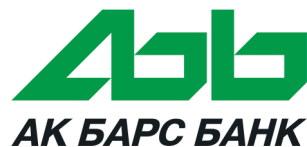


Анкеты КҮС для межбанковского взаимодействия



Проблема

- Кредитная организация обязана удовлетворять 115 ФЗ
- При взаимодействии банки обмениваются КҮС-анкетами
 - Наименование, координаты, структура капитала, акционеры, управление, меры по противодействию отмыванию денег и терроризму
- Бумажный обмен при каждом обновлении данных
 - Медленно
 - Трудоёмко

Решение: межбанковский КҮС реестр

Интуиция:

- Распространение информации по схеме «издатель-подписчик»
- В первом приближении, банк – это ключ
- Версия анкеты и версия прав доступа – разные вещи
- Анкету можно хранить где угодно
- Нельзя развидеть уже увиденное

Схема хранения

Слои:

1. Блокчейн как единая точка доступа
2. Swarm как хранилище прав доступа
 - Чтобы не загружать собственно блокчейн
3. HTTP/Swarm как хранилище документа

Ключи

- Ka – (асим) ключ банка-издателя информации
- Kb – (асим) ключ банка-подписчика информации
- Kd – (сим) ключ документа

Схема процесса

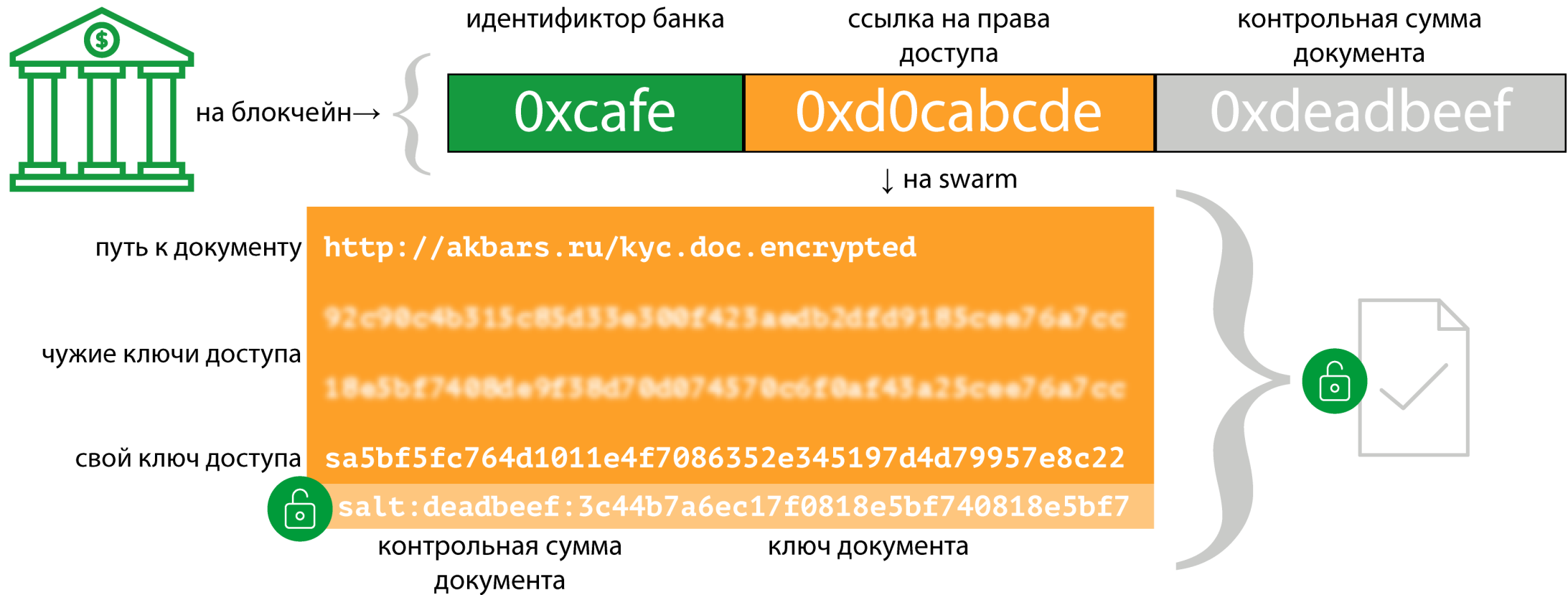


Схема процесса

1. Шифруем документ Kd,
публикуем



на блокчейн →

идентификтор банка

0xcafe

ссылка на права
доступа

0xd0cabcd

контрольная сумма
документа

0xdeadbeef

↓ на swarm

путь к документу

http://akbars.ru/kyc.doc.encrypted

чужие ключи доступа

92c90c4b315c85d33e3b01427a4001d9185cee76a7cc
18e5bf7408de9e38d70d074570c6f0af43a25cee76a7cc

свой ключ доступа

sa5bf5fc764d1011e4f7086352e345197d4d79957e8c22



salt:deadbeef:3c44b7a6ec17f0818e5bf740818e5bf7

контрольная сумма
документа

ключ документа



Схема процесса

2. Сохраняем права доступа на Swarm: Kd, зашифрованный Kb

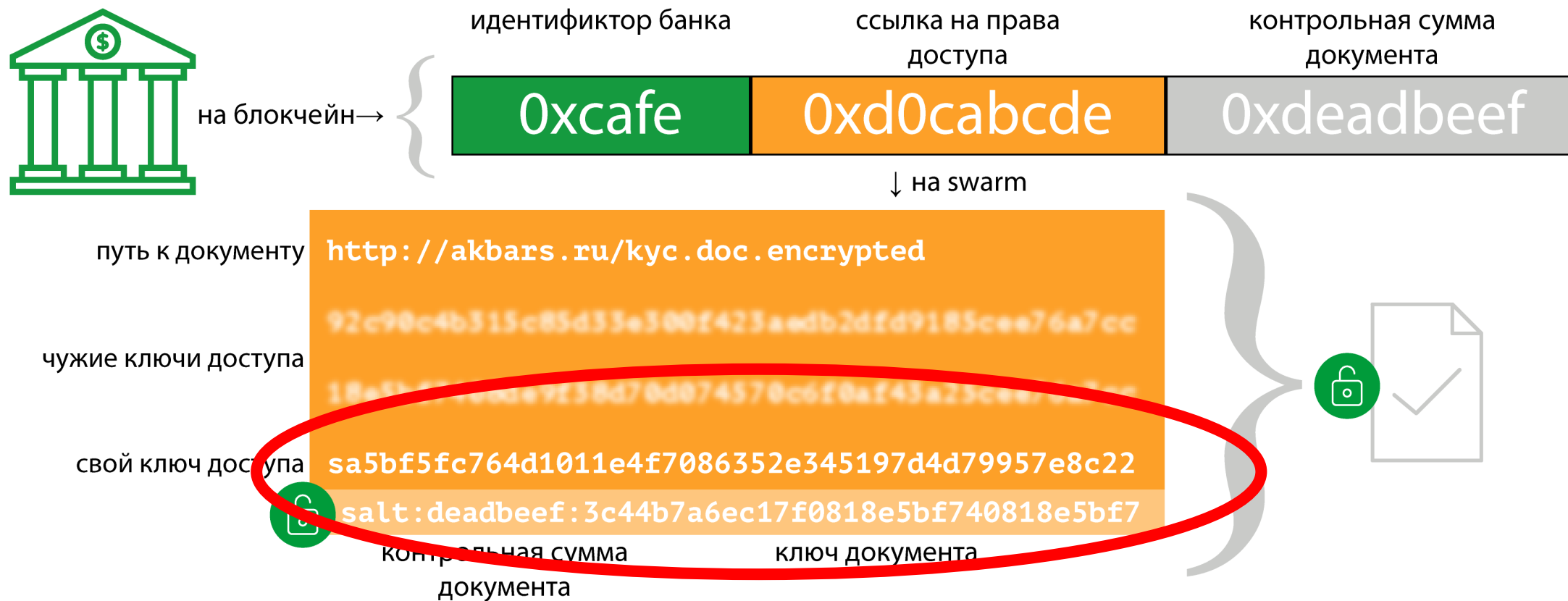


Схема процесса

3. Публикуем метаданные на блокчейн



на блокчейн →

идентификтор банка

ссылка на права
доступа

контрольная сумма
документа

0xcafe

0xd0cabcd

0xdeadbeef

↓ на swarm

путь к документу

<http://akbars.ru/kyc.doc.encrypted>

чужие ключи доступа

92c90c4b315c85d33e300f423aedb2dfd9185cee76a7cc
18e5bf7408de9f38d70d074570c6f0af43a25cee76a7cc

свой ключ доступа

sa5bf5fc764d1011e4f7086352e345197d4d79957e8c22



salt:deadbeef:3c44b7a6ec17f0818e5bf740818e5bf7

контрольная сумма
документа

ключ документа



Схема процесса

4. Подписчик смотрит на строку интересующего банка

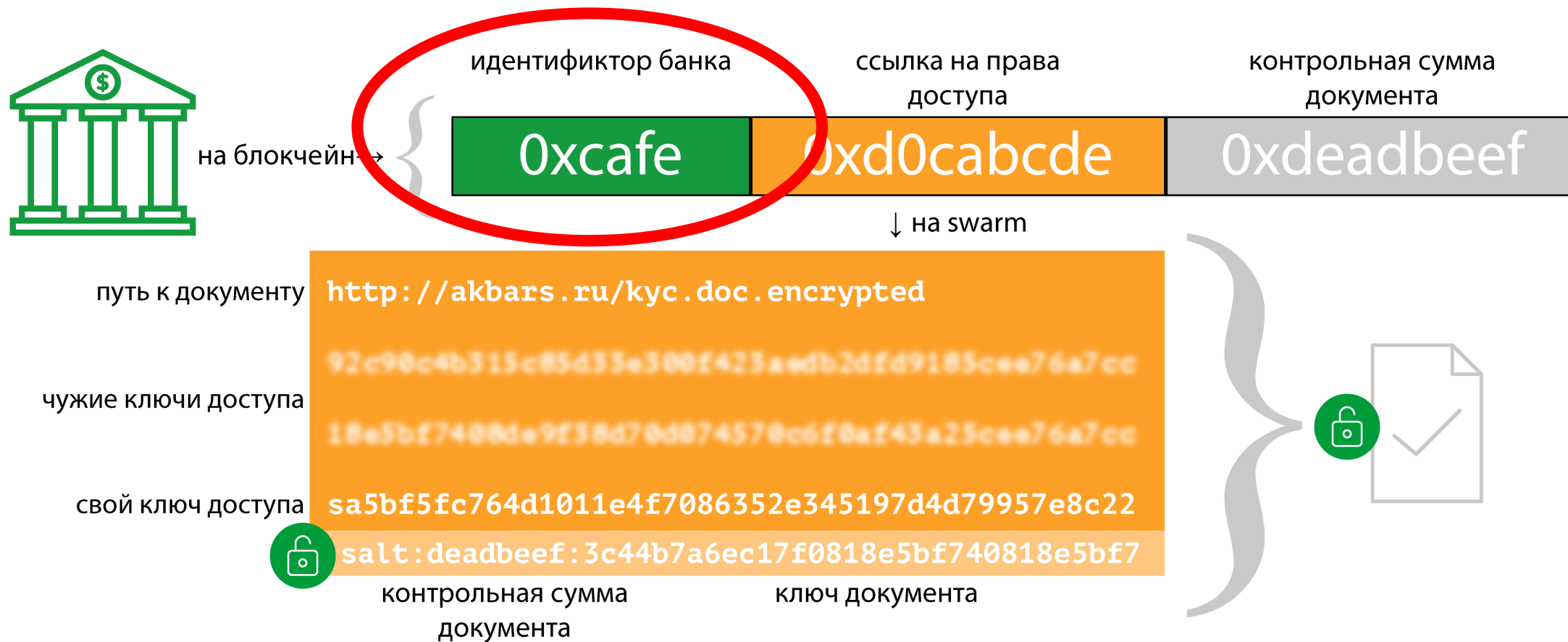


Схема процесса

5. Подписчик открывает права доступа со Swarm

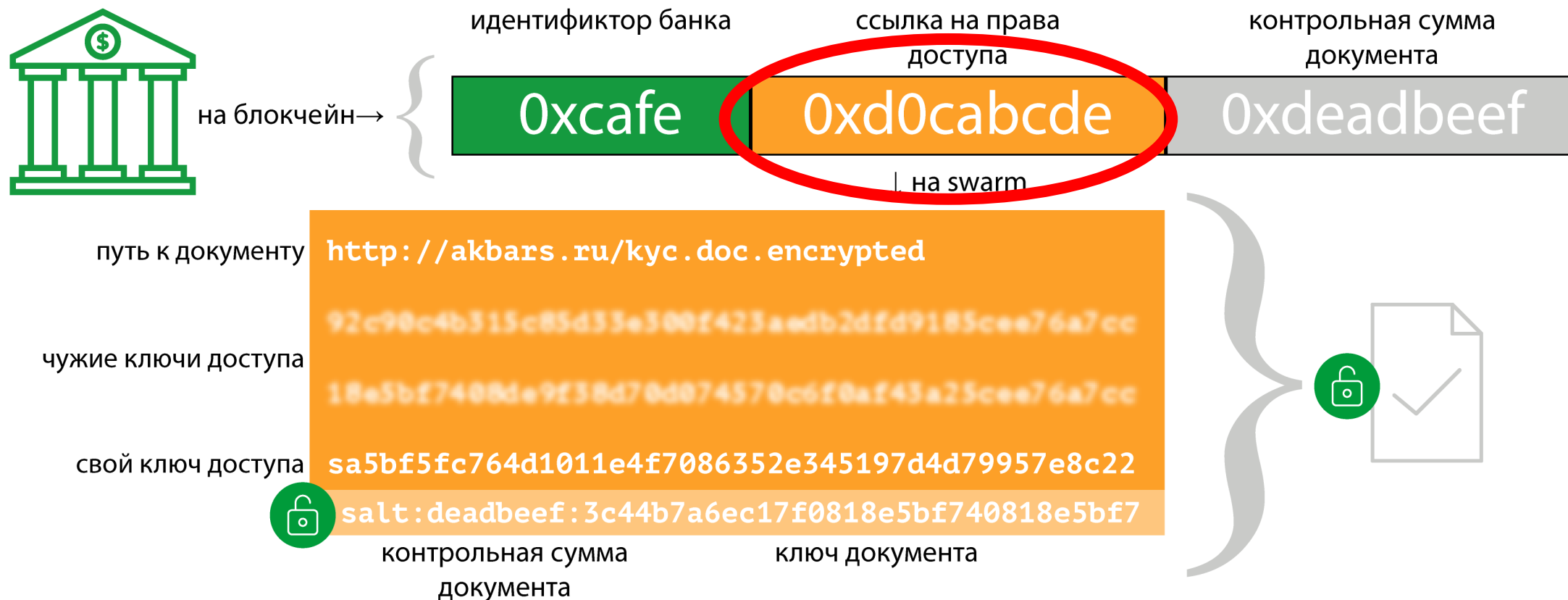


Схема процесса

6. Пытается расшифровать своим ключом Kb записи

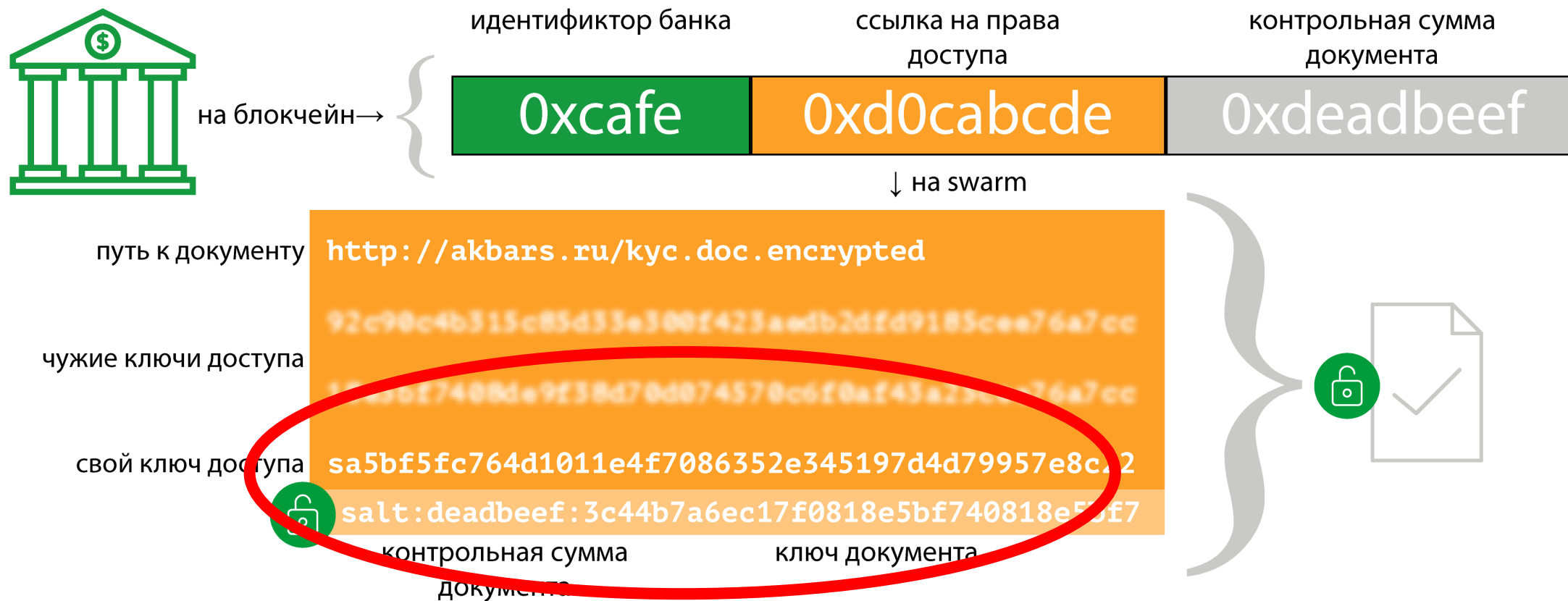


Схема процесса

7. Находит свою расшифрованную запись стандартного формата

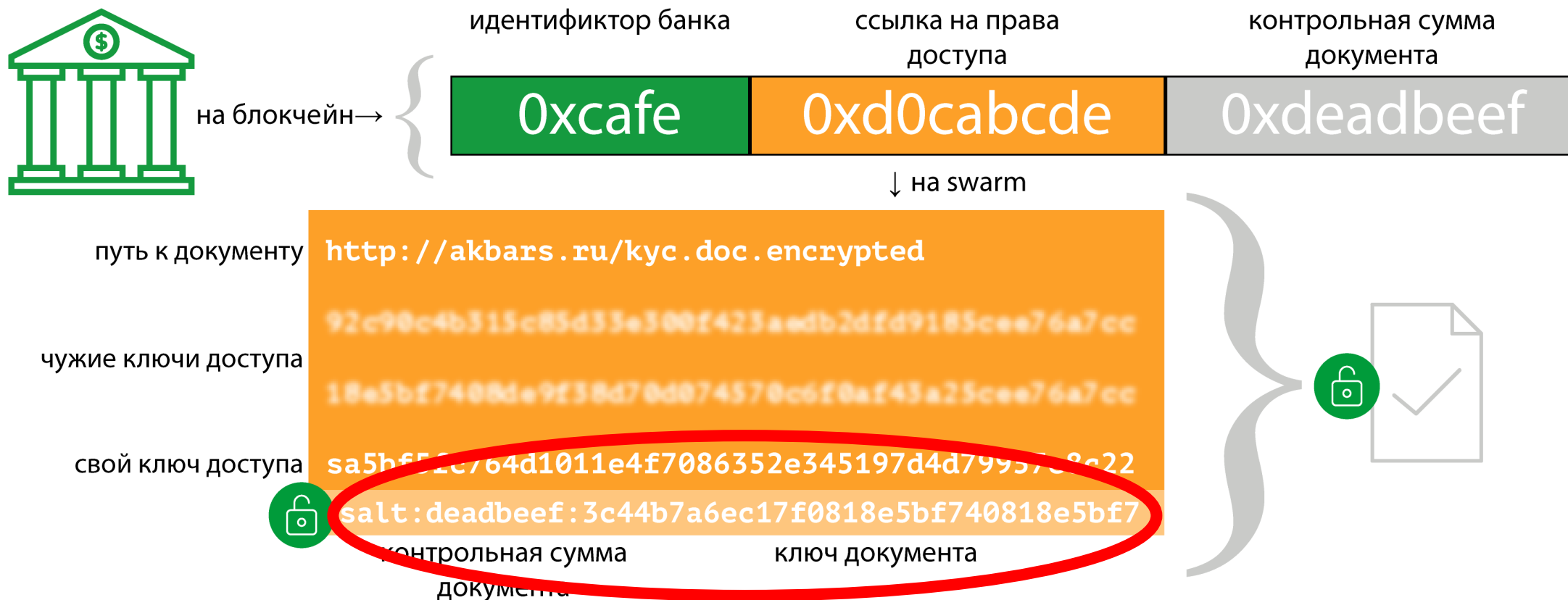


Схема процесса

8. Скачивает документ,
расшифровывает его найденным
ключом документа Kd



на блокчейн →

идентификтор банка

0xcafe

ссылка на права
доступа

0xd0cabcd

контрольная сумма
документа

0xdeadbeef

↓ на swarm

путь к документу

<http://akbars.ru/kyc.doc.encrypted>

чужие ключи доступа

92c90c4b315c85d33e300f423aedb2dfd9185cee76a7cc
18e5bf7408de9f38d70d074570c6f0af43a25cee76a7cc

свой ключ доступа

sa5bf5fc764d1011e4f7086352e345197d4d79957e8c22



salt:deadbeef:3c44b7a6ec17f0818e5bf740818e5bf7

контрольная сумма
документа

ключ документа



Схема процесса

9. Следит за обновлениями в блокчейне. Видны обновления в документе и в правах доступа.



на блокчейн →

идентификтор банка

0xcafe

ссылка на права
доступа

0xd0cabcd

контрольная сумма
документа

0xdeadbeef

↓ на swapp

путь к документу

<http://akbars.ru/kyc.doc.encrypted>

чужие ключи доступа

92c90c4b315c85d33e300f423aedb2dfd9185cee76a7cc
18e5bf7408de9f38d70d074570c6f0af43a25cee76a7cc

свой ключ доступа

sa5bf5fc764d1011e4f7086352e345197d4d79957e8c22



salt:deadbeef:3c44b7a6ec17f0818e5bf740818e5bf7

контрольная сумма
документа

ключ документа



Ожидаемые результаты пилота

- Сокращение времени на ведение КҮС-анкеты на 20% - 40%
 - Оформление индивидуальных писем
 - Пересылка бумажных экземпляров
 - Напоминания о грядущих обновлениях

Открытые вопросы

- Как мы можем приблизиться к юридически значимому обмену карточками КҮС?