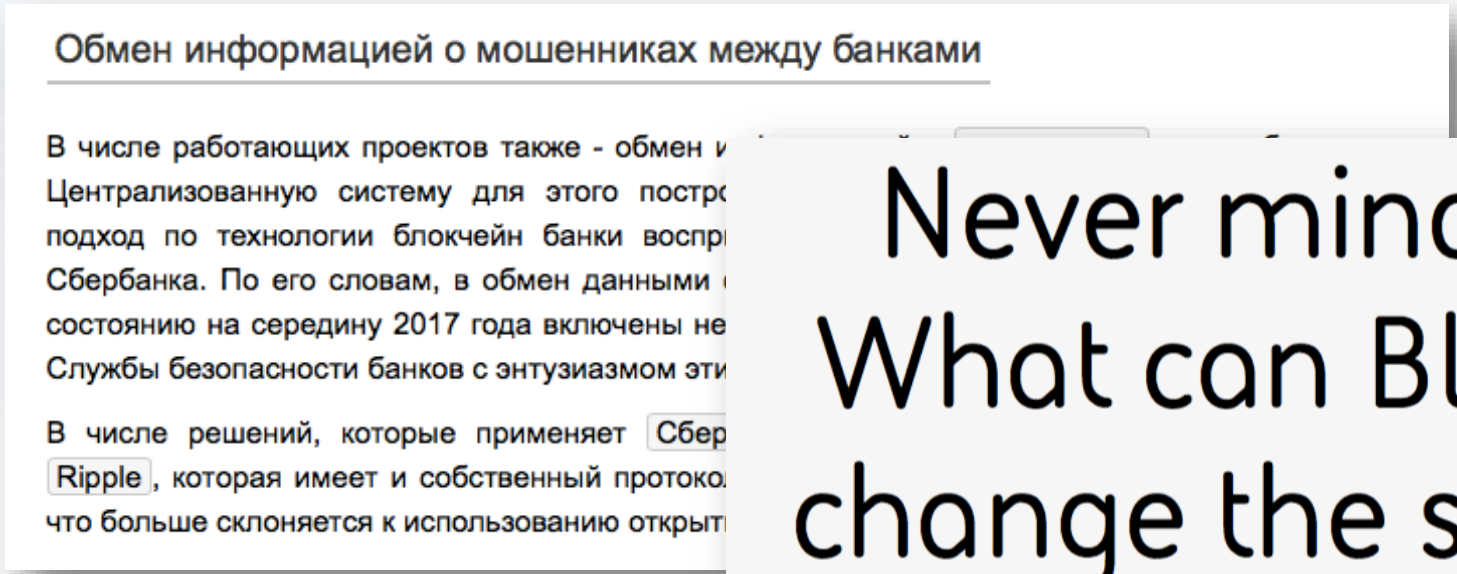
Блокчейн в деятельности SOC

Алексей Лукацкий
Бизнес-консультант по безопасности

22 ноября 2017

Как используется блокчейн в деятельности SOC?



Обмен информацией о мошенниках между банками

В числе работающих проектов также - обмен и
Централизованную систему для этого постро
подход по технологии блокчейн банки воспри
Сбербанка. По его словам, в обмен данными
состоянию на середину 2017 года включены не
Службы безопасности банков с энтузиазмом эти

В числе решений, которые применяет Сбер
Ripple, которая имеет и собственный протоко
что больше склоняется к использованию открыт

Never mind the Bitcoin - What can Blockchain do to change the shape of Threat Intelligence?

Neena Sharma, Global Head of Cyber Insights
12 July 2017

А еще можно использовать блокчейн для хранения данных об инцидентах…

cisco

Блокчейн – серебряная пуля?

What can Blockchain do for the threat intelligence sector?

Another area that is not much talked about yet, but could benefit from blockchain technology, is threat intelligence and how it is shared. Businesses are generally aware of the value of sharing threat intelligence and information on cyber attacks amongst peers and with government. But, the fear of exposure is significant. It's highly likely that a great deal of threat intelligence is left to moulder away or used in duplicate. Shared effectively, such intelligence could change the whole shape of the threat intelligence market segment. Blockchain technology allows the sharing of information in real time, anonymously and confidentially.

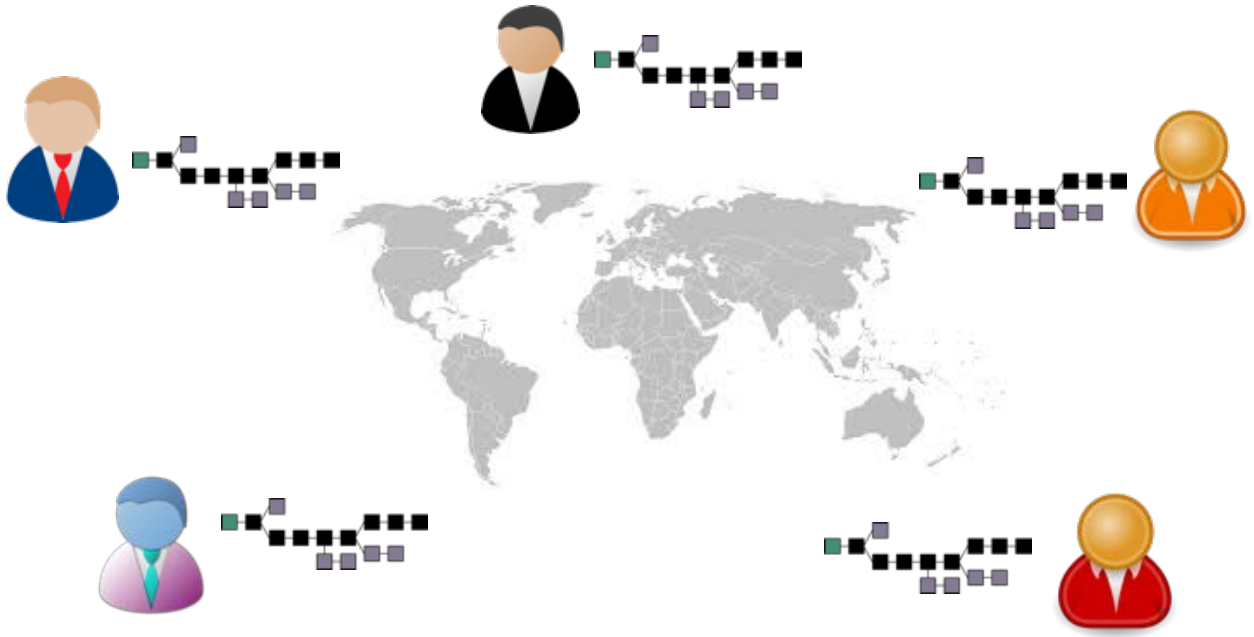
cisco

Для начала…


Должны вы использовать блокчейн?
Вы делаете криптова-люту?
Да
Нет
Пожалуйста, остановитесь
Нет

Знаем ли мы, что такое блокчейн?

Криптографически защищенная, распределенная, транзакционная база данных…

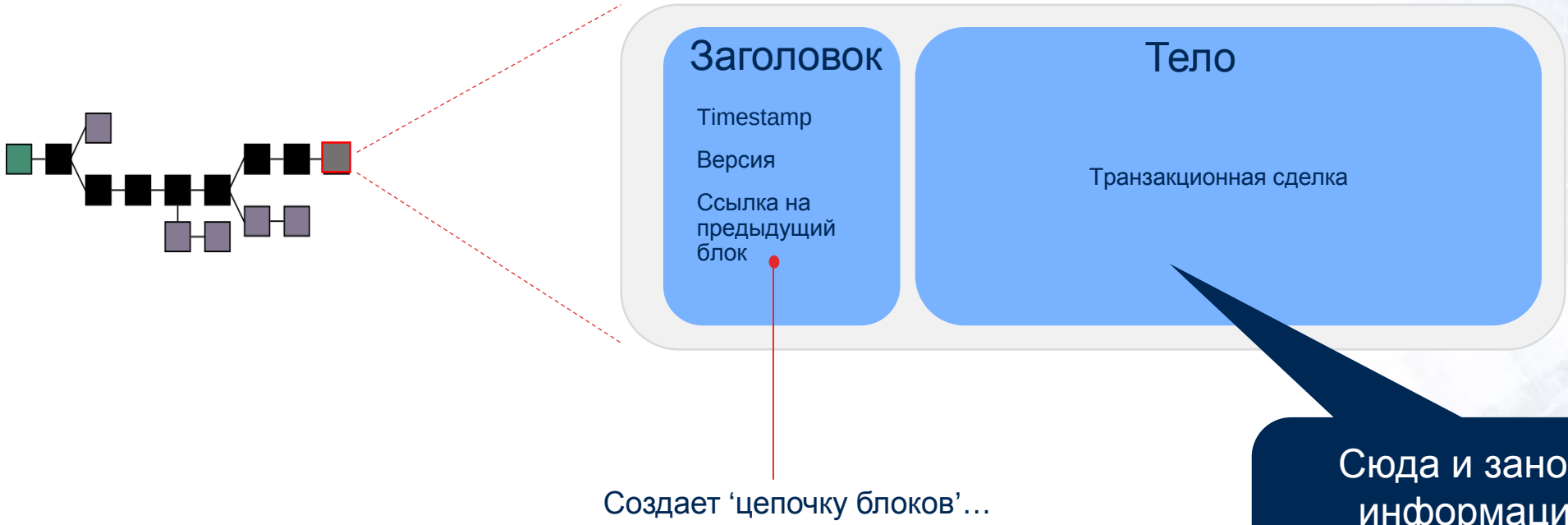


…каждый имеет копию, никто не контролирует

cisco

Как работает блокчейн…

Анатомия блокчейна



Преимущества блокчейна для ведения базы инцидентов или рассылки IoC

?!

- Независимость (каждый может вносить данные об инцидентах самостоятельно)
- Неизменяемость и контроль всех блоков (невозможность удаления данных об инцидентах)
- Контроль доступа (доступ к инцидентам имеют только те, у кого есть ключи шифрования)
- Снижение транзакционных издержек (формирование базы инцидентов происходит дешевле и доступ к ней проще)
- Скорость транзакций (формирование базы инцидентов происходит быстрее)
- Распределенность и отсутствие точки отказа (сложно уничтожить все копии баз инцидентов)
- Отсутствие посредников

cisco

А теперь задумаемся…

- При регулярном обновлении карточки инцидента вам нужна неизменность блокчейна?
- При потере актуальности IoC вам нужно его удалить и как это сделать в блокчейне?
- При закрытости информации об инцидентах вам нужна открытость блокчейна?
- При необходимости обеспечения доверия к источнику IoC вам нужна неконтролируемость участников блокчейна?

cisco

Блокчейн может быть и другим

- Блокчейн не обязан быть децентрализованным
- Блокчейн не обязан быть открытым (а для базы инцидентов он и не должен быть таковым)
- Блокчейн не обязан быть построен на криптографии

cisco

Типы блокчейна

Любой (даже недоверенный участник) может отправить данные в блокчейн, которые никто не проверяет

За поддержание открытого блокчейна подразумевается награда (мотивация) «майнерам»

Открытый публичный

Транзакции никем не контролируются и их формирование осуществляется в свободном порядке

Закрытый частный

Все транзакции отслеживаются и контролируются центральным органом (ЦБ, Сбербанк, ФСБ…)

Закрытый публичный (консорциум)

Согласование транзакций происходит среди избранных участников консорциума (финансовая отрасль, КИИ…)

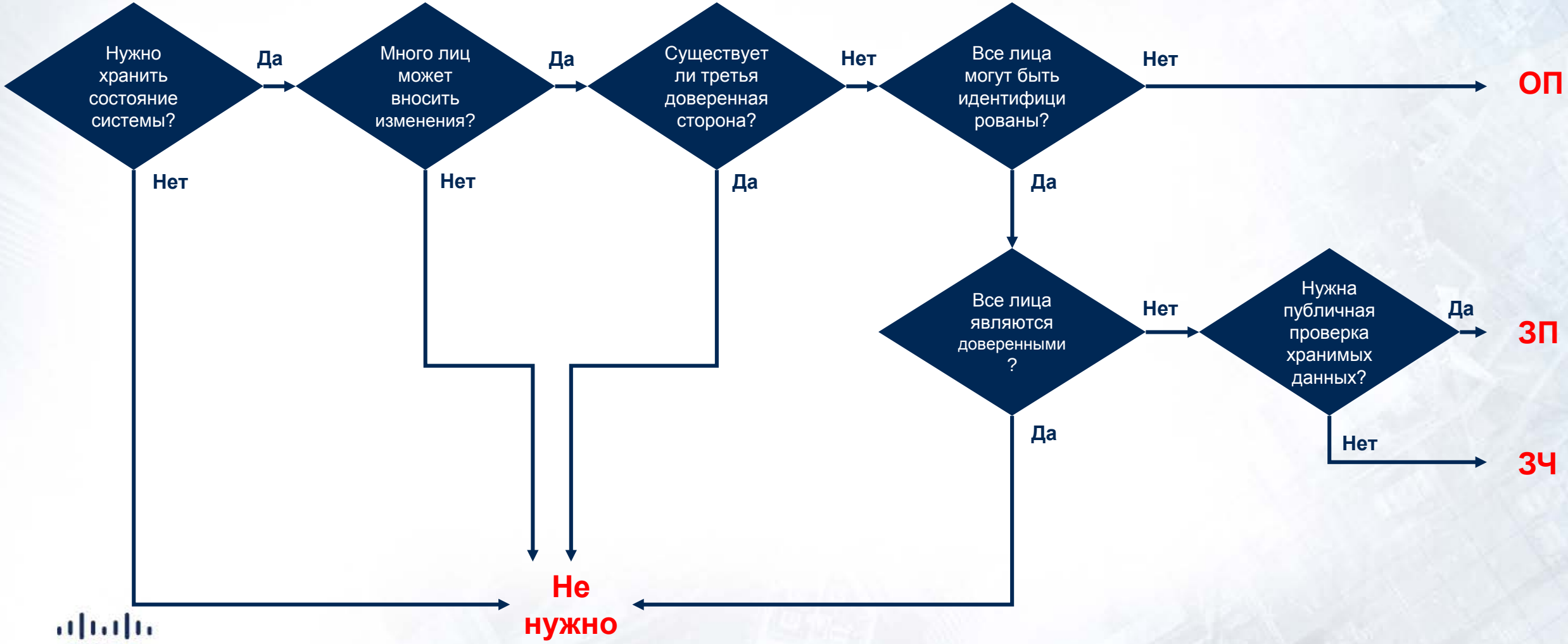
Может проще без блокчейна?

cisco

Сравнение разных типов баз данных

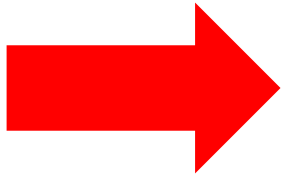
	Централизованная БД	Распределенная БД	Открытый блокчейн	Закрытый блокчейн
Хранилище	Единый экземпляр	Множество копий		
Определение данных	Многомерное		Специализированное одномерное, например, для права собственности или суммы	
Участие	**Закрытое**		Открытое, Новые участники добавляются сами	**Открытое. Новые участники добавляются по согласованию**
Права / полномочия	Управляется отдельной СУБД		Встроены в протокол	Файл конфигурации определяет права всех участников
Проверка данных			Использование PoW или иных весовых схем голосования, например, PoS	Обычно базируется на подтверждении ключевых участников
Сверка данных	Необходимо только при переносе данных	Итерационно, не зависит от доступности		
Надежность	Уязвима к отказу сервера	Надежна, продолжает обновляться даже при частичной доступности участников		

От чего зависит выбор типа блокчейна?



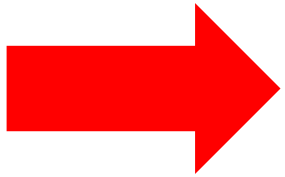
…то есть

Все равны, посторонних быть не должно



Закрытый публичный блокчейн

Есть центральный орган контроля/надзора



Блокчейн не нужен!

cisco

Но нормативные акты в России сегодня подразумевают централизацию

- По одному из законопроектов Банк России обязан вести базу инцидентов
- По одному из законопроектов именно Банк России будет распространять признаки мошеннических действий
- По 382-П/552-П финансовые организации обязаны уведомлять ФинЦЕРТ об инцидентах
- По 187-ФЗ субъекты КИИ обязаны уведомлять об инцидентах ГосСОПКУ
- По 187-ФЗ НКЦКИ будет распространять IoC

cisco

На текущем этапе развития технологий и законодательства блокчейн в деятельности SOC не дает никаких преимуществ!

Спасибо!

alukatsk@cisco.com