О БЛОКЧЕЙН ПЛАТФОРМЕ ДЛЯ ЭЛЕКТРОННЫХ ДЕНЕГ ГОСУДАРСТВА С ПРИМЕНЕНИЕМ ОТЕЧЕСТВЕННОЙ КРИПТОГРАФИИ

КОМИСАРЕНКО В.В.
ДИРЕКТОР ПО РАЗВИТИЮ ЗАО «БЕЛТИМ СБ»
ДИРЕКТОР АССОЦИАЦИИ «РУСКРИПТО»

Общие свойства денег

1. Приемлемость
2. Стабильность стоимости
3. Экономичность
4. Продолжительность использования
5. Однородность
6. Делимость
7. Портативность

Материал или товар, из которого изготавливаются деньги, обычно обладает рядом свойств:

1. Качественная однородность (отдельные экземпляры товара, монеты, купюры не должны обладать уникальными свойствами)
2. Делимость и объединяемость (свойство размена, деньги не должны существенно менять свои свойства, если их делить на мелкие части или объединять в одну крупную часть)
3. Сохраняемость (деньги должны хорошо храниться, не изменяя своих физических и/или химических свойств на протяжении долгого времени)
4. Портативность (высокая стоимость, заключённая в небольших объёме и массе)
5. Узнаваемость (можно легко и быстро определить, что это за предмет)
6. Безопасность (защищённость от хищения, подделки, изменения номинала и т. п.).

Аналогия с документами. Общее понятие документа

Документ - это зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

Названные признаки документа предполагают:

1. **Наличие информации, смыслового содержания**
2. **Стабильную вещественную (материальную) форму, обеспечивающую долговременное использование и хранение документа**
3. **Функциональную предназначенность для передачи информации в пространстве и времени, т.е. для использования в социальных коммуникационных каналах.**

Аналогия с документами. Носители документов

1. Бумага
2. Электронный
3. Камень, краской на асфальте (?)
4. …

Формы представления денег

1. металлы
2. бумага
3. электронные
4. …

Экономика

За проведение электронных платежных инструкций юридические лица Российской Федерации платят банковской системе не менее двух миллиардов долларов в год, в Республике Беларусь – порядка двухсот миллионов долларов в год. Погрешность 25% не критична для начала размышлений

Что происходит с блокчейн и криптовалютами

1. Мода
2. Мода проходит, наступает разочарование
3. Возьмем из этого лучшие идеи
4. Блокчейн и смарт-контракты

Основные функциональные требования

1. ЕД перечисляются от лица лицу
2. Для использования ЕД не нужно открывать счет в банке
3. ЕД лежат у лица в ЕК в электронном виде
4. Изменить сумму в ЕК можно только путем получения или снятия ЕД (только путем совершения легальных транзакций)
5. Должна быть исключения возможность «двойной траты». Если сумма ЕД переведена со счета, то она должна списаться с ЕК отправителя и поступить в ЕК получателя.

Эмиссия и обмен

1. ЕД эмитирует только главный банк государства (взамен на наличные или безналичные) со своей ЕК
2. ЕД могут обмениваться на наличные или безналичные (за плату за эту услугу)
3. Курс ЕД к национальной валюте один к одному, неизменный.

Экономические требования

1. Стоимость транзакции равна 0,05 долларов
2. Если сумма транзакции меньше 0,05 доллара, то стоимость транзакции равна 0,01 доллара
3. Стоимость транзакций может меняться в соответствии с утверждаемым тарифом эксплуатирующей систему организации.

Требования по надзору

1. Должна быть реализована возможность просмотра необходимых транзакций (по регламенту доступа, через эксплуатирующую организацию) только авторизованным пользователям (контролирующим органам)
2. Информация о транзакциях должна быть доступна в течении не менее 70 лет.

Эксплуатация

1. **Процессинг системы осуществляет организация, определенная государством.**

Защита информации

1. Сложность взлома системы должна быть не ниже сложности взлома используемого алгоритма электронной подписи, включая хэширование.
2. Система защиты должна быть аттестована в соответствии с законодательством.
3. Система должна быть защищена от атак.
4. Основные атаки:
   - наполнение ЕК деньгами, без применения легальных транзакций;
   - перевод ЕД с чужой ЕК в свою;
   - хищение ЕК;
   - нелегальное (скрытое) использование ЕК;
   - уничтожение данных всей системы ЕД (уничтожить историю);
   - отказ в обслуживании.

Элементы технологии

1. Для перевода ЕД нужно владеть ключом ЕК
2. Для получения ЕД нужно передать отправителю идентификатор своего ЕК (на основе открытого ключа проверки подписи)
3. Система работает на основе приватного блокчейна
4. Система должна предусматривать возможность смены криптографических алгоритмов
5. Гарантированное уничтожение ЕК
6. Блокировка при хищении ЕК
7. Сервис депонирования ЕК
8. Сервис сохранения ЕД при случайной утере ЕК
9. Идентификация лиц через государственную систему удостоверяющих центров.

О БЛОКЧЕЙН ПЛАТФОРМЕ ДЛЯ ЭЛЕКТРОННЫХ ДЕНЕГ ГОСУДАРСТВА С ПРИМЕНЕНИЕМ ОТЕЧЕСТВЕННОЙ КРИПТОГРАФИИ

КОМИСАРЕНКО В.В.
ДИРЕКТОР ПО РАЗВИТИЮ ЗАО «БЕЛТИМ СБ»
ДИРЕКТОР АССОЦИАЦИИ «РУСКРИПТО»