Privacy in Distributed Ledger Systems: Cryptographic Mechanisms

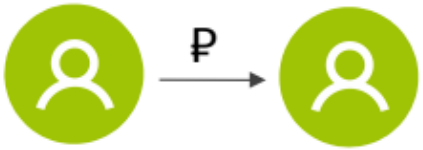
Криптографические механизмы обеспечения анонимности и конфиденциальности в системах распределенного реестра

Сергей Кяжин
к.ф.-м.н.
Лаборатория блокчейн, Сбербанк России

CTCrypt 2020

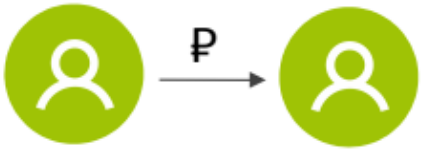
Sberbank Blockchain Laboratory

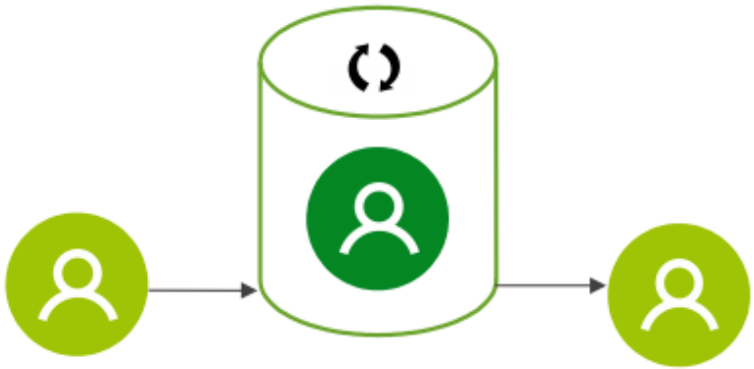
Пример задачи — электронные платежи



Sberbank
Blockchain
Laboratory

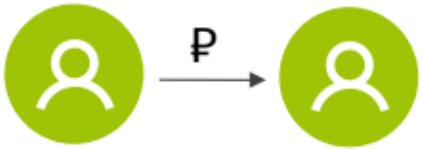
Пример задачи — электронные платежи

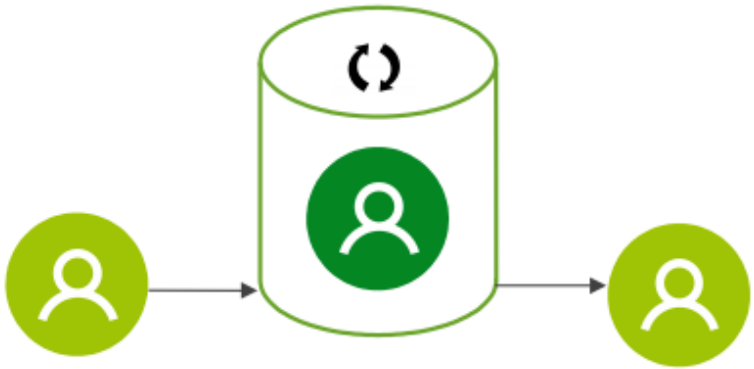




Sberbank
Blockchain
Laboratory

Пример задачи — электронные платежи

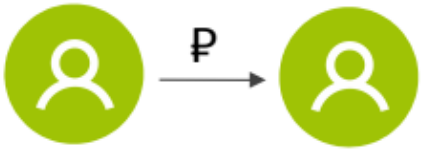


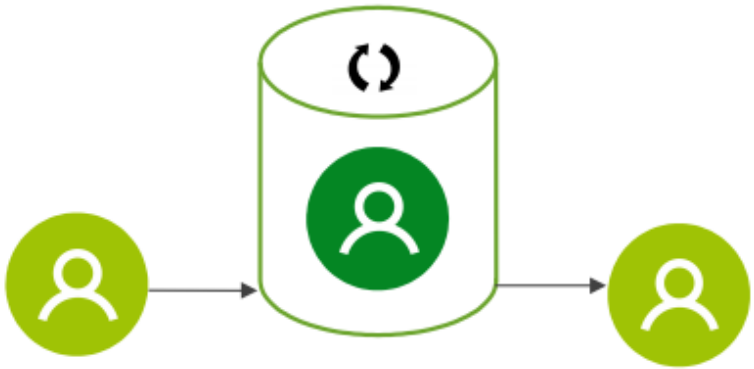


Пользователи вынуждены доверять
электронной платежной системе
и ее оператору

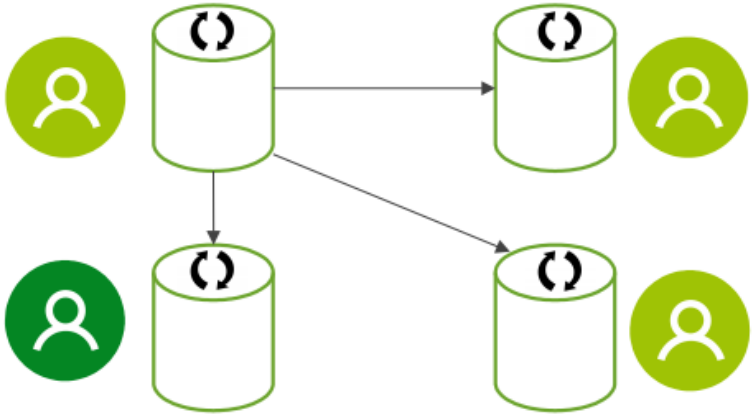
Sberbank
Blockchain
Laboratory

Пример задачи — электронные платежи





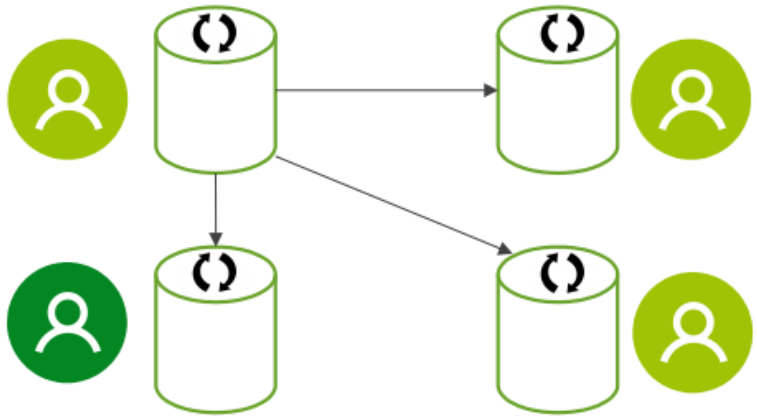
Пользователи вынуждены доверять электронной платежной системе и ее оператору



Децентрализованная система

Sberbank Blockchain Laboratory

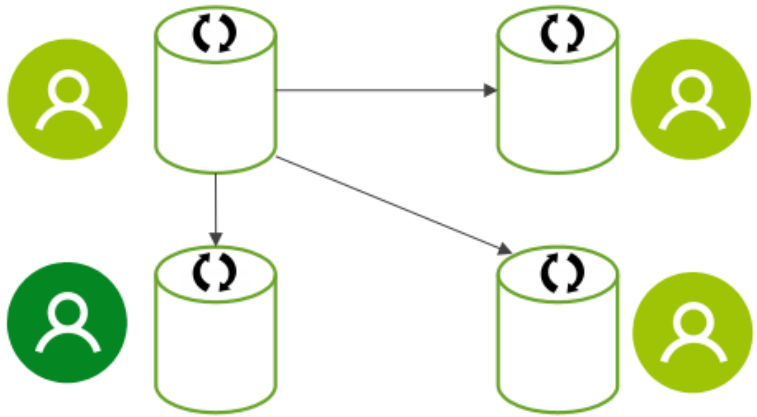
Децентрализованная система



Множество всех узлов сети

Sberbank
Blockchain
Laboratory

Децентрализованная система

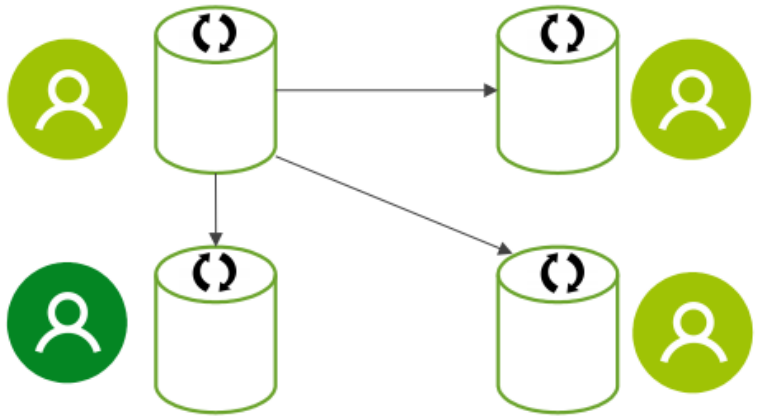


Множество всех узлов сети

- непустое подмножество узлов, хранящих текущую копию БД

Sberbank
Blockchain
Laboratory

Децентрализованная система

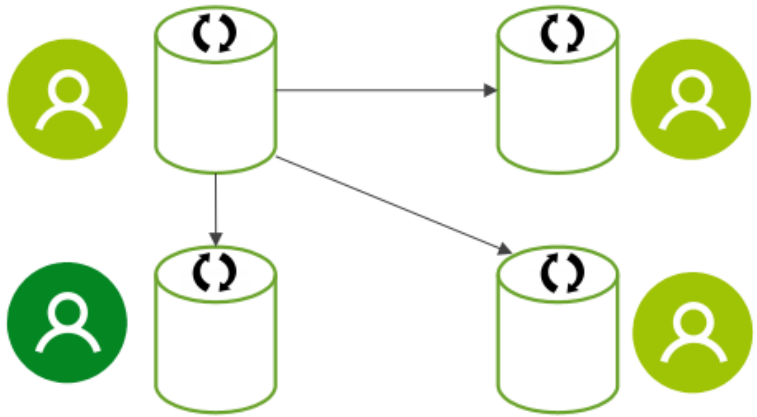


Множество всех узлов сети

- непустое подмножество узлов, хранящих текущую копию БД
  - непустое подмножество узлов, принимающих решение об изменении БД

Sberbank
Blockchain
Laboratory

Децентрализованная система



Множество всех узлов сети

- непустое подмножество узлов, хранящих текущую копию БД
  - непустое подмножество узлов, принимающих решение об изменении БД

Состояние — текущее состояние базы данных
Валидаторы — узлы, принимающие решение об изменении БД
Транзакция — предлагаемые изменения в БД

Sberbank Blockchain Laboratory

Permissioned-системы

Для примера (системы электронных платежей):

Sberbank
Blockchain
Laboratory

Permissioned-системы

Для примера (системы электронных платежей):

- валидаторы контролируются оператором, постоянными (крупными) участниками переводов $\Rightarrow$ **список валидаторов ограничен, требует регистрации, статический**

Sberbank
Blockchain
Laboratory

Permissioned-системы

Для примера (системы электронных платежей):

- валидаторы контролируются оператором, постоянными (крупными) участниками переводов $\Rightarrow$ **список валидаторов ограничен, требует регистрации, статический**
- остальные участники являются пользователями системы $\Rightarrow$ **список пользователей ограничен, требует регистрации, динамический**

Sberbank
Blockchain
Laboratory

Permissioned-системы

Для примера (системы электронных платежей):

- валидаторы контролируются оператором, постоянными (крупными) участниками переводов $\Rightarrow$ **список валидаторов ограничен, требует регистрации, статический**
- остальные участники являются пользователями системы $\Rightarrow$ **список пользователей ограничен, требует регистрации, динамический**

Существуют системы, которые в подобных условиях корректно работают при не более 1/3 недоверенных участников

Sberbank
Blockchain
Laboratory

Состояние

В примере

Идентификатор пользователя 1	Количество денежных средств 1
Идентификатор пользователя 2	Количество денежных средств 2
...	...

Sberbank
Blockchain
Laboratory

Состояние

В примере

Идентификатор пользователя 1	Количество денежных средств 1
Идентификатор пользователя 2	Количество денежных средств 2
...	...

Account-based модель

		Изменение
Идентификатор пользователя 1	Количество токенов 1	Вычесть
Идентификатор пользователя 2	Количество токенов 2	Прибавить
...	...	

Sberbank
Blockchain
Laboratory

Состояние

В примере

Идентификатор пользователя 1	Количество денежных средств 1
Идентификатор пользователя 2	Количество денежных средств 2
...	...

Account-based модель

		Изменение
Идентификатор пользователя 1	Количество токенов 1	Вычесть
Идентификатор пользователя 2	Количество токенов 2	Прибавить
...	...	

Модель UTXO

			Изменение
Идентификатор UTXO 1	Количество токенов 1	Идентификатор владельца 1	Удалить
Идентификатор UTXO 2	Количество токенов 2	Идентификатор владельца 2	
...	...	...	Создать

Sberbank Blockchain Laboratory

Свойства системы

Свойства для задачи из примера

Sberbank
Blockchain
Laboratory

Свойства системы

Свойства для задачи из примера

Базовые:

Дополнительные:

Sberbank
Blockchain
Laboratory

Свойства системы

Свойства для задачи из примера

Базовые:

- невозможность создать денежные средства, не имея полномочий

Дополнительные:

Sberbank
Blockchain
Laboratory

Свойства системы

Свойства для задачи из примера

Базовые:

- невозможность создать денежные средства, не имея полномочий
- невозможность передать “чужие” денежные средства

Дополнительные:

Sberbank
Blockchain
Laboratory

Свойства системы

Свойства для задачи из примера

Базовые:

- невозможность создать денежные средства, не имея полномочий
- невозможность передать “чужие” денежные средства
- невозможность уничтожить “чужие” денежные средства

Дополнительные:

Sberbank
Blockchain
Laboratory

Свойства системы

Свойства для задачи из примера

Базовые:

- невозможность создать денежные средства, не имея полномочий
- невозможность передать “чужие” денежные средства
- невозможность уничтожить “чужие” денежные средства

Дополнительные:

- узлам сети неизвестно, кем и сколько денежных средств было отправлено/получено

Sberbank Blockchain Laboratory

Свойства системы

Свойства для задачи из примера

Базовые:

- невозможность создать денежные средства, не имея полномочий
- невозможность передать “чужие” денежные средства
- невозможность уничтожить “чужие” денежные средства

Дополнительные:

- узлам сети неизвестно, кем и сколько денежных средств было отправлено/получено

Свойства для более общего случая

Базовые:

Дополнительные:

Sberbank
Blockchain
Laboratory

Свойства системы

Свойства для задачи из примера

Базовые:

- невозможность создать денежные средства, не имея полномочий
- невозможность передать “чужие” денежные средства
- невозможность уничтожить “чужие” денежные средства

Дополнительные:

- узлам сети неизвестно, кем и сколько денежных средств было отправлено/получено

Свойства для более общего случая

Базовые:

- невозможность неполномочного выпуска токенов

Дополнительные:

Sberbank Blockchain Laboratory

Свойства системы

Свойства для задачи из примера

Базовые:

- невозможность создать денежные средства, не имея полномочий
- невозможность передать “чужие” денежные средства
- невозможность уничтожить “чужие” денежные средства

Дополнительные:

- узлам сети неизвестно, кем и сколько денежных средств было отправлено/получено

Свойства для более общего случая

Базовые:

- невозможность неполномочного выпуска токенов
- невозможность неполномочного перевода токенов

Дополнительные:

Sberbank Blockchain Laboratory

Свойства системы

Свойства для задачи из примера

Базовые:

- невозможность создать денежные средства, не имея полномочий
- невозможность передать “чужие” денежные средства
- невозможность уничтожить “чужие” денежные средства

Дополнительные:

- узлам сети неизвестно, кем и сколько денежных средств было отправлено/получено

Свойства для более общего случая

Базовые:

- невозможность неполномочного выпуска токенов
- невозможность неполномочного перевода токенов
- невозможность неполномочного уничтожения токенов

Дополнительные:

Sberbank Blockchain Laboratory

Свойства системы

Свойства для задачи из примера

Базовые:

- невозможность создать денежные средства, не имея полномочий
- невозможность передать “чужие” денежные средства
- невозможность уничтожить “чужие” денежные средства

Дополнительные:

- узлам сети неизвестно, кем и сколько денежных средств было отправлено/получено

Свойства для более общего случая

Базовые:

- невозможность неполномочного выпуска токенов
- невозможность неполномочного перевода токенов
- невозможность неполномочного уничтожения токенов

Дополнительные:

- **анонимность** отправителя и получателя

Sberbank
Blockchain
Laboratory

Свойства системы

Свойства для задачи из примера

Базовые:

- невозможность создать денежные средства, не имея полномочий
- невозможность передать “чужие” денежные средства
- невозможность уничтожить “чужие” денежные средства

Дополнительные:

- узлам сети неизвестно, кем и сколько денежных средств было отправлено/получено

Свойства для более общего случая

Базовые:

- невозможность неполномочного выпуска токенов
- невозможность неполномочного перевода токенов
- невозможность неполномочного уничтожения токенов

Дополнительные:

- **анонимность** отправителя и получателя
- **конфиденциальность** количества токенов

Sberbank Blockchain Laboratory

Особенность обеспечения анонимности и конфиденциальности

Sberbank
Blockchain
Laboratory

Особенность обеспечения анонимности и конфиденциальности

валидация транзакции выполняется несколькими валидаторами

Sberbank
Blockchain
Laboratory

Особенность обеспечения анонимности и конфиденциальности

валидация транзакции выполняется несколькими валидаторами

валидаторам необходимо знать отправителя, получателя, количество переводимых токенов

Sberbank
Blockchain
Laboratory

Особенность обеспечения анонимности и конфиденциальности

валидация транзакции выполняется несколькими валидаторами

$\Downarrow$

валидаторам необходимо знать отправителя, получателя, количество переводимых токенов

узлам сети (в т.ч. валидаторам) должны быть неизвестны отправитель, получатель, количество переводимых токенов

Sberbank Blockchain Laboratory

Особенность обеспечения анонимности и конфиденциальности

валидация транзакции выполняется несколькими валидаторами

$\Downarrow$

валидаторам необходимо знать отправителя, получателя, количество переводимых токенов

узлам сети (в т.ч. валидаторам) должны быть неизвестны отправитель, получатель, количество переводимых токенов

$\Downarrow$

валидация транзакции без получения доступа к информации об отправителе, получателе, количестве переводимых токенов

Sberbank Blockchain Laboratory

Примеры систем и криптографических механизмов

Примеры систем: zCash, CryptoNote, RingCT, AZTEC, Zether, Alibaba Patent, MimbleWimble, ...

Sberbank
Blockchain
Laboratory

Примеры систем и криптографических механизмов

Примеры систем: zCash, CryptoNote, RingCT, AZTEC, Zether, Alibaba Patent, MimbleWimble, ...

Наиболее часто встречающиеся классы неклассических механизмов:

- схема гомоморфного шифрования
- схема обязательства (commitment)
- схема кольцевой подписи
- протокол доказательства с нулевым разглашением

Sberbank
Blockchain
Laboratory

Схема гомоморфного шифрования

- $KGen(1^k)$ — алгоритм генерации ключей, возвращает секретный ключ sk и открытый ключ pk
- $Enc(pk, m)$ — алгоритм шифрования, возвращает шифртекст c
- $Dec(sk, c)$ — алгоритм расшифрования, возвращает открытый текст m

Sberbank
Blockchain
Laboratory

Схема гомоморфного шифрования

- $KGen(1^k)$ — алгоритм генерации ключей, возвращает секретный ключ sk и открытый ключ pk
- $Enc(pk, m)$ — алгоритм шифрования, возвращает шифртекст c
- $Dec(sk, c)$ — алгоритм расшифрования, возвращает открытый текст m

Схема гомоморфного шифрования позволяет производить элементарные операции над шифртекстами

Sberbank
Blockchain
Laboratory

Схема обязательства (commitment)

- $Setup(1^\lambda)$ — алгоритм генерации ключей, возвращает открытый параметр pk
- $Cmt(pk, r, v)$ — алгоритм вычисления коммитмента, возвращает значение коммитмента c
- $Open(pk, r, c)$ — алгоритм “открытия” коммитмента, возвращает значение v или ошибку

Sberbank
Blockchain
Laboratory

Схема обязательства (commitment)

- $Setup(1^\lambda)$ — алгоритм генерации ключей, возвращает открытый параметр pk
- $Cmt(pk, r, v)$ — алгоритм вычисления коммитмента, возвращает значение коммитмента c
- $Open(pk, r, c)$ — алгоритм "открытия" коммитмента, возвращает значение v или ошибку

Свойства схемы обязательства:

Sberbank
Blockchain
Laboratory

Схема обязательства (commitment)

- $Setup(1^\lambda)$ — алгоритм генерации ключей, возвращает открытый параметр pk
- $Cmt(pk, r, v)$ — алгоритм вычисления коммитмента, возвращает значение коммитмента c
- $Open(pk, r, c)$ — алгоритм "открытия" коммитмента, возвращает значение v или ошибку

Свойства схемы обязательства:

- binding — невозможно "открыть" коммитмент c двумя разными способами

Sberbank
Blockchain
Laboratory

Схема обязательства (commitment)

- $Setup(1^\lambda)$ — алгоритм генерации ключей, возвращает открытый параметр pk
- $Cmt(pk, r, v)$ — алгоритм вычисления коммитмента, возвращает значение коммитмента c
- $Open(pk, r, c)$ — алгоритм "открытия" коммитмента, возвращает значение v или ошибку

Свойства схемы обязательства:

- binding — невозможно "открыть" коммитмент c двумя разными способами
- hiding — значение коммитмента c не раскрывает никакой информации о значении v

Sberbank
Blockchain
Laboratory

Схема кольцевой подписи

- $KGen(1^k)$ — алгоритм генерации ключей, возвращает i-му участнику ключ подписи sk_i и ключ проверки подписи pk_i, $i = 1, \ldots, n$
- $Sign(m, pk_1, \ldots, pk_n, i, sk_i)$ — алгоритм подписи, возвращает значение подписи σ
- $Verify(m, pk_1, \ldots, pk_n, \sigma)$ — алгоритм проверки подписи, возвращает 1/0

Sberbank
Blockchain
Laboratory

Схема кольцевой подписи

- $KGen(1^k)$ — алгоритм генерации ключей, возвращает i-му участнику ключ подписи sk_i и ключ проверки подписи pk_i, $i = 1, \ldots, n$
- $Sign(m, pk_1, \ldots, pk_n, i, sk_i)$ — алгоритм подписи, возвращает значение подписи σ
- $Verify(m, pk_1, \ldots, pk_n, \sigma)$ — алгоритм проверки подписи, возвращает 1/0

Схема кольцевой подписи позволяет одному из участников группы подписать некоторое сообщение от имени группы, при этом по значению подписи невозможно узнать, кто именно из участников группы подписал сообщение

Sberbank
Blockchain
Laboratory

Протокол доказательства с нулевым разглашением

- $Kgen(1^\lambda)$ — алгоритм генерации ключей, возвращает открытый параметр pk
- $Prove(u, w)$ — алгоритм доказательства, возвращает доказательство π
- $Verify(u, \pi)$ — алгоритм проверки доказательства, возвращает 1/0

Протокол позволяет одному участнику доказать другому, что утверждение u о значении w верно, не раскрывая значение w

Sberbank
Blockchain
Laboratory

Протокол доказательства с нулевым разглашением

- $Kgen(1^\lambda)$ — алгоритм генерации ключей, возвращает открытый параметр pk
- $Prove(u, w)$ — алгоритм доказательства, возвращает доказательство π
- $Verify(u, \pi)$ — алгоритм проверки доказательства, возвращает 1/0

Протокол позволяет одному участнику доказать другому, что утверждение u о значении w верно, не раскрывая значение w

Свойства протокола доказательства с нулевым разглашением:

Sberbank
Blockchain
Laboratory

Протокол доказательства с нулевым разглашением

- $Kgen(1^\lambda)$ — алгоритм генерации ключей, возвращает открытый параметр pk
- $Prove(u, w)$ — алгоритм доказательства, возвращает доказательство π
- $Verify(u, \pi)$ — алгоритм проверки доказательства, возвращает 1/0

Протокол позволяет одному участнику доказать другому, что утверждение u о значении w верно, не раскрывая значение w

Свойства протокола доказательства с нулевым разглашением:

- полнота — если утверждение верно, то доказывающий убедит проверяющего с наперед заданной точностью

Sberbank
Blockchain
Laboratory

Протокол доказательства с нулевым разглашением

- $Kgen(1^\lambda)$ — алгоритм генерации ключей, возвращает открытый параметр pk
- $Prove(u, w)$ — алгоритм доказательства, возвращает доказательство π
- $Verify(u, \pi)$ — алгоритм проверки доказательства, возвращает 1/0

Протокол позволяет одному участнику доказать другому, что утверждение u о значении w верно, не раскрывая значение w

Свойства протокола доказательства с нулевым разглашением:

- полнота — если утверждение верно, то доказывающий убедит проверяющего с наперед заданной точностью
- корректность — если утверждение неверно, то любой доказывающий сможет убедить проверяющего с пренебрежимо малой вероятностью

Sberbank Blockchain Laboratory

Протокол доказательства с нулевым разглашением

- $Kgen(1^\lambda)$ — алгоритм генерации ключей, возвращает открытый параметр pk
- $Prove(u, w)$ — алгоритм доказательства, возвращает доказательство π
- $Verify(u, \pi)$ — алгоритм проверки доказательства, возвращает 1/0

Протокол позволяет одному участнику доказать другому, что утверждение u о значении w верно, не раскрывая значение w

Свойства протокола доказательства с нулевым разглашением:

- полнота — если утверждение верно, то доказывающий убедит проверяющего с наперед заданной точностью
- корректность — если утверждение неверно, то любой доказывающий сможет убедить проверяющего с пренебрежимо малой вероятностью
- нулевое разглашение — доказательство π не раскрывает никакой информации о значении w

Sberbank Blockchain Laboratory

Использование криптографических механизмов

Механизмы:

- схема гомоморфного шифрования
- схема commitment
- схема кольцевой подписи

- протокол доказательства с нулевым разглашением

Цель использования:

Sberbank Blockchain Laboratory

Использование криптографических механизмов

Механизмы:

- схема гомоморфного шифрования
- схема commitment
- схема кольцевой подписи

- протокол доказательства с нулевым разглашением

Цель использования:

- сокрытие количества токенов

Sberbank
Blockchain
Laboratory

Использование криптографических механизмов

Механизмы:

- схема гомоморфного шифрования
- схема commitment
- схема кольцевой подписи

- протокол доказательства с нулевым разглашением

Цель использования:

- сокрытие количества токенов
- сокрытие количества токенов

Sberbank
Blockchain
Laboratory

Использование криптографических механизмов

Механизмы:

- схема гомоморфного шифрования
- схема commitment
- схема кольцевой подписи
- протокол доказательства с нулевым разглашением

Цель использования:

- сокрытие количества токенов
- сокрытие количества токенов
- “перемешивание” идентификаторов пользователей/UTXO

Sberbank Blockchain Laboratory

Использование криптографических механизмов

Механизмы:	Цель использования:
• схема гомоморфного шифрования	• сокрытие количества токенов
• схема commitment	• сокрытие количества токенов
• схема кольцевой подписи	• “перемешивание” идентификаторов пользователей/UTXO
• протокол доказательства с нулевым разглашением	• валидация транзакции без доступа к содержимому

Sberbank
Blockchain
Laboratory

Alibaba Patent: состояние

Sberbank
Blockchain
Laboratory

Alibaba Patent: состояние

Состояние в account-based модели

		Изменение
pk_A	v_A	Вычесть
pk_B	v_B	Прибавить
...	...	

Sberbank
Blockchain
Laboratory

Alibaba Patent: состояние

Состояние в account-based модели

		Изменение
pk_A	v_A	Вычесть
pk_B	v_B	Прибавить
...	...	

Состояние Alibaba Patent

		Изменение
pk_A	(V_A, R_A, S_A)	Вычесть
pk_B	(V_B, R_B, S_B)	Прибавить
...	...	

- $V_A = PC(v_A, r_A)$ — гомоморфный Pedersen Commitment для значения количества токенов v_A с использованием "ослепляющего" параметра r_A
- $R_A = HE(pk_A, r_A)$ — гомоморфно зашифрованное значение r_A на открытом ключе pk_A
- $S_A = HE(pk_A, v_A)$ — гомоморфно зашифрованное значение v_A на открытом ключе pk_A

Sberbank Blockchain Laboratory

Alibaba Patent: транзакция

Содержимое транзакции перевода v токенов:

Валидация транзакции:

Изменение состояния:

Sberbank
Blockchain
Laboratory

Alibaba Patent: транзакция

Содержимое транзакции перевода v токенов:

- открытые ключи отправителя и получателя pk_A, pk_B

Валидация транзакции:

Изменение состояния:

Sberbank
Blockchain
Laboratory

Alibaba Patent: транзакция

Содержимое транзакции перевода v токенов:

- открытые ключи отправителя и получателя pk_A, pk_B
- $T = PC(v, r)$, где r — новый "ослепляющий" параметр для транзакции

Валидация транзакции:

Изменение состояния:

Sberbank
Blockchain
Laboratory

Alibaba Patent: транзакция

Содержимое транзакции перевода v токенов:

- открытые ключи отправителя и получателя pk_A, pk_B
- $T = PC(v, r)$, где r — новый "ослепляющий" параметр для транзакции
- $T_A = HE(pk_A, r)$, $T'_A = HE(pk_A, v)$

Валидация транзакции:

Изменение состояния:

Sberbank Blockchain Laboratory

Alibaba Patent: транзакция

Содержимое транзакции перевода v токенов:

- открытые ключи отправителя и получателя pk_A, pk_B
- $T = PC(v, r)$, где r — новый "ослепляющий" параметр для транзакции
- $T_A = HE(pk_A, r)$, $T'_A = HE(pk_A, v)$
- $T_B = HE(pk_B, r)$, $T'_B = HE(pk_B, v)$

Валидация транзакции:

Изменение состояния:

Sberbank Blockchain Laboratory

Alibaba Patent: транзакция

Содержимое транзакции перевода v токенов:

- открытые ключи отправителя и получателя pk_A, pk_B
- $T = PC(v, r)$, где r — новый "ослепляющий" параметр для транзакции
- $T_A = HE(pk_A, r)$, $T'_A = HE(pk_A, v)$
- $T_B = HE(pk_B, r)$, $T'_B = HE(pk_B, v)$
- доказательство:

Валидация транзакции:

Изменение состояния:

Sberbank Blockchain Laboratory

Alibaba Patent: транзакция

Содержимое транзакции перевода v токенов:

- открытые ключи отправителя и получателя pk_A, pk_B
- $T = PC(v, r)$, где r — новый "ослепляющий" параметр для транзакции
- $T_A = HE(pk_A, r)$, $T'_A = HE(pk_A, v)$
- $T_B = HE(pk_B, r)$, $T'_B = HE(pk_B, v)$
- доказательство:
  - передается неотрицательная сумма $(v > 0)$

Валидация транзакции:

Изменение состояния:

Sberbank Blockchain Laboratory

Alibaba Patent: транзакция

Содержимое транзакции перевода v токенов:

- открытые ключи отправителя и получателя pk_A, pk_B
- $T = PC(v, r)$, где r — новый "ослепляющий" параметр для транзакции
- $T_A = HE(pk_A, r)$, $T'_A = HE(pk_A, v)$
- $T_B = HE(pk_B, r)$, $T'_B = HE(pk_B, v)$
- доказательство:
  - передается неотрицательная сумма $(v > 0)$
  - у отправителя достаточно токенов $(v_A - v > 0)$

Валидация транзакции:

Изменение состояния:

Sberbank Blockchain Laboratory

Alibaba Patent: транзакция

Содержимое транзакции перевода v токенов:

- открытые ключи отправителя и получателя pk_A, pk_B
- $T = PC(v, r)$, где r — новый "ослепляющий" параметр для транзакции
- $T_A = HE(pk_A, r)$, $T'_A = HE(pk_A, v)$
- $T_B = HE(pk_B, r)$, $T'_B = HE(pk_B, v)$
- доказательство:
  - передается неотрицательная сумма $(v > 0)$
  - у отправителя достаточно токенов $(v_A - v > 0)$
  - при вычислении T, T_A, T_B, T'_A, T'_B использовались одинаковые r, v

Валидация транзакции:

Изменение состояния:

Sberbank Blockchain Laboratory

Alibaba Patent: транзакция

Содержимое транзакции перевода v токенов:

- открытые ключи отправителя и получателя pk_A, pk_B
- $T = PC(v, r)$, где r — новый "ослепляющий" параметр для транзакции
- $T_A = HE(pk_A, r)$, $T'_A = HE(pk_A, v)$
- $T_B = HE(pk_B, r)$, $T'_B = HE(pk_B, v)$
- доказательство:
  - передается неотрицательная сумма $(v > 0)$
  - у отправителя достаточно токенов $(v_A - v > 0)$
  - при вычислении T, T_A, T_B, T'_A, T'_B использовались одинаковые r, v
- подпись отправителя ко всему содержимому транзакции

Валидация транзакции:

Изменение состояния:

Sberbank Blockchain Laboratory

Alibaba Patent: транзакция

Содержимое транзакции перевода v токенов:

- открытые ключи отправителя и получателя pk_A, pk_B
- $T = PC(v, r)$, где r — новый "ослепляющий" параметр для транзакции
- $T_A = HE(pk_A, r)$, $T'_A = HE(pk_A, v)$
- $T_B = HE(pk_B, r)$, $T'_B = HE(pk_B, v)$
- доказательство:
  - передается неотрицательная сумма $(v > 0)$
  - у отправителя достаточно токенов $(v_A - v > 0)$
  - при вычислении T, T_A, T_B, T'_A, T'_B использовались одинаковые r, v
- подпись отправителя ко всему содержимому транзакции

Валидация транзакции:

- проверить подпись отправителя

Изменение состояния:

Sberbank Blockchain Laboratory

Alibaba Patent: транзакция

Содержимое транзакции перевода v токенов:

- открытые ключи отправителя и получателя pk_A, pk_B
- $T = PC(v, r)$, где r — новый "ослепляющий" параметр для транзакции
- $T_A = HE(pk_A, r)$, $T'_A = HE(pk_A, v)$
- $T_B = HE(pk_B, r)$, $T'_B = HE(pk_B, v)$
- доказательство:
  - передается неотрицательная сумма $(v > 0)$
  - у отправителя достаточно токенов $(v_A - v > 0)$
  - при вычислении T, T_A, T_B, T'_A, T'_B использовались одинаковые r, v
- подпись отправителя ко всему содержимому транзакции

Валидация транзакции:

- проверить подпись отправителя
- проверить доказательство

Изменение состояния:

Sberbank Blockchain Laboratory

Alibaba Patent: транзакция

Содержимое транзакции перевода v токенов:

- открытые ключи отправителя и получателя pk_A, pk_B
- $T = PC(v, r)$, где r — новый "ослепляющий" параметр для транзакции
- $T_A = HE(pk_A, r)$, $T'_A = HE(pk_A, v)$
- $T_B = HE(pk_B, r)$, $T'_B = HE(pk_B, v)$
- доказательство:
  - передается неотрицательная сумма $(v > 0)$
  - у отправителя достаточно токенов $(v_A - v > 0)$
  - при вычислении T, T_A, T_B, T'_A, T'_B использовались одинаковые r, v
- подпись отправителя ко всему содержимому транзакции

Валидация транзакции:

- проверить подпись отправителя
- проверить доказательство

Изменение состояния:

- $V_{A_{new}} = V_A - T$, $R_{A_{new}} = R_A - T_A$, $S_{A_{new}} = S_A - T'_A$

Sberbank Blockchain Laboratory

Alibaba Patent: транзакция

Содержимое транзакции перевода v токенов:

- открытые ключи отправителя и получателя pk_A, pk_B
- $T = PC(v, r)$, где r — новый "ослепляющий" параметр для транзакции
- $T_A = HE(pk_A, r)$, $T'_A = HE(pk_A, v)$
- $T_B = HE(pk_B, r)$, $T'_B = HE(pk_B, v)$
- доказательство:
  - передается неотрицательная сумма $(v > 0)$
  - у отправителя достаточно токенов $(v_A - v > 0)$
  - при вычислении T, T_A, T_B, T'_A, T'_B использовались одинаковые r, v
- подпись отправителя ко всему содержимому транзакции

Валидация транзакции:

- проверить подпись отправителя
- проверить доказательство

Изменение состояния:

- $V_{A_{new}} = V_A - T$, $R_{A_{new}} = R_A - T_A$, $S_{A_{new}} = S_A - T'_A$
- $V_{B_{new}} = V_B + T$, $R_{B_{new}} = R_B + T_B$, $S_{B_{new}} = R_B + T'_B$

Sberbank Blockchain Laboratory

Alibaba Patent: используемые механизмы

Sberbank
Blockchain
Laboratory

Alibaba Patent: используемые механизмы

- гомоморфный Commitment используется для сокрытия количества токенов и упрощения изменения состояния

Sberbank
Blockchain
Laboratory

Alibaba Patent: используемые механизмы

- гомоморфный Commitment используется для сокрытия количества токенов и упрощения изменения состояния
- гомоморфное шифрование используется для того, чтобы пользователи смогли узнать свой баланс (поскольку после изменения состояния “ослепляющий” параметр, соответствующий балансу, меняется)

Sberbank
Blockchain
Laboratory

Alibaba Patent: используемые механизмы

- гомоморфный Commitment используется для сокрытия количества токенов и упрощения изменения состояния
- гомоморфное шифрование используется для того, чтобы пользователи смогли узнать свой баланс (поскольку после изменения состояния "ослепляющий" параметр, соответствующий балансу, меняется)
- протокол доказательства с нулевым разглашением используется как Range Proof ($v > 0$, $v_A - v > 0$)

Sberbank
Blockchain
Laboratory

Alibaba Patent: используемые механизмы

- гомоморфный Commitment используется для сокрытия количества токенов и упрощения изменения состояния
- гомоморфное шифрование используется для того, чтобы пользователи смогли узнать свой баланс (поскольку после изменения состояния "ослепляющий" параметр, соответствующий балансу, меняется)
- протокол доказательства с нулевым разглашением используется как Range Proof ($v > 0$, $v_A - v > 0$)
- авторский протокол доказательства с нулевым разглашением используется для проверки оставшихся свойств

Sberbank
Blockchain
Laboratory

MimbleWimble: состояние

Sberbank
Blockchain
Laboratory

MimbleWimble: состояние

Состояние в модели UTXO

			Изменение
UTXO id 1	v_1	pk_1	Удалить
UTXO id 2	v_2	pk_2	
...	...	...	Создать

Sberbank
Blockchain
Laboratory

MimbleWimble: состояние

Состояние в модели UTXO

			Изменение
UTXO id 1	v_1	pk_1	Удалить
UTXO id 2	v_2	pk_2	
...	...	...	Создать

Состояние MimbleWimble

		Изменение
UTXO id 1	C_1	Удалить
UTXO id 2	C_2	
...	...	Создать

- $C_1 = PC(v_1, r_1)$ — гомоморфный Pedersen Commitment для значения количества токенов v_1 с использованием “ослепляющего” параметра r_1

Sberbank Blockchain Laboratory

MimbleWimble: транзакция

Содержимое транзакции перевода v токенов:

Валидация транзакции:

Изменение состояния:

Sberbank
Blockchain
Laboratory

MimbleWimble: транзакция

Содержимое транзакции перевода v токенов:

- входной UTXO $C^I = PC(v, r_0)$, где r_0 известно отправителю

Валидация транзакции:

Изменение состояния:

Sberbank
Blockchain
Laboratory

MimbleWimble: транзакция

Содержимое транзакции перевода v токенов:

- входной UTXO $C^I = PC(v, r_0)$, где r_0 известно отправителю
- выходной (новый) UTXO $C^O = PC(v, r)$, где r — новый “ослепляющий” параметр (формирует получатель)

Валидация транзакции:

Изменение состояния:

Sberbank
Blockchain
Laboratory

MimbleWimble: транзакция

Содержимое транзакции перевода v токенов:

- входной UTXO $C^I = PC(v, r_0)$, где r_0 известно отправителю
- выходной (новый) UTXO $C^O = PC(v, r)$, где r — новый "ослепляющий" параметр (формирует получатель)
- доказательство, что $v > 0$

Валидация транзакции:

Изменение состояния:

Sberbank
Blockchain
Laboratory

MimbleWimble: транзакция

Содержимое транзакции перевода v токенов:

- входной UTXO $C^I = PC(v, r_0)$, где r_0 известно отправителю
- выходной (новый) UTXO $C^O = PC(v, r)$, где r — новый "ослепляющий" параметр (формирует получатель)
- доказательство, что $v > 0$
- сообщение

Валидация транзакции:

Изменение состояния:

Sberbank
Blockchain
Laboratory

MimbleWimble: транзакция

Содержимое транзакции перевода v токенов:

- входной UTXO $C^I = PC(v, r_0)$, где r_0 известно отправителю
- выходной (новый) UTXO $C^O = PC(v, r)$, где r — новый "ослепляющий" параметр (формирует получатель)
- доказательство, что $v > 0$
- сообщение
- подпись к сообщению (формируется совместно отправителем и получателем, в качестве секретных ключей отправителя и получателя используются $-r_0$ и r)

Валидация транзакции:

Изменение состояния:

Sberbank Blockchain Laboratory

MimbleWimble: транзакция

Содержимое транзакции перевода v токенов:

- входной UTXO $C^I = PC(v, r_0)$, где r_0 известно отправителю
- выходной (новый) UTXO $C^O = PC(v, r)$, где r — новый "ослепляющий" параметр (формирует получатель)
- доказательство, что $v > 0$
- сообщение
- подпись к сообщению (формируется совместно отправителем и получателем, в качестве секретных ключей отправителя и получателя используются $-r_0$ и r)

Валидация транзакции:

- проверить подпись отправителя и получателя, используя $C^O - C^I = R$ в качестве открытого ключа

Изменение состояния:

Sberbank Blockchain Laboratory

MimbleWimble: транзакция

Содержимое транзакции перевода v токенов:

- входной UTXO $C^I = PC(v, r_0)$, где r_0 известно отправителю
- выходной (новый) UTXO $C^O = PC(v, r)$, где r — новый "ослепляющий" параметр (формирует получатель)
- доказательство, что $v > 0$
- сообщение
- подпись к сообщению (формируется совместно отправителем и получателем, в качестве секретных ключей отправителя и получателя используются $-r_0$ и r)

Валидация транзакции:

- проверить подпись отправителя и получателя, используя $C^O - C^I = R$ в качестве открытого ключа
- проверить доказательство

Изменение состояния:

Sberbank Blockchain Laboratory

MimbleWimble: транзакция

Содержимое транзакции перевода v токенов:

- входной UTXO $C^I = PC(v, r_0)$, где r_0 известно отправителю
- выходной (новый) UTXO $C^O = PC(v, r)$, где r — новый "ослепляющий" параметр (формирует получатель)
- доказательство, что $v > 0$
- сообщение
- подпись к сообщению (формируется совместно отправителем и получателем, в качестве секретных ключей отправителя и получателя используются $-r_0$ и r)

Валидация транзакции:

- проверить подпись отправителя и получателя, используя $C^O - C^I = R$ в качестве открытого ключа
- проверить доказательство

Изменение состояния:

- удалить C^I из множества UTXO

Sberbank Blockchain Laboratory

MimbleWimble: транзакция

Содержимое транзакции перевода v токенов:

- входной UTXO $C^I = PC(v, r_0)$, где r_0 известно отправителю
- выходной (новый) UTXO $C^O = PC(v, r)$, где r — новый "ослепляющий" параметр (формирует получатель)
- доказательство, что $v > 0$
- сообщение
- подпись к сообщению (формируется совместно отправителем и получателем, в качестве секретных ключей отправителя и получателя используются $-r_0$ и r)

Валидация транзакции:

- проверить подпись отправителя и получателя, используя $C^O - C^I = R$ в качестве открытого ключа
- проверить доказательство

Изменение состояния:

- удалить C^I из множества UTXO
- добавить C^O в множество UTXO

Sberbank Blockchain Laboratory

MimbleWimble: используемые механизмы

Sberbank
Blockchain
Laboratory

MimbleWimble: используемые механизмы

- гомоморфный Commitment используется для сокрытия количества токенов и упрощения валидации транзакции

Sberbank
Blockchain
Laboratory

MimbleWimble: используемые механизмы

- гомоморфный Commitment используется для сокрытия количества токенов и упрощения валидации транзакции
- протокол доказательства с нулевым разглашением Bulletproof используется как Range Proof ($v > 0$)

Sberbank
Blockchain
Laboratory

MimbleWimble: используемые механизмы

- гомоморфный Commitment используется для сокрытия количества токенов и упрощения валидации транзакции
- протокол доказательства с нулевым разглашением Bulletproof используется как Range Proof ($v > 0$)
- “гомоморфная” подпись, которую можно вычислить как сумму нескольких подписей, используется:

Sberbank
Blockchain
Laboratory

MimbleWimble: используемые механизмы

- гомоморфный Commitment используется для сокрытия количества токенов и упрощения валидации транзакции
- протокол доказательства с нулевым разглашением Bulletproof используется как Range Proof ($v > 0$)
- “гомоморфная” подпись, которую можно вычислить как сумму нескольких подписей, используется:
  - как замена обычной подписи

Sberbank
Blockchain
Laboratory

MimbleWimble: используемые механизмы

- гомоморфный Commitment используется для сокрытия количества токенов и упрощения валидации транзакции
- протокол доказательства с нулевым разглашением Bulletproof используется как Range Proof ($v > 0$)
- "гомоморфная" подпись, которую можно вычислить как сумму нескольких подписей, используется:
  - как замена обычной подписи
  - как часть доказательства других свойств (ключ проверки подписи $R = C^O - C^I$)

Sberbank
Blockchain
Laboratory

Открытые задачи

Sberbank
Blockchain
Laboratory

Открытые задачи

1. Анализ оптимальности существующих систем для конкретной модели ведения реестра

Sberbank
Blockchain
Laboratory

Открытые задачи

1. Анализ оптимальности существующих систем для конкретной модели ведения реестра
2. Синтез более эффективных/стойких представителей классов криптографических механизмов, используемых в существующих системах

Sberbank
Blockchain
Laboratory

Открытые задачи

1. Анализ оптимальности существующих систем для конкретной модели ведения реестра
2. Синтез более эффективных/стойких представителей классов криптографических механизмов, используемых в существующих системах
3. Синтез более эффективных/стойких систем

Sberbank
Blockchain
Laboratory

Открытые задачи

1. Анализ оптимальности существующих систем для конкретной модели ведения реестра
2. Синтез более эффективных/стойких представителей классов криптографических механизмов, используемых в существующих системах
3. Синтез более эффективных/стойких систем
   - синтез принципиально других криптографических механизмов

Sberbank
Blockchain
Laboratory

Спасибо!

Сергей Кяжин

Лаборатория блокчейн, Сбербанк России

blockchain-research@sberbank.ru

Sberbank
Blockchain
Laboratory