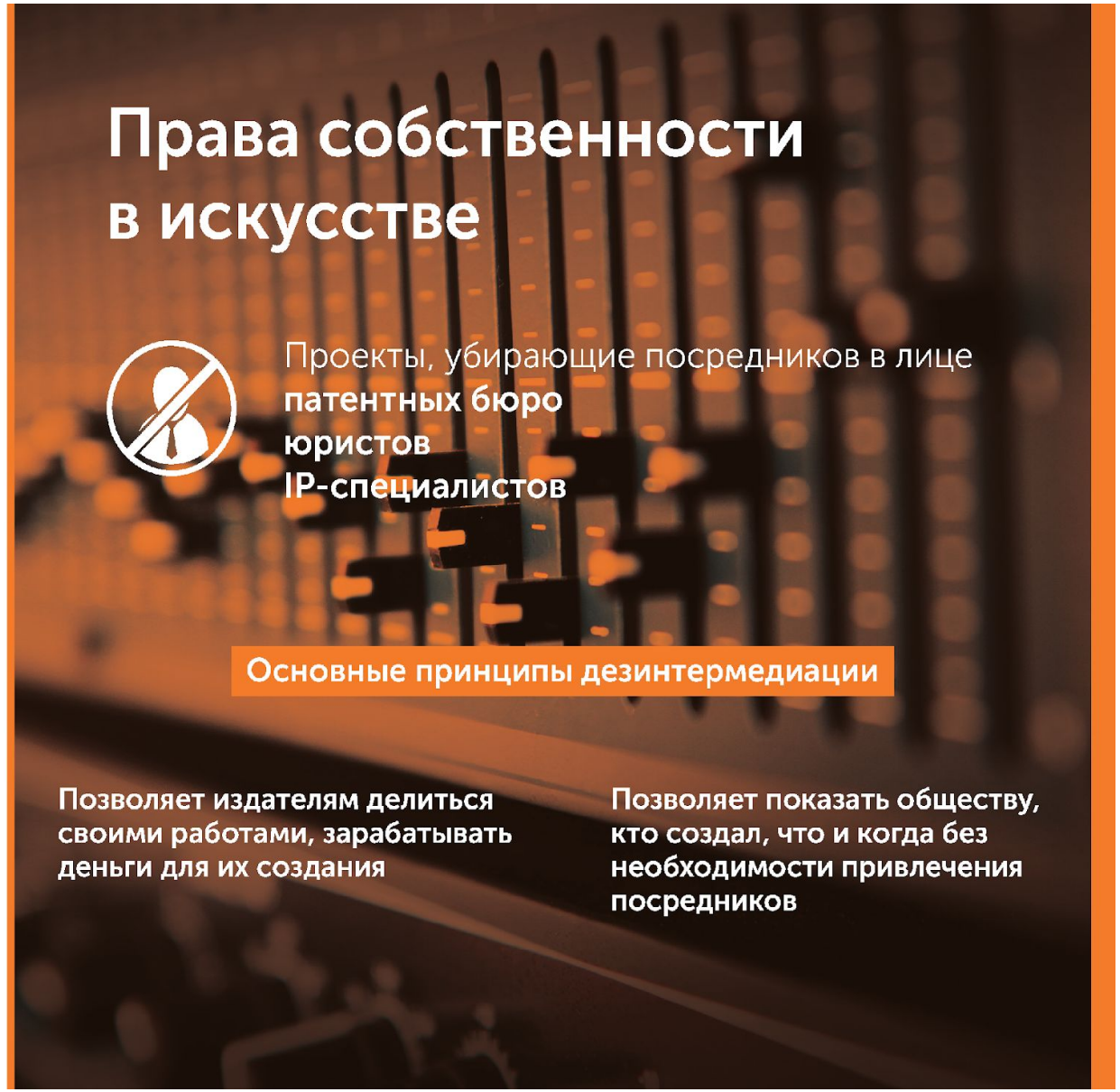
Ascribe – платформа для учета, передачи и проверки авторских прав без патентных бюро.

Авторам и создателям:

- Создавать неуязвимую связь между собой и своими творениями
- Делиться своей работой с кем угодно
- Прослеживать распространение своей работы в интернете
- Использовать сертификаты с криптозащитой для подтверждения прав собственности
- Выпускать ограниченные тиражи (впервые для электронного контента)
- Выдавать лицензии на использование твоих проектов без потери права собственности

Маркетплейсам:

- Интеграция в API Ascribe для подтверждения авторских прав, сотрудничества с авторами и управления контентом



Штаб-квартира: **Blacksburg, Virginia**
Год основания: **2012**
Финансирование: **$50k** (February, 2016)
$21.4k Product Crowdfunding (June, 2016)

Followmyvote - безопасная и прозрачная система онлайн-голосований

Убирает необходимость

для государств и органов власти в:

- Организации и управлении офлайн-площадками
- В контроле за соблюдением правил голосования
- В сборе, подсчете и анализе голосовых бюллетеней
- Голосующим – стоять в очередях на площадках

для акционерных обществ в:

- Регистраторах и трансфер-агентах
- Организации съездов акционеров

OTONOMOS

Штаб-квартира: **London, England**
Год основания: **2015**
Финансирование: **$36.85k** (April, 2015)
$16.25k Seed (July, 2015)

Otonomos – создание blockchain-chartered компании полностью онлайн в Сингапуре, Гонконге или Великобритании и управление компанией онлайн:

- Кошелек для каждого акционера и p2p-переводы акций
- Виртуальный кабинет директоров
- Автоматизация работы с помощью смарт-контрактов
- Онлайн-раунды финансирования

Управление

Проекты, убирающие посредников в лице

оффлайн организации процессов и контроля, сборе, анализе данных

Основные принципы дезинтермедиации

Содержит полную историю обновлений, защищенную от искажений криптошифрованием

Увеличивается скорость до 80 голосов в секунду

Копии реестра хранятся у всех участников сети

FILAMENT

Штаб-квартира: **Reno, Nevada**
Год основания: **2012**
Финансирование: **$7.45M**
/ Rounds from 25 Investors
Top Investors: **AngelList, Techstars, Samsung Ventures**

Filament – устройства, позволяющие объединять электронные приборы и технику в единую сеть. Имеет внешний прибор подключения – The Tap, и встраиваемый процессор для специальных решений – The Patch

Для:

Vending (торговые автоматы) – подключив автоматы к сети, следи эффективно за запасами товаров и состоянием машин.

Мониторинг оборудования – с помощью filament и GPS, отслеживай местоположение передвижного оборудования и состояние объектов.

Здоровье и безопасность – встроенные в защитные шлемы и прочие инструменты безопасности IOT-девайсы могут сигнализировать удары, приводить в исполнение геозональные ограничения и др.

EDC

Штаб-квартира: **Toronto, Ontario**
Год основания: **2015**
Финансирование: **$150k / Angel**
(February, 2016)

Equibit – дезентрализованный внебиржевой (over-the-counter, OTC) финансовый рынок.

Акционерное общество? Позволяет выпускать акции, следить за реестром акционеров и распределять дивиденды – без регистраторов, трансфер-агентов и брокеров.

Инвестор? Позволяет производить операции с ценными бумагами быстро в любое время в любом месте – на прямую с другими участниками, без центральных контрагентов и брокеров.

Интернет вещей и финансовая сфера

Проекты, убирающие посредников в лице

регистраторов

брокеров

трансфер-агентов

Основные принципы дезинтермедиации

Трекинг истории конкретного устройства в сети

Данные о взаимодействии данного устройства с людьми, сетью, внешним миром

Сокращение расходов на физических процессах финансовых институтов

Увеличение скорости проведения транзакций и др

blocksign

Штаб-квартира: New York, US
Год основания: 2011
Финансирование: $1M Series A (July, 2015, from 5 Investors)
Top Investors: Empire Ventures, Mesa Ventures

Blocksign – нотариальная блокчейн-книга, позволяющая подписывать и проверять на подлинность документы – без нотариусов

ORIGIN STAMP

Штаб-квартира: Germany
Год основания: 2012
Финансирование: Noncommercial project

OriginStamp – Ставит временной штамп на файле любого формата, подтверждающий время создания и автора документа – без нотариусов

UPROOV

Штаб-квартира: Perth, W.Australia

Uproov – мобильное приложение, позволяющее снимать фото и видео с автоматической фиксацией времени, места и автора съемки в блокчейне – без нотариусов

Нотариусы

Проекты, убирающие посредников в лице

юристов

нотариусов

Основные принципы дезинтермедиации

Упрощение процедуры заверения документов, интеллектуальной собственности, завещаний, доверенностей, договоров

Значительно сокращает время и цену заверения документов

Штаб-квартира:	**London, England**
Год основания:	**2013**
Финансирование:	**£120k Grant** (2014, from 2 investors)
	£40k Seed (Dec, 2013, from 1 investor)
Top Investors:	**Technology Strategy Board** **Wayr**

Provenance - Платформа для записи электронной истории всех физических продуктов, позволяющая прослеживать и удостоверять его происхождение, свойства и владельцев, уменьшая потребность в аудиторах, надзорных органах, контроле качества и т.д., а также в таможенном контроле.

skuchain

Штаб-квартира:	**Tel Aviv**
Год основания:	**2014**
Финансирование:	**$400k Seed** (January, 2015)

Skuchain – Устанавливает прозрачность и надежность и повышает эффективность производственного процесса, позволяя участникам действовать напрямую друг с другом без лишних звеньев цепи.

Supply chains и процессы производства

Проекты, убирающие посредников в лице

аудиторов

контроллеров

надзорных учреждений

Основные принципы дезинтермедиации

Создание прозрачности и доверия, предотвращение продажи краденного или фальсифицированного товара

Отслеживаются абсолютно все товары, ниже цена и выше прозрачность

КАК ИСПОЛЬЗОВАТЬ БИЗНЕСУ BLOCKCHAIN

1. ICO – initial coin offering
2. Краудфандинг
3. Умные контракты
4. Цепочки поставок
5. Сертификация

ЭЛЕКТРОННЫЙ ОПЦИОН НА ПРИОБРЕТЕНИЕ ПЕСКА

SAND COIN

Первый мире проект песчаного карьера, финансирующегося через привлечение криптовалют путем выпуска криптовалютного токена на добычу нерудных материалов. SAND COIN – блокчейн – дериватив, подкрепленный реальной продукцией.

Задача - привлечение средств в размере 3 528 600 US $ для финансирования разработки карьера. За 1й день ICO привлечено
1 200 000 US$

PRE-ICO

ПЕРВАЯ ФРАНШИЗА VR ПАРКОВ ПОД УПРАВЛЕНИЕМ БЛОКЧЕЙН.

Планируется выпустить токенов: 100 000 000

КРАУДФАНДИНГ

KICKICO.COM

Помогает стартаперам, разработчикам игр, лидерам блокчейн сообществ, предпринимателям, дизайнерам, и другим создателям находить поддержку, силы и ресурсы, необходимые им для воплощения своих идей

Как работают умные контракты

ПРИМЕР КОДА УМНОГО КОНТРАКТА НА ETHEREUM

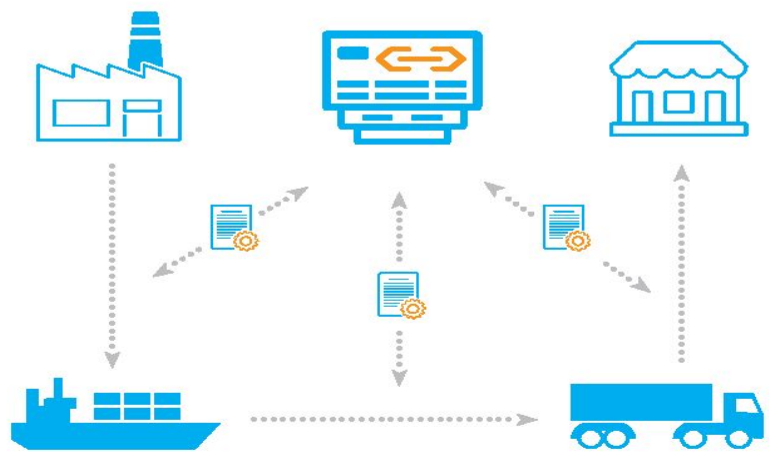
```
/* Allow another contract to spend some tokens in your behalf */
function approve(address _spender, uint256 _value)
    returns (bool success) {
    allowance[msg.sender][_spender] = _value;
    return true;
}

/* Approve and then comunicate the approved contract in a single tx */
function approveAndCall(address _spender, uint256 _value, bytes _extraData)
    returns (bool success) {
    tokenRecipient spender = tokenRecipient(_spender);
    if (approve(_spender, _value)) {
        spender.receiveApproval(msg.sender, _value, this, _extraData);
        return true;
    }
}

/* A contract attempts to get the coins */
function transferFrom(address _from, address _to, uint256 _value) returns (bool success) {
    if (balanceOf[_from] < _value) throw;                 // Check if the sender has enough
    if (balanceOf[_to] + _value < balanceOf[_to]) throw;  // Check for overflows
    if (_value > allowance[_from][msg.sender]) throw;   // Check allowance
    balanceOf[_from] -= _value;                           // Subtract from the sender
    balanceOf[_to] += _value;                             // Add the same to the recipient
    allowance[_from][msg.sender] -= _value;
    Transfer(_from, _to, _value);
    return true;
}

/* This unnamed function is called whenever someone tries to send ether to it */
function () {
    throw;     // Prevents accidental sending of ether
}
```

Государство и Бизнес:
КАНАЛЫ ПОСТАВОК

Блокчейн отслеживает движение товаров в одном распределённом реестре и обеспечивает соблюдение существующих процедур и правил.

Проблемы:

- Несвоевременные поставки;
- Корректность оформленных заказов;
- Коррупция на уровне закупок и доставок.



Результат:

Прозрачное взаимодействие с налоговой и контрольными органами;

Исключение манипуляций с отчетностью;

Беспрепятственное включение новых участников;

Минимизация коррупции;

Timestamping;

Может использоваться в ВПК, госзакупках, образовании.

Блокчейн — интернет нового тысячелетия.

«Интернет — это временная мода»
РОБЕРТ МЕТКАФ, ИЗОБРЕТАТЕЛЬ ETHERNET, INFOWORLD, 1995 ГОД

Роберт ошибся. Интернет оказался не модой для гиков, а реальностью, в которой живем все мы.

Сегодня, мир без Интернета невозможно представить.

20 лет понадобилось Интернету, чтобы завоевать мир.

**Парадоксально, но благодаря Интернету,
Блокчейн покорит мир гораздо быстрей.**

Блокчейн – будущее уже наступило.

Сегодня.

Спасибо!

gregfili@mail.ru Слынько Григорий