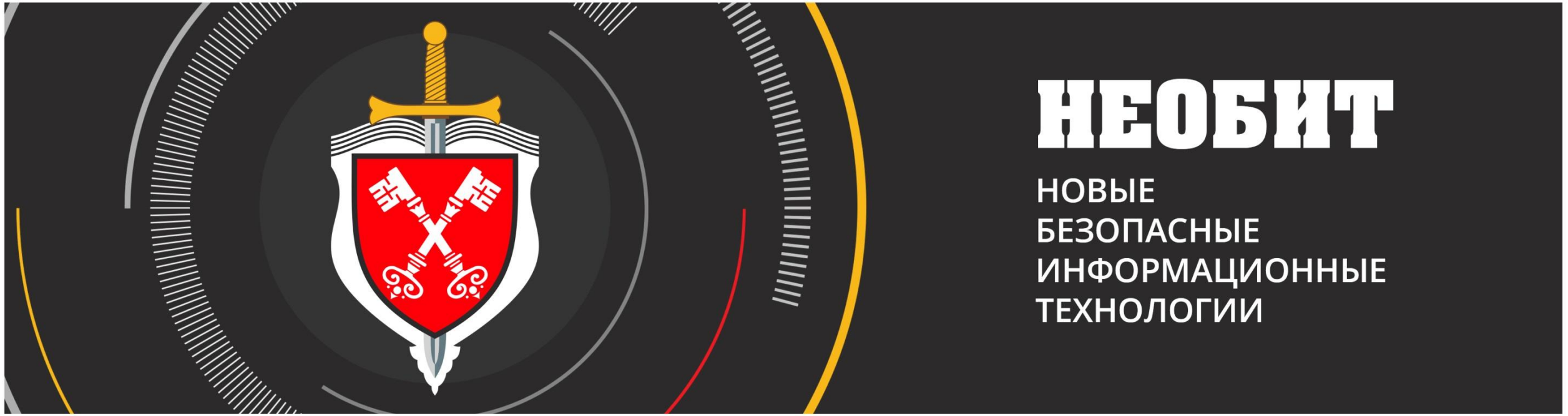
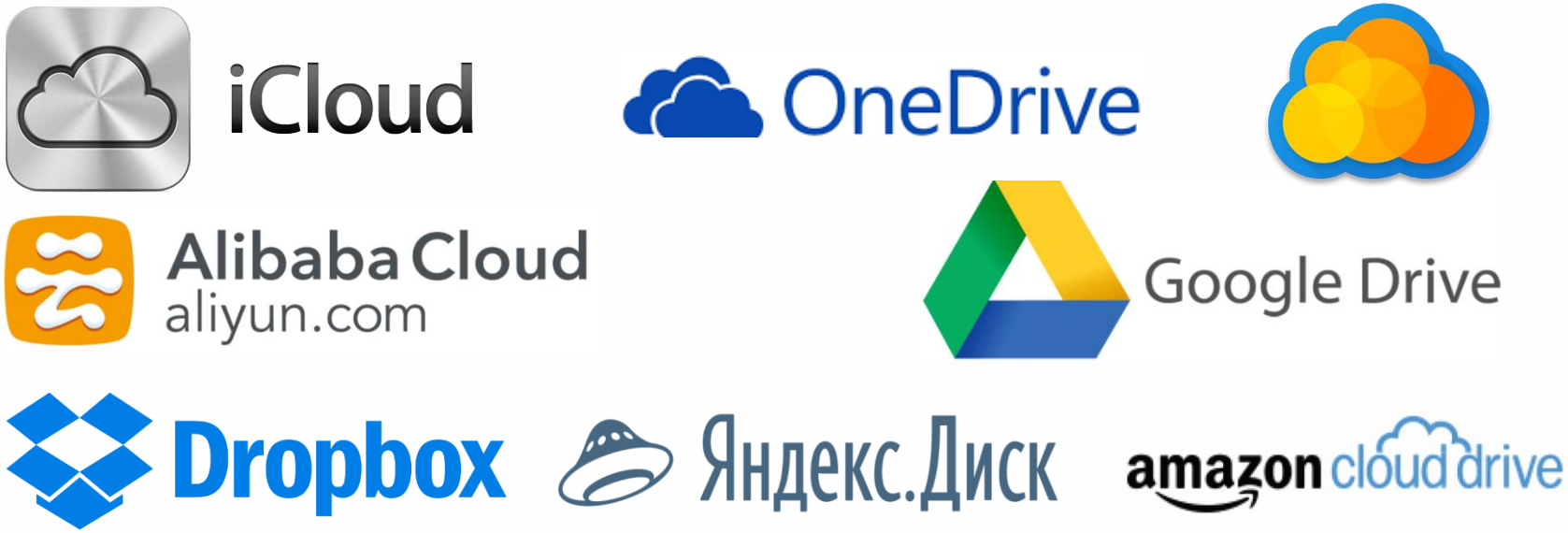


Обеспечение безопасности в распределенных системах хранения и обработки данных на основе технологии blockchain

Мясников Алексей, РусКрипто - 2018

Сервисы облачного хранения данных

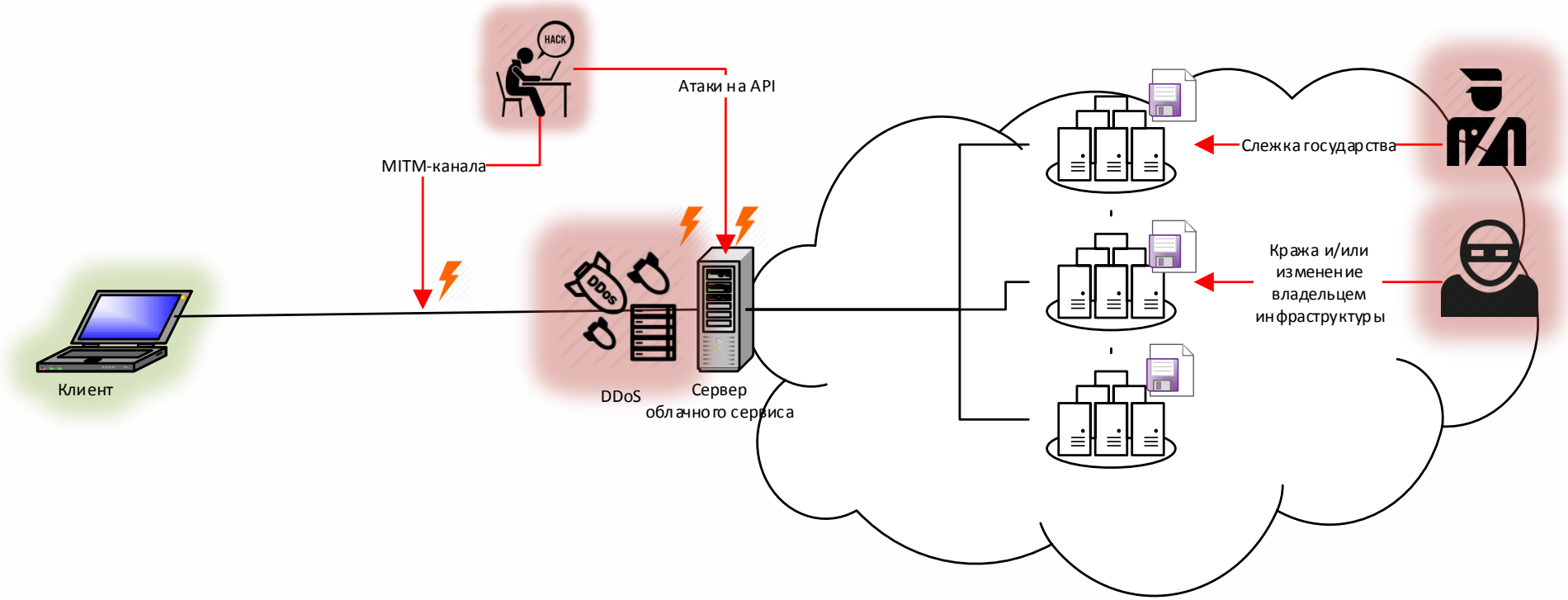


- Присутствие «точек отказа»
- Отсутствие доверия к среде

- 2013 г. – 1 млрд. аккаунтов, 685 Мб на аккаунт
- 2018 г. – 3,61 млрд. аккаунтов, 975 Мб на аккаунт

*По данным ABI

Угрозы безопасности централизованных облачных сервисов

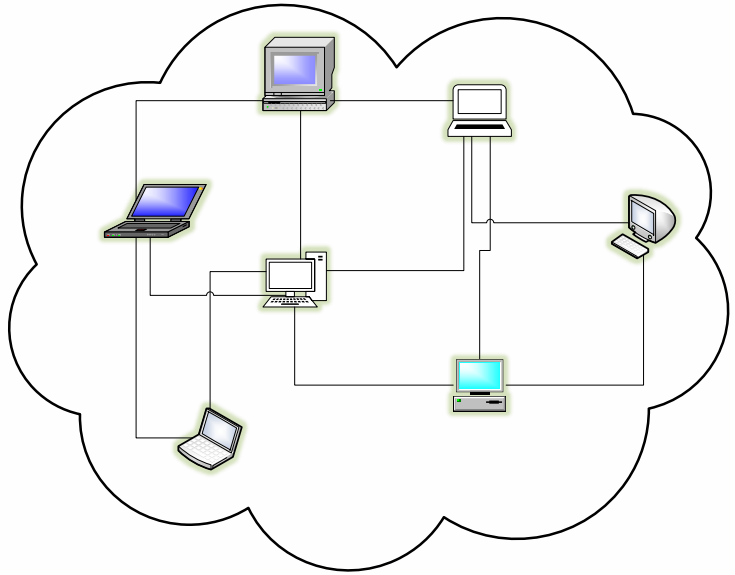


Угрозы безопасности централизованных облачных сервисов

Конфиденциальность	• Ошибки в реализации API-доступа к облаку • Кража данных, сбор метаданных владельцем облака
Целостность	• MITM между клиентским ПО и облаком • Изменение данных владельцем облака
Доступность	• DDOS-атаки на поставщика облачных услуг • Расположение серверов в одной географической локации

Концепция децентрализованного облачного хранилища

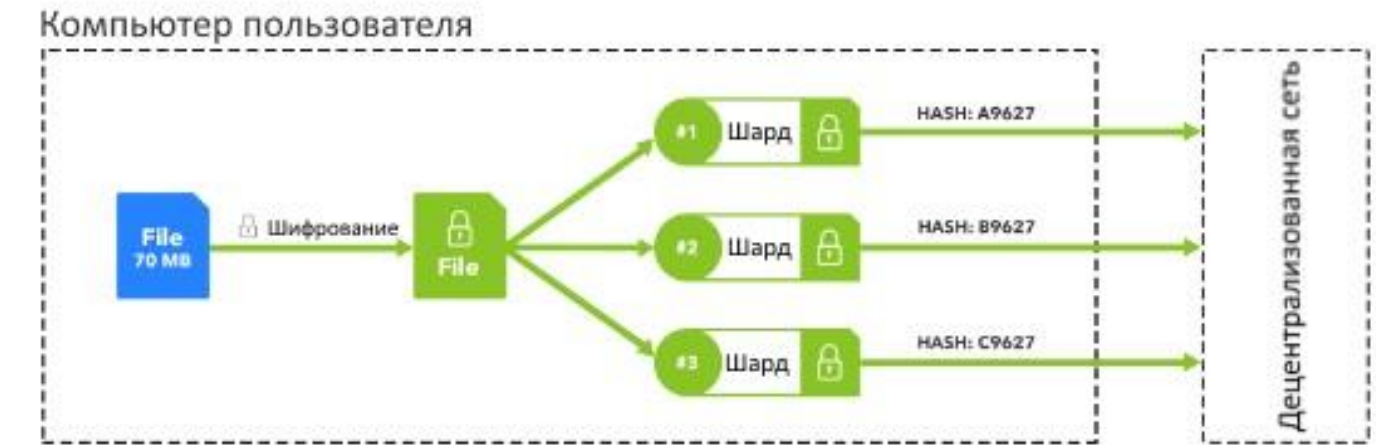
- Отсутствие центральных серверов
- Блокчейн для хранения информации о взаимоотношениях между узлами
- Каждый хост сети может выступать в роли клиента и поставщика для хранения ресурсов
- Гетерогенная инфраструктура (клиенты под различные ОС и аппаратную платформу)



1. Узлам нельзя доверять
2. Узлы не предоставляют услуги бесплатно
3. Узлы могут быть не всегда доступны
4. Сети нельзя доверять

Механизмы обеспечения безопасности

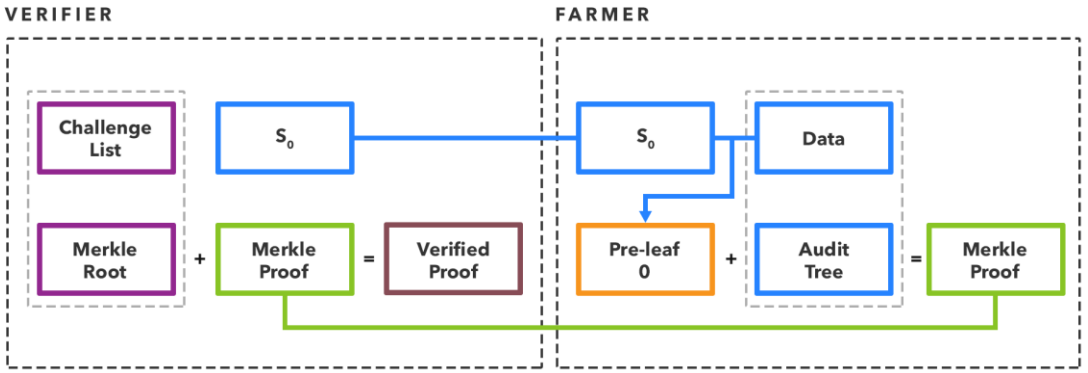
Шифрование пользовательских данных

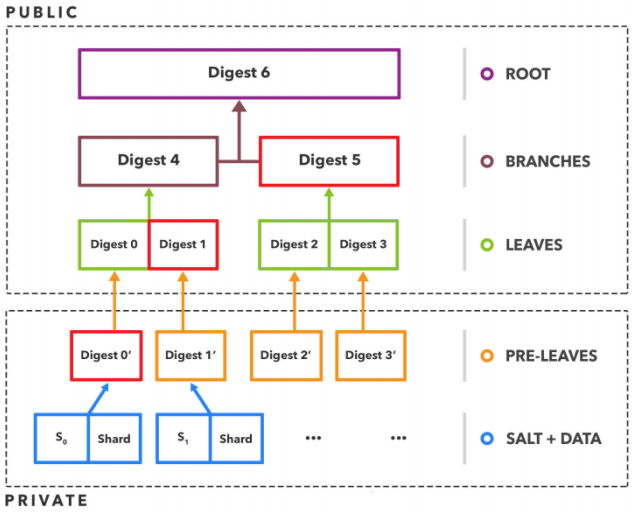


- Шифрование файла
- Разбиение файла на фрагменты
- Выгрузка каждого фрагмента на узлы-хранилища в децентрализованной сети
- Пользователь контролирует избыточность, размер фрагментов, географическое положение, технические характеристики узла

Аудит доступности файлов

- Proof-of-Retrievability
- Через определенные промежутки времени происходит процедура аудита
- Аудит может быть полным или частичным
- После каждой процедуры-аудита узлу, хранящему файл, начисляется вознаграждение за работу





Умные контракты

- «Умный контракты» – структура данных, описывающая взаимодействие владельца файла и хранящего узла
- «Умный контракт» содержит информацию, необходимую для взаимодействия сторон:
  - Хэш зашифрованного фрагмента файла
  - Размер фрагмента файла
  - Стратегия аудита
  - Информация о вознаграждении для хранящего узла
- Умный контракт хранится у обеих сторон, а так же в сторонней БД на базе блокчейна

Схемы резервирования данных

Резервирование данных	Количество фрагментов каждой части файла задаётся пользователем
	Применение избыточного кодирования для восстановления потерянных блоков

$$\Pr_{failure}(n;k,p) = \sum_{i=0}^{k-1} p^i (1-p)^{n-i} \binom{n}{i}$$

n	k	p	$\Pr_{failure}(n,k,p)$
18	6	0.5	4.812e-02
18	6	0.75	3.424e-05
18	6	0.9	5.266e-10
18	6	0.98	6.391e-19
36	12	0.5	1.440e-02
36	12	0.75	2.615e-08
36	12	0.9	1.977e-17
36	12	0.98	1.628e-34

Расчет вероятности неудачного восстановления данных при использовании *k-n* кодирования Рида-Соломона при вероятности *p* сохранения узла в сети

Атаки на хранилища

Атака	Описание	Защита
Spartacus	Подделка идентичности узла	Использование в качестве адреса узла открытого ключа, таким образом поддельный узел не имеет возможности подписи сообщений
Sybil/Google	Создание множества зловредных узлов с целью деградации производительности сети	Наращивание мощности сети. Механизмы изоляции зловредных узлов.
Eclipse	Изоляция легитимного узла, путем создания группы близких к нашему зловредных узлов	Наращивание мощности сети. В больших распределенных сетях такая атака сложноосуществима.
Hostage Bytes	Отказ хранящего узла в передаче своего фрагмента файла с целью поулчения дополнительных выплат от владельца файла	Использование резервных узлов, введение рейтинговых систем для узлов.
Cheating owner	Отказ владельца файла оплачивать контракт хранящего узла	Введение рейтинговых систем для клиентов.
Defeated Audit Attacks	Атака на процесс аудита доступности файла	Хранение дополнительных метаданных для проверки подлинности произведенного аудита

Сравнительная таблица угроз безопасности облачных хранилищ

	Централизованные	Децентрализованные
Ошибки программной реализации	+	+
MITM	+	Не имеет смысла
Манипуляции над данными владельцем инфраструктуры	+	-
Угрозы атак отказа в обслуживании	+	+/-
Угрозы характерные для децентрализованных сетей	-	+

Преимущества децентрализованной архитектуры

- Отсутствие центральных серверов
- Безопасное хранение файлов (Фрагментация, шифрование на стороне пользователя, распределение по сети)
- Анонимность (Все, что известно о пользователе – его открытый ключ)
- Самоаутентификация, ключи шифрования файлов не передаются по сети
- Контроль за географическим положением файлов
- Архитектура системы поощряет «честные» отношения между узлами
- Гетерогенная среда позволяет избежать сбоев одного рода, как в среде передачи, так и на узлах хранения

Существующие децентрализованные облачные решения

Прогнозы развития децентрализованных хранилищ

- Рост количества узлов – повышение стабильности децентрализованных сетей
- Развитие алгоритмов децентрализованного взаимодействия повышает масштабируемость и устойчивость сетей
- Переход от идеи облачных хранилищ к полноценной облачной инфраструктуре с предоставлением вычислительных ресурсов и возможностью размещения приложений.

Размещение приложений
в децентрализованной сети

Спасибо за внимание!

Мясников Алексей
ООО «НеоБИТ»
Специалист по ИБ
myasnikov@neobit.ru

НЕОБИТ

Адрес: 195220 Санкт-Петербург, ул. Гжатская, д. 21, "Г"

Телефон: 535-88-67
Сайт: www.neobit.ru / www.необит.рф