Федеральное государственное автономное образовательное учреждение высшего образования
Национальный исследовательский ядерный университет «МИФИ»

Кафедра «Криптология и кибербезопасность»

Криптографические протоколы

курс лекций

Запечников Сергей Владимирович,
профессор кафедры «Криптология
и кибербезопасность» НИЯУ МИФИ

Москва – 2018

Криптографические протоколы

курс лекций

Лекция 4.
Системы распределенного реестра (блокчейн-технологии)

26 февраля 2018 г.

Виды блокчейн-платформ

Открытые (permissionless) – позволяют стать участниками платформы неограниченному кругу лиц, никакой регистрации или отзыва полномочий не требуется.

Примеры: Bitcoin, Ethereum, многочисленные “Altcoins”, Toda- Algorand и пр.

Закрытые (permissioned) – ограничивают круг участников пределами сообщества, для участия требуется регистрация, при выходе из сообщества право доступа отзывается.

Примеры: Corda, проект Hyperledger (5 платформ, самая известная – Hyperledger Fabric), Quorum, Tendermint и др.

Особенности открытых блокчейн-платформ

- **Формирование новых блоков транзакций происходит посредством «доказательства выполнения работы» (proof-of-work), «доказательства обладания долей» (proof-of-stake) или другим аналогичным способом *(принцип лотереи)*.**
- **Участники могут легко добавляться и выходить из блокчейн-сети, от присутствия или отсутствия конкретного участника в целом ничего не зависит, возможно анонимное участие.**
- **Для работы открытого блокчейна *требуется криптовалюта*, чтобы стимулировать майнеров. «Внешняя» и «внутренняя» криптовалюта может быть одинаковой (Bitcoin) или разной (Ethereum: эфир и газ).**
- **Открытые блокчейн-платформы очень ресурсоёмки (электроэнергия, машинное время): предполагается, что к 2035 году на майнинг биткоинов будет тратиться столько же электроэнергии, сколько сейчас потребляет среднее европейское государство.**

Особенности закрытых блокчейн-платформ

- **Формирование новых блоков транзакций происходит за 3 шага:**
  1) **валидация,**
  2) **упорядочение отдельных транзакций в блок,**
  3) **выполнение протокола византийского соглашения *(принцип голосования)*.**
- **Участники не могут самостоятельно добавляться и выходить из блокчейн-сети – для этого удостоверяющий центр (центр регистрации) должен выдать участнику его цифровой идентификатор и ключи.**
- **Корпоративные блокчейн-платформы обладают высоким быстродействием и хорошей масштабируемостью.**
- **Для работы корпоративного блокчейна *не требуется криптовалюта*.**

Возможности блокчейн-платформ

- **Реестровые применения: блокчейн-платформы могут использоваться как особые базы данных – распределенный реестр (distributed ledger). Основные свойства распределенного реестра:**

1) невозможно изменить историю транзакций,

2) копии реестра у всех участников блокчейн-платформы синхронизированы,

3) добавление новых блоков записей выполняется только в результате достижения консенсуса,

4) Формируемая структура данных – ациклический ориентированный граф (DAG – Directed acyclic graph)

- **Смарт-контракты: блокчейн-платформа становится платформой децентрализованных вычислений**

Сферы применения блокчейн-платформ

- **Системы валовых расчетов реального времени** (RTGS – Real-Time Gross Settlement)
- **Системы международных банковских переводов**
- **Страхование:** Обработка страховых случаев
- **Международная торговля:** Экспортно-импортные операции
- **Логистика:** Управление цепочками поставок (supply chain management)
- **Кредитование юридических лиц:** Синдицированный кредит

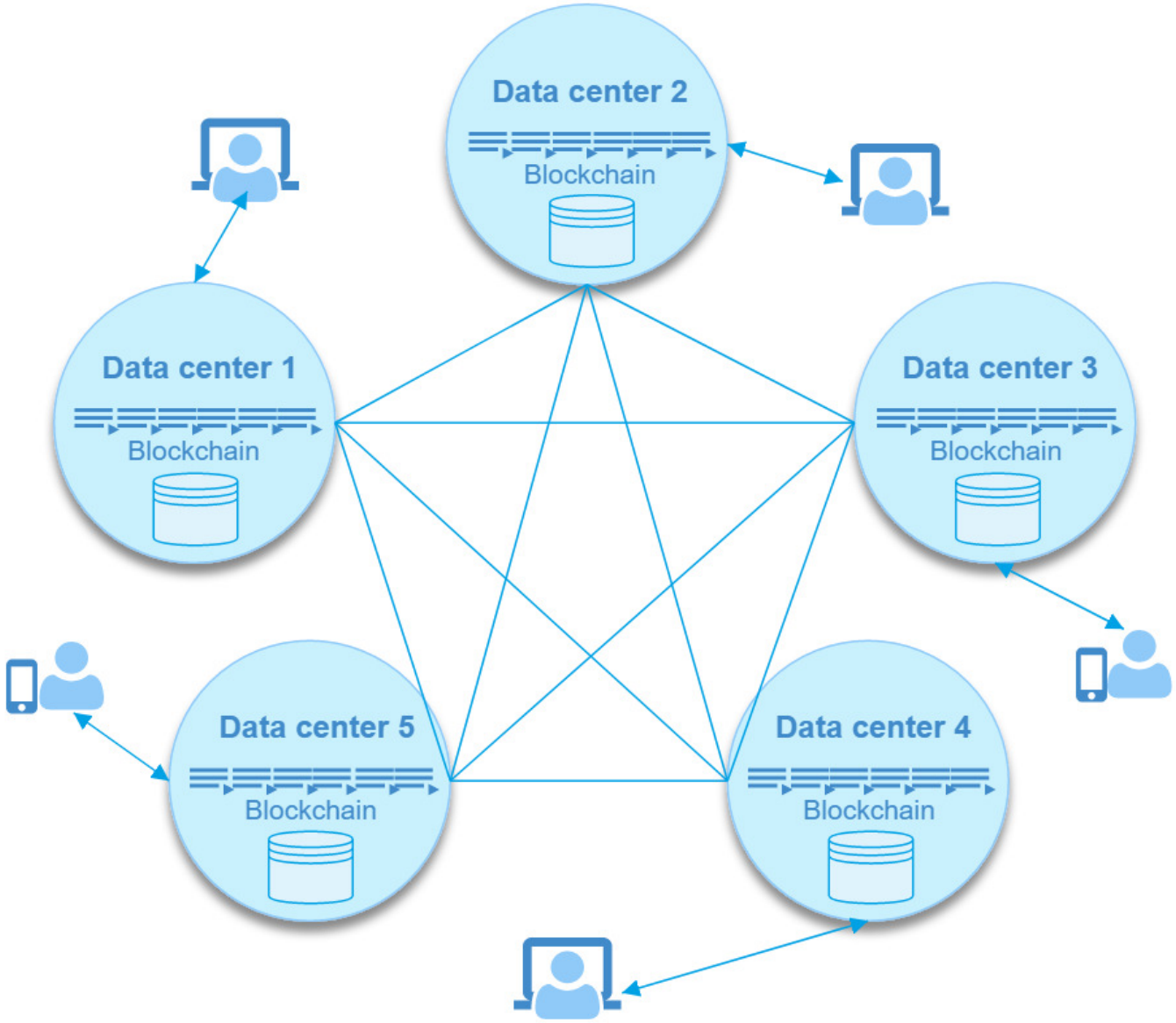
Важные идеи, положенные в основу блокчейн-платформ

1. **Полностью децентрализованная система. Нет одного такого узла, который можно вывести из строя, чтобы разрушить или «подвесить» всю систему.**
2. **Каждая нода блокчейна поддерживает синхронную (или почти синхронную) с остальными нодами копию общей базы данных. Это называется репликацией.**
3. **Базу данных можно только дополнять. Никакие изменения в ранее внесённые записи не допускаются. Таким образом, формируется нередактируемый реестр транзакций.**
4. **Любые новые записи в реестр можно вносить только с согласия квалифицированного большинства участников. В зависимости от технологии это *1/2 + 1 голос* либо *2/3 + 1 голос*. Это называется консенсусом.**
5. **Транзакция может сопровождаться выполнением произвольного программного кода, в котором описаны правила взаимодействия участников блокчейн-платформы и правила их обращения с активами, которые учитываются в базе данных. Этот код называется смарт-контрактом.**

Основные составляющие блокчейн-платформы с технической точки зрения

- ***Прикладной уровень – смарт-контракты*** **– код (программа), исполняемый каждой нодой сети при валидации транзакций. Криптовалюты – это частный случай, когда нет смарт-контрактов, а есть просто множество наборов данных**
  (*адрес, баланс*),
  а единственная разрешённая транзакция – перевод между адресами:
  (адрес_1, баланс – сумма_перевода),
  (адрес_2, баланс + сумма_перевода).
- ***Уровень хранения данных – база данных*** **специального вида, которая поддерживается совместными усилиями всех узлов: собственно набор данных, описывающих состояние некоторого множества активов, и история операций с этими активами (транзакций).**
- ***Транспортный уровень – одноранговая (peer-to-peer) сеть*** **– сеть, состоящая из узлов (нод – node), в которой нет клиентов и серверов, все ноды равны (клиенты могут подключаться к нодам, но они не являются участниками сети).**

Система распределенного реестра как одноранговая сеть

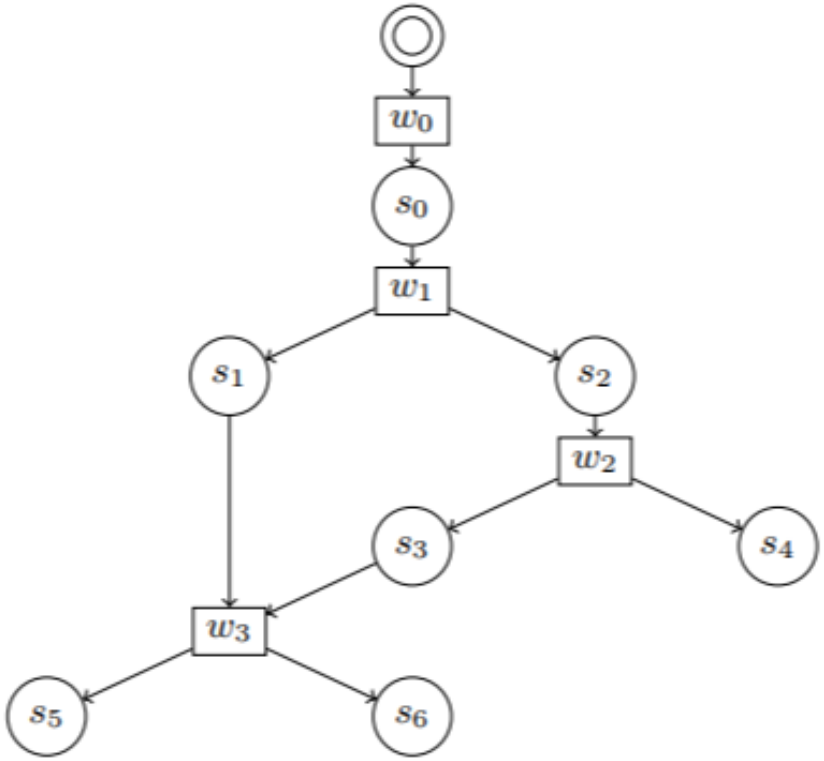


Система распределенного реестра как база данных

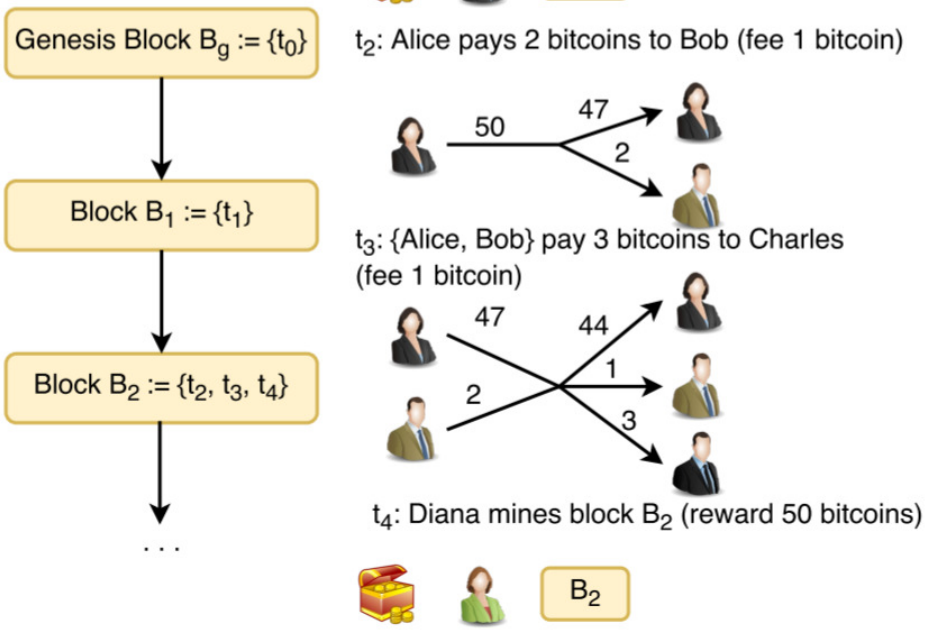
Реляционные базы данных

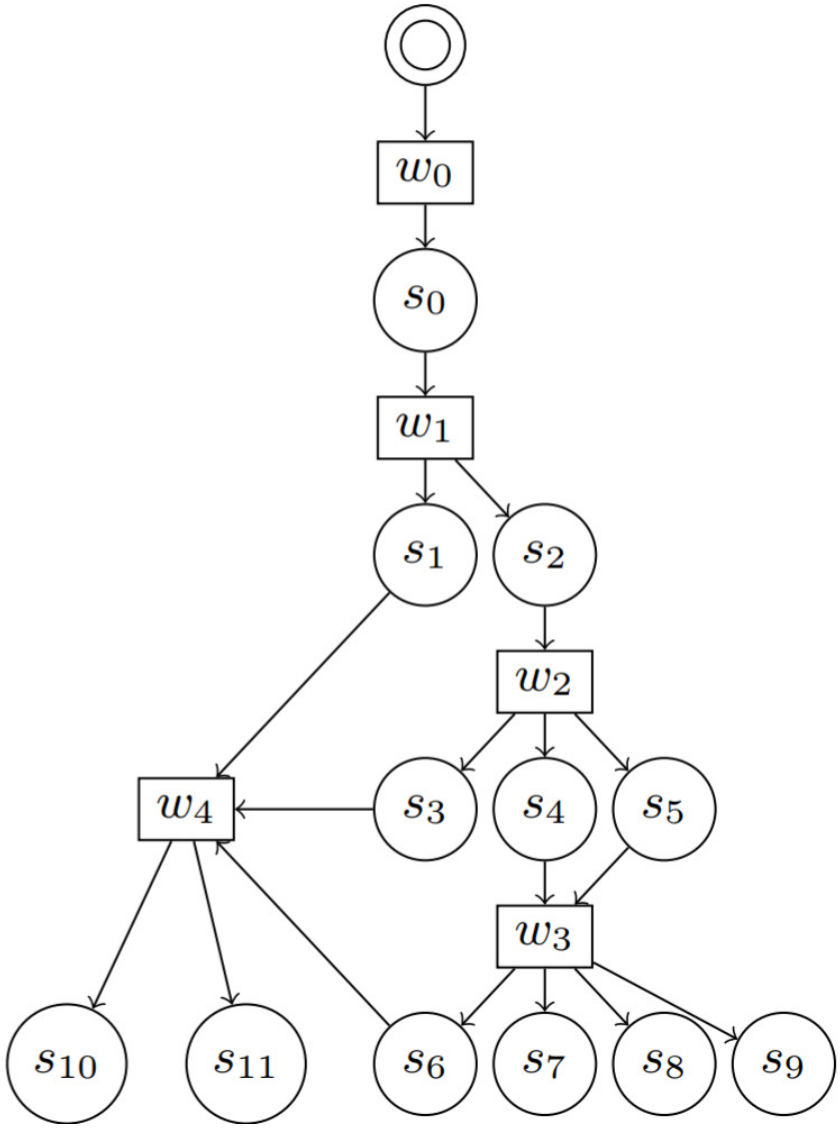
Столбец 1	Столбец 2	...	Столбец N
Запись 1			
Запись 2			
Запись 3			
...			
Запись M			

Распределенный реестр – ациклический ориентированный граф



Пример графа для платформы Bitcoin





Представление графа

Пример 1: **Bitcoin - на каждой ноде хранится копия всей истории транзакций от первого блока до текущего момента времени. Балансы адресов хранятся только в кошельках пользователей – на нодах они не хранятся.**

Пример 2: **Hyperledger Fabric – на каждой ноде хранится копия базы данных типа «ключ-значение», описывающая текущее состояние всех активов (т.е. все «несгоревшие» вершины графа) и копия всей истории транзакций от первого блока до текущего момента времени.**

Каждая транзакция подписывается *электронной цифровой подписью*, чтобы можно было точно установить, кто её автор.

Транзакции собираются в блоки, блоки в цепочку, цепочка связана *хэш-функцией*. Почему транзакции собирают в блоки? Блокчейн - высоконагруженная система, майнинг блоков более выгоден, чем майнинг отдельных транзакций, хотя размер блока можно сократить до 1 транзакции на блок. В то же время пользователь не может ждать бесконечно, поэтому формирование новых блоков должно происходить с приемлемой для пользователя частотой.

Нельзя просто так записать блок – для этого ноды должны достичь *консенсуса*!

Платформа Ethereum

- **Проект некоммерческой организации Ethereum Foundation, основатель – Виталик Бутерин**
- **Открытый блокчейн, использует метод «доказательства работой» (майнинг), планируется переход на «доказательство долей»**
- **Внешняя криптовалюта – эфир, внутренняя – газ (обеспечивает вознаграждение майнерам)**
- **Первая блокчейн-платформа, которая стала поддерживать смарт-контракты, обеспечивает Тьюринг-полные вычисления**

  Полнота по Тьюрингу — характеристика исполнителя (множества вычисляющих элементов) в теории вычислимости, означающая возможность реализовать на нём любую вычислимую функцию. Другими словами, для каждой вычислимой функции существует вычисляющий её элемент (например, машина Тьюринга) или программа для исполнителя, а все функции, вычисляемые множеством вычислителей, являются вычислимыми функциями (возможно, при некотором кодировании входных и выходных данных).
- **Большое количество приложений, специализированные языки программирования смарт-контрактов (самый употребительный - Solidity)**
- **Не решены проблемы информационной безопасности**

Ссылки:

www.ethereum.org

http://gavwood.com/paper.pdf

Платформа Hyperledger Fabric

- **Проект фонда Linux Foundation, основной разработчик – IBM**
- **Закрытый блокчейн, для достижения консенсуса использует протоколы византийского соглашения, не требует криптовалюты**
- **Поддерживает исполнение чейнкода (аналог смарт-контрактов), написанного на языке программирования Go**
- **Единственная блокчейн-платформа, которая *поддерживает исполнение вероятностных (недетерминированных) алгоритмов*, т.е. на ней могут исполняться действительно любые программы**
- **Конфиденциальность транзакций обеспечивается механизмом каналов, однако в текущей версии (1.0) не поддерживаются кросс-канальные коммуникации**
- **Хорошо подходит для логистических приложений (управление цепочками поставок, отслеживание происхождения товаров), плохо подходит для финансовых приложений**

Ссылки:
http://hyperledger.org/projects/fabric

Платформа Corda

- **Проект консорциума R3**
- **Закрытый блокчейн, используются протоколы консенсуса, не требует криптовалюты**
- ***Ориентирован на финансовые приложения*: встроен механизм поддержки нескольких типов цифровых активов, поддерживаются сервисы третьей стороны (нотариальные сервисы и пр.)**
- **Поддерживается исполнение бизнес-логики приложений (аналог смарт-контрактов) на языке программирования Kotlin**
- **Конфиденциальность транзакций обеспечивается посредством распространения информации в сети по принципу «только тому, кому она действительно нужна», содержимое всех транзакций шифруется**

Ссылки:
https://www.corda.net/

Платформа Quorum

- **Проект американского финансового холдинга JPMorgan Chase и компании Microsoft**
- **Закрытый блокчейн, построенный на базе блокчейн-клиента Ethereum, в котором механизм «доказательства работой» заменён на протокол консенсуса Raft, не требует криптовалюты**
- **Ориентирован на финансовые приложения, есть опыт внедрения приложений центральными банками нескольких стран (Канада, Сингапур, Франция)**
- **Поддерживается исполнение смарт-контрактов, обеспечивается полная совместимость с платформой Ethereum на уровне виртуальной машины EVM**
- **Конфиденциальность транзакций обеспечивается посредством специальной «надстройки» для шифрования информации – Constellation, а также протоколов доказательства с нулевым разглашением (zk-SNARKs) – *самый передовой подход к безопасности!***

Ссылки:

https://www.jpmorgan.com/global/Quorum

Функции криптографии в блокчейн-платформах

Функция	Способ реализации
Связывание транзакций в блоки	Криптографическая хэш-функция
Связывание блоков в цепочку	Криптографическая хэш-функция
Подписание транзакций	Электронная цифровая подпись
Формирование адресов кошельков из ключей электронной цифровой подписи	Криптографическая хэш-функция
Консенсус в открытом блокчейне	Криптографическая хэш-функция
Консенсус в закрытом блокчейне	Протоколы византийского соглашения
Обеспечение конфиденциальности транзакций (не во всех блокчейн-платформах)	Шифрование, доказательства с нулевым разглашением (zk-SNARKs, zk-STARKs)

Хэш-функция нужна в любом блокчейне, вне зависимости от его типа (permissionless/permissioned)

- **Чтобы связать блоки в цепочку**
- **Чтобы связать в дерево транзакции внутри одного блока – дерево Меркле (Merkle tree)**

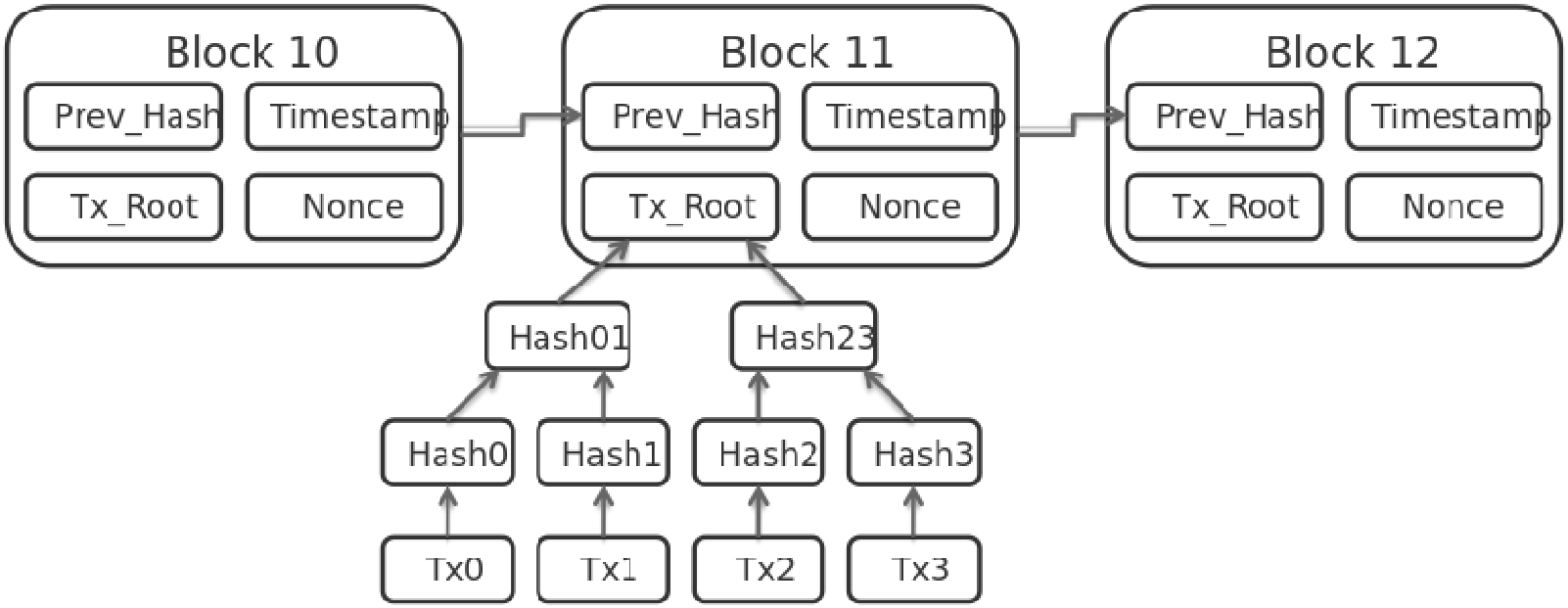


Схема генерации ключей электронной цифровой подписи и формирования адреса кошелька