МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ Н.Э. БАУМАНА
(НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)

Методы хранения данных с защитой от неправомерного доступа

Студент: Пересторонин Павел Геннадьевич
Группа: ИУ7-73Б
Руководитель: преподаватель кафедры ИУ7
Александр Сергеевич Григорьев

МОСКВА, 2021 ГОД

Цель и задачи

Цель — рассмотреть существующие методы хранения информации с защитой от неправомерного доступа.

Задачи:

- описать способы защиты информации от неправомерного доступа;
- рассмотреть базовые элементы и понятия, используемые при проектировании методов хранения информации с возможностью защиты от неправомерного доступа;
- провести анализ существующих методов хранения информации с защитой от неправомерного доступа.

Способы защиты информации

Можно выделить 3 уровня защиты от неправомерного доступа:

1. отсутствие возможности неправомерного доступа;
2. наличие возможности устранения последствий неправомерного доступа;
3. наличие возможности доказательства неправомерного доступа.

Способы защиты информации

Основные операции при работе с хранилищем данных:

- чтение;
- изменение;
- удаление;
- частичное изменение (при наличии резервного копирования или репликации);
- частичное удаление (при наличии резервного копирования или репликации).

Способы защиты информации

Таким образом при построении метода хранения данных можно выделить следующие возможные методы защиты информации от неправомерного доступа:

- исключение неправомерного чтения;
- исключение неправомерного изменения;
- исключение неправомерного удаления;
- возможность устраненения последствий частичного неправомерного удаления;
- возможность устраненения последствий частичного неправомерного изменения;
- доказательство неправомерного удаления;
- доказательство неправомерного изменения.

Способы защиты информации

Можно выделить 3 уровня защиты от неправомерного доступа:

1. обеспечение невозможности неправомерного доступа;
2. обеспечение возможности устранения последствий неправомерного доступа;
3. обеспечение возможности доказательства неправомерного доступа.

Базовые понятия

Можно выделить 3 базовых понятия, которые используются в построении методов хранения с обеспечением защиты от неправомерного доступа:

1. хэш-функция;
2. блокчейн;
3. дерево и ациклический граф Меркла.

Хэш-функция

Хэш-функция — функция, осуществляющая преобразование массива входных данных произвольной длины в выходную битовую строку установленной длины, выполняемое определенным алгоритмом.

Свойства:

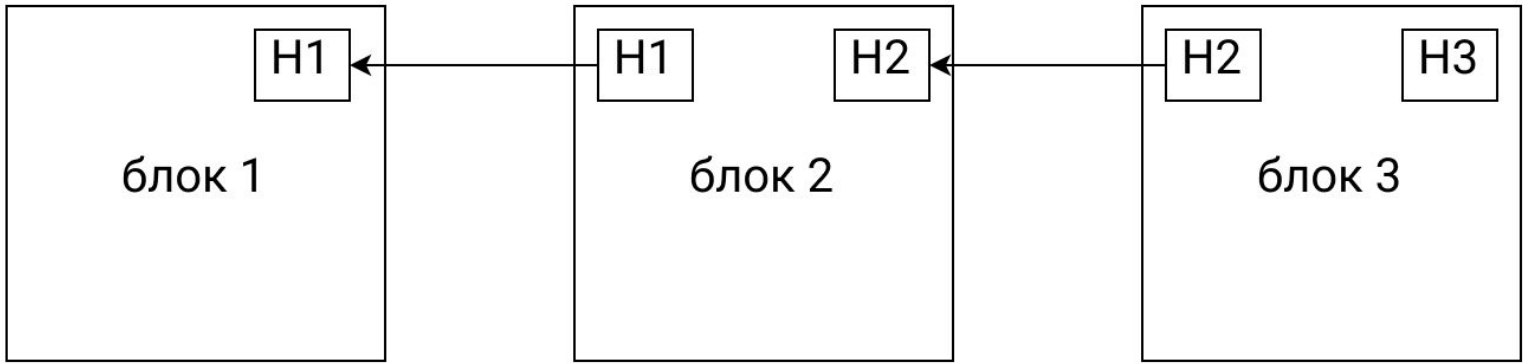
- используется для расчета контрольных сумм;
- при использовании криптографически стойкой хэш-функции для расчета контрольных сумм цена атаки ниже ценности данных.

Блокчейн

Блокчейн — выстроенная по определенным правилам непрерывная по следовательная цепочка блоков — элементов, содержащих информацию. В общем случае такая цепочка поддерживает 2 операции:

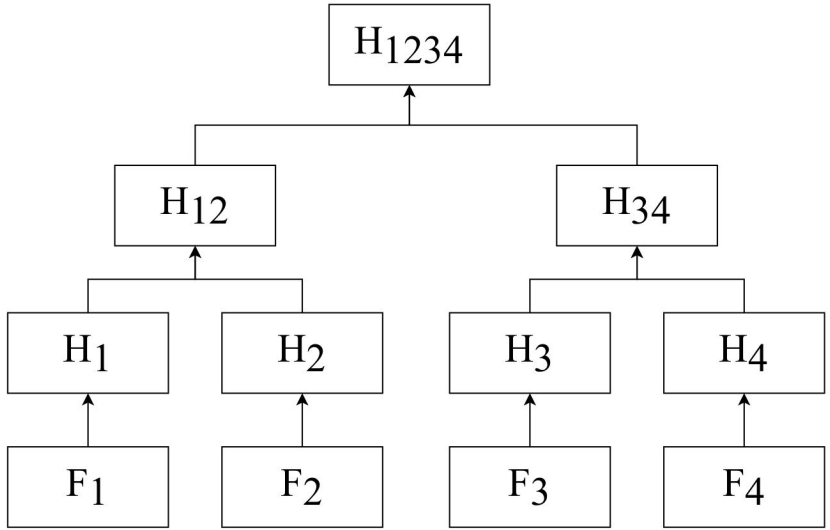
1. добавление нового элемента в конец цепочки;
2. проверка целостности всей цепочки.

Блокчейн



Дерево Меркла

Дерево Меркла — двоичное дерево, в листовые вершины которого по мещены хэши блоков данных, а внутренние вершины содержат хэши суммы значений в дочерних вершинах.



PASIS

Система хранения данных на N серверах, называемых узлами.

Применяемые методы защиты:

- распределенная система;
- стирающие коды (возможность восстановления данных из любых m фрагментов (при общем числе фрагментов N, N > m));
- объединенные контрольные суммы (возможность контроля корректности данных в целом).

Криптографические файловые системы

Реализуется как дополнительный слой шифрования между ВФС и драйвером файловой системы.

Свойства:

- использование шифрования с ключом;
- без наличия ключа прочитать данные или записать нужные данные в нужную ячейку невозможно;
- возможно повредить данные записью при доступе к устройству напрямую (не через драйвер).

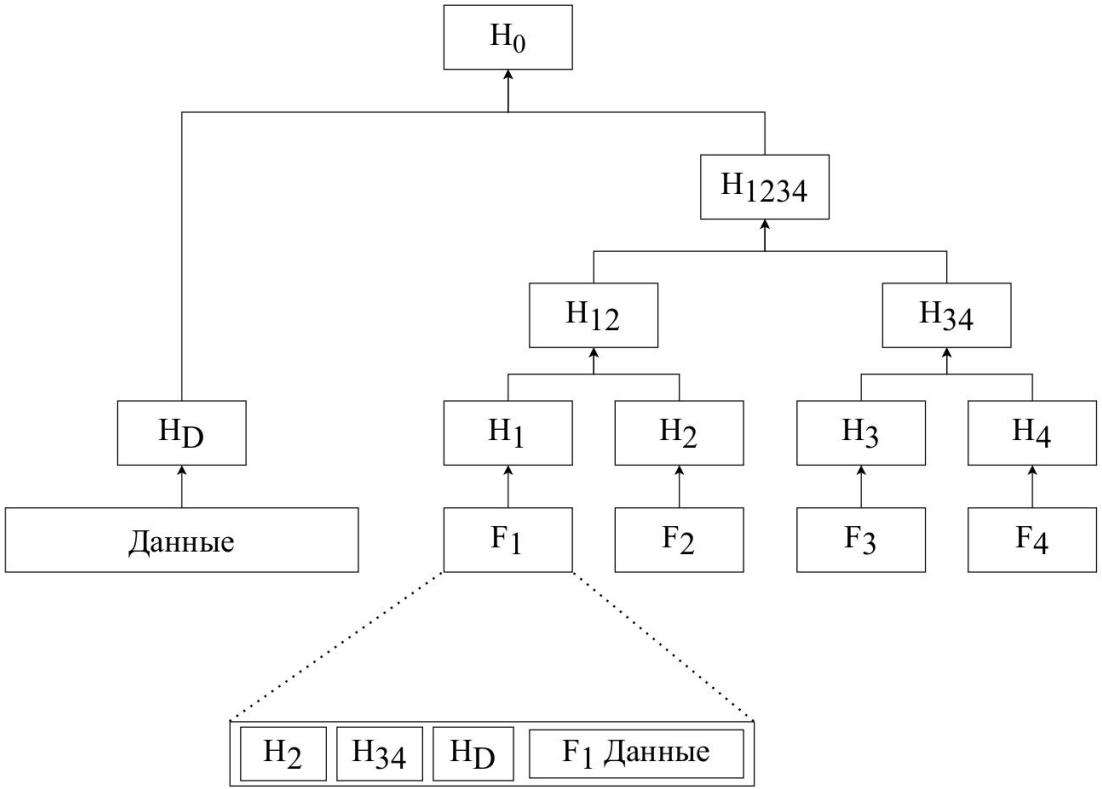
OceanStore

Система хранения данных на N серверах, называемых узлами.

Отличия от PASIS:

- валидация не только целых данных, но и фрагментов;
- имя ресурса — контрольная сумма от его содержимого;
- контрольная сумма в формате дерева Меркла;
- не поддерживает изменение данных.

OceanStore


H0
H1234
H12
H34
HD
H1
H2
H3
H4
Данные
F1
F2
F3
F4
H2
H34
HD
F1 Данные

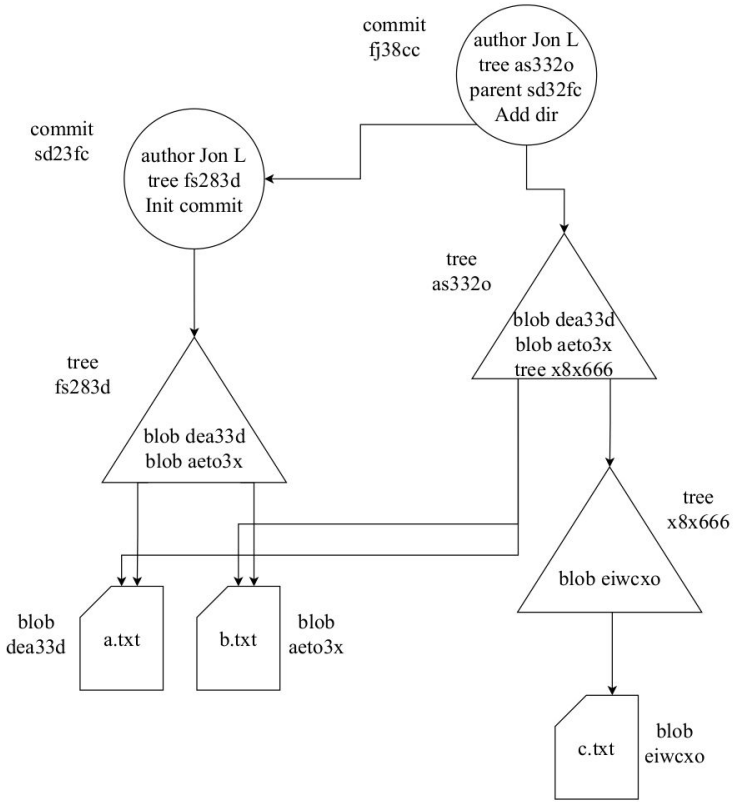
Git

Система версионного контроля.

Свойства:

- контроль целостности с помощью контрольных сумм;
- внутренняя структура в формате ациклического направленного графа Меркла;
- иерархическая структура поверх ассоциативного массива;

Git


commit
fj38cc
author Jon L
tree as332o
parent sd32fc
Add dir
commit
sd23fc
author Jon L
tree fs283d
Init commit
tree
as332o
blob dea33d
blob aeto3x
tree x8x666
tree
fs283d
blob dea33d
blob aeto3x
tree
x8x666
blob eiwcxo
blob
dea33d
a.txt
b.txt
blob
aeto3x
c.txt
blob
eiwcxo

Bitcoin

Bitcoin — одноранговая децентрализованная система электронных транзакций.

Свойства:

- использование PKI на уровне транзакций;
- использование корня дерева Меркла в качестве контрольной суммы на уровне набора транзакций в блоке;
- использование концепта proof-of-work на уровне блоков;
- использование блокчейна для контроля целостности цепочки блоков (состояния системы).

Заключение

Сокращения:

- НД — неправомерное действие;
- КФС — криптографические файловые системы;
- ЧУ — частичное удаление;
- УЗ — уровень защиты;
- ЧИ — частичное изменение.

Заключение

НД (УЗ)	PASIS	КФС	OceanStore	Git	Bitcoin
чтение (исключение)	-	+	-	-	-
ЧУ или ЧИ (восстановление)	+	-	+	-	-
изменение (исключение)	-	-	-	-	+
удаление (исключение)	-	-	-	-	+
изменение (доказательство)	+	-	+	+/-	+
удаление (доказательство)	-	-	-	+/-	+

Заключение

В ходе выполнения данной работы:

1. были описаны способы защиты информации от неправомерного доступа;
2. были рассмотрены базовые элементы и понятия, используемые при проектировании методов хранения информации с возможностью защиты от неправомерного доступа;
3. был проведен анализ существующих методов хранения информации с защитой от неправомерного доступа.

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ Н.Э. БАУМАНА (НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)

МОСКВА, 2021 ГОД