

**MANAGEMENT AND ECONOMICS
SCIENTIFIC RESEARCH JOURNAL**

**MENEJMENT VA IQTISODIYOT
ILMIY-TADQIQOT JURNALI**

**НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ЖУРНАЛ
МЕНЕДЖМЕНТА И ЭКОНОМИКИ**



MANAGEMENT AND ECONOMICS SCIENTIFIC RESEARCH JOURNAL

☎ +998 95 651 90 00

✉ journals@timeedu.uz

📍 Shota Rustaveli ko'chasi, 114

🌐 tmijournals.ndc-agency.uz

✈ @TMII_ilmiy_bolim

Bosh muharrir:

Narbayev Sharafatdin Kengeshovich

Bosh muharrir o'rinbosari:

Nosirova Nargiza Jamoliddin qizi

Muharrir:

Qarshiyeva Shahnoza Davlatovna

Tahrir hay'ati:

1. Sharipov Kongratbay Avezimbetovich – O'zbekiston Respublikasi Oliy ta'lim, fan va innovatsiyalar vaziri, t.f.d., prof.;
2. Axmedov Xojiakbarxon Dilshatovich – Toshkent menejment va iqtisodiyot instituti rektori i.f.n., dotsent;
3. Gulyamov Saidasror Saidaxmedovich – O'zbekiston Fanlar akademiyasi akademigi, i.f.d, professor;
4. Gulyamov Saidaxror Saidaxmedovich – O'zbekiston Fanlar akademiyasi akademigi i.f.d, professor;
5. Sultanov Mansur Qilichovich – Oliy ta'lim, fan va innovatsiyalar vazirligi huzuridagi "Inno" innovatsion o'quv-ishlab chiqarish texnoparki bosh direktori, t.f.f.d., dotsent;
6. Chertovitskiy Aleksandr Stepanovich - „Toshkent irrigatsiya va qishloq xo'jaligini mexanizatsiyalash muxandislari instituti“ Milliy tadqiqot universiteti professori, iqtisodiyot fanlari doktori;
7. Popkova Yelena Gennadyevna - Rossiya Federatsiyasi avtonom notijorat tashkiloti "Ilmiy kommunikatsiyalar instituti" prezidenti, iqtisodiyot fanlari doktori, professor;
8. Dr Goh Khang Wen – Malaziyaning INTI Xalqaro universiteti prorektori;
9. Wang Cheng – XXR "Hebei Institute of Mechanical and Electrical Technology" instituti i.f.f.d., dotsent;
10. Yo'ldoshev Nuriddin Qurbonovich – Toshkent menejment va iqtisodiyot instituti Biznes boshqaruvi va moliya kafedrasini i.f.d., professor;
11. Akramov Tohir Abdirahmonovich Toshkent menejment va iqtisodiyot instituti Biznes boshqaruvi va moliya kafedrasini i.f.d., professor;
12. Temirov Abdulaziz Alimjonovich – Toshkent menejment va iqtisodiyot instituti Biznes boshqaruvi va moliya kafedrasini i.f.n., professor;
13. Rajabov Nazirjon Razzaqovich – Toshkent menejment va iqtisodiyot instituti Iqtisodiyot kafedrasini mudiri, i.f.n., dotsent;
14. Xotamov Ibodullo Sadulloyevich – Toshkent menejment va iqtisodiyot instituti Iqtisodiyot kafedrasini i.f.n., professor;
15. Sobirov Aziz Avazbekovich – Toshkent menejment va iqtisodiyot instituti Biznes boshqaruvi va moliya kafedrasini mudiri, i.f.f.d., dotsent;
16. Raximova Shahlo Baxtiyorovna – Ta'lim sifatini nazorat qilish bo'limi boshlig'i, p.f.f.d., dotsent;
17. Kadirova Istora Bobirovna – Toshkent menejment va iqtisodiyot instituti Karyera markazi direktori, i.f.f.d.;
18. Turakulov Otabek Xolmirzayevich – Toshkent menejment va iqtisodiyot instituti Muhandislik va axborot texnologiyalari kafedrasini mudiri, t.f.f.d.

MUHANDISLIK OYLIGI

“RAQAMLI TEXNOLOGIYALARNI RIVOJLANTIRISH VA INNOVATSION MUHANDISLIK YECHIMLARI: ZAMONAVIY TENDENSIYALAR VA ISTIQBOLLAR” MAVZUSIDA RESPUBLIKA ILMIY-AMALIY ANJUMANI TO‘PLAMI MATERIALLARI

17-18 APREL, 2025

TOSHKENT

ПОСТРОЕНИЕ ДЕРЕВА МЕРКЛА

Мухамедиева Д.К.

*Ташкентский университет информационных технологий имени
Мухаммада ал-Хоразмий*

Annotatsiya. Maqolada blokcheyn texnologiyasining muhim komponenti sifatida Merkle daraxtini qurish tamoyili muhokama qilinadi. Merkle daraxtini yaratish algoritmi, uning tranzaktsiyalarni tekshirish va blokcheyn tarmog'ining ishlashini optimallashtirishdagi roli tasvirlangan. Python-da blokcheynning minimal amalga oshirilishi, shu jumladan Merkle daraxtini yaratish va ko'rsatish funktsiyalari taqdim etilgan. Tranzaktsiyalarning blokga kiritilishini tekshirish va taqsimlangan tarmoqda ma'lumotlar yaxlitligini ta'minlash uchun ushbu yondashuvning samaradorligi ko'rsatilgan.

Kalit so'zlar: Blokcheyn, Merkle daraxti, xesh funktsiyasi, tranzaktsiyalar, ma'lumotlarni tekshirish, Python, genezis bloki, kriptografiya, taqsimlangan tizimlar.

Abstract. The article discusses the principle of constructing a Merkle tree as an important component of blockchain technology. The algorithm for creating a Merkle tree, its role in verifying transactions and optimizing the operation of a blockchain network are described. A minimal implementation of a blockchain in Python is presented with the inclusion of functions for creating and displaying a Merkle tree. The effectiveness of this approach for checking the inclusion of transactions in a block and ensuring data integrity in a distributed network is demonstrated.

Keywords: Blockchain, Merkle tree, hash function, transactions, data verification, Python, genesis block, cryptography, distributed systems.

Аннотация. В статье рассматривается принцип построения дерева Меркла как важного компонента блокчейн-технологии. Описан алгоритм создания дерева Меркла, его роль в верификации транзакций и оптимизации работы блокчейн-сети. Представлена минимальная реализация блокчейна на языке Python с включением функций для создания и отображения дерева Меркла. Продемонстрирована эффективность данного подхода для проверки включения транзакций в блок и обеспечения целостности данных в распределенной сети.

Ключевые слова: Блокчейн, дерево Меркла, хеш-функция, транзакции, верификация данных, Python, генезисный блок, криптография, распределенные системы.

При помощи дерева Меркла можно легко убедиться включена ли конкретная транзакция в данный блок, тем самым удешевляя данный процесс как технически, так и финансово, для пользователей самой сети. Так как каждый следующий блок транзакций

ссылается на предыдущий то зная текущий блок можно с легкостью считать все транзакции с сети, продолжая следовать по цепочке блоков до самого первого, который называется – генезисный блок. Построение дерева Меркла показано на рисунке 1.

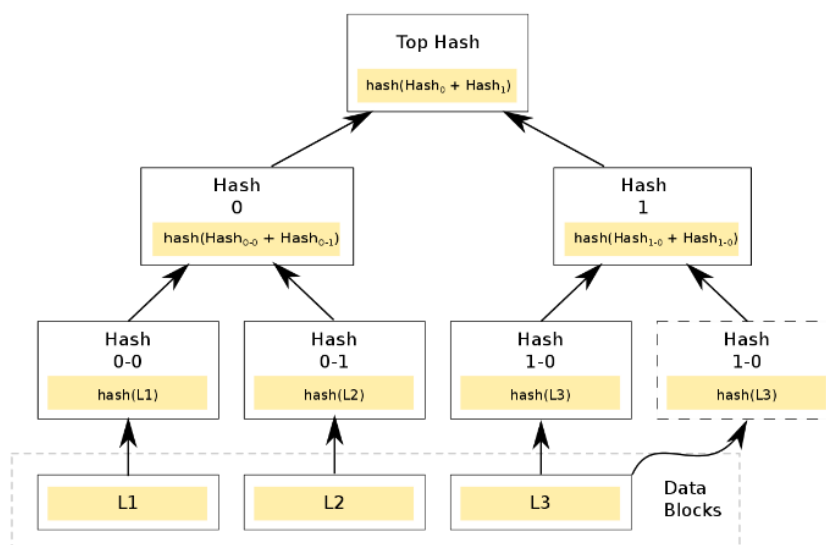


Рисунок 1. Дерево Меркла

Алгоритм построения дерева Меркла:

1. Вычисляются хеши каждой транзакции, находящийся в блоке: $\text{hash}(L1)$, $\text{hash}(L2)$ и т.д.

2. Вычисляются хеши от суммы хешей транзакций: $\text{hash}(\text{hash}(L1) + \text{hash}(L2))$. Число элементов на каждой итерации должно быть четным, так как дерево является бинарным. Если блок содержит нечетное количество транзакций, то последняя дублируется и складывается сама с собой;

3. Второй пункт происходит до тех пор, пока не будет высчитан единый хэш, который и является корнем дерева Меркла.

При помощи дерева Меркла можно легко убедиться включена ли конкретная транзакция в данный блок, тем самым удешевляя данный процесс как технически, так и финансово, для пользователей самой сети. Так как каждый

следующий блок транзакций ссылается на предыдущий то зная текущий блок можно с легкостью считать все транзакции с сети, продолжая следовать по цепочке блоков до самого первого, который называется – генезисный блок.

Создадим простую и минимальную блокчейн-реализацию на языке Python.

Результат:

Block #1 has been added to the blockchain!

Hash:

70f64d189467eb343a845db74a59d9c
0053e609eb382500f8a5de761aa9292
84

Block #2 has been added to the blockchain!

Hash:

640b702913f50d5664757c96845ddb
877bd167b50ca97d66c5b20b4f3654e
46a

Block #3 has been added to the blockchain!

Hash:

03ef6369a807716b5ea419961bbe6f3
c00ffb02c2a76744afda06780f17b3a6
2

Block #4 has been added to the
blockchain!

Hash:

cd4036a2578e699a8e827c6573f30c9
cc555e852019af59884c577871eac3b
4d

Block #5 has been added to the
blockchain!

Hash:

d6430d1034046e1ce220410bb9fff8da
fdfd7b3c98ffe285ef5dcc5bef43c1a6

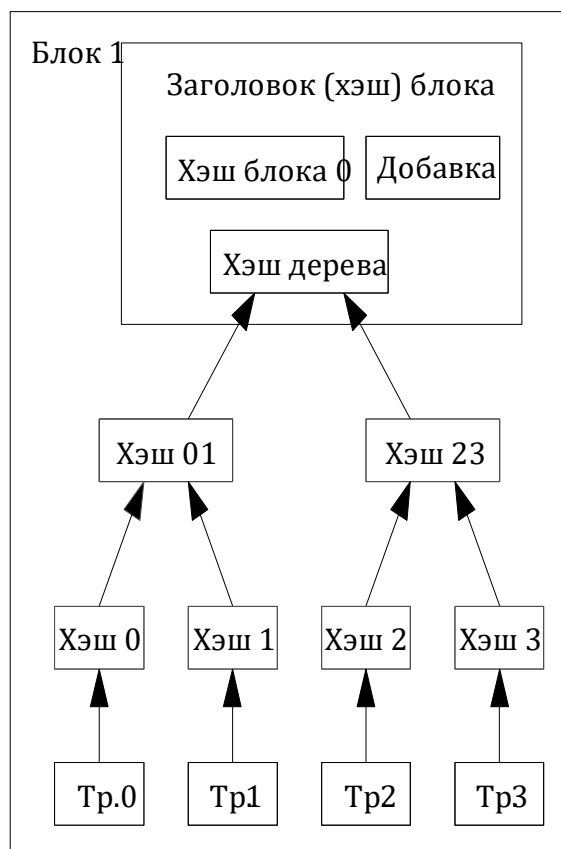
Этот код создает простую
цепочку блоков. Важные моменты:

Block представляет собой
блок в цепочке.

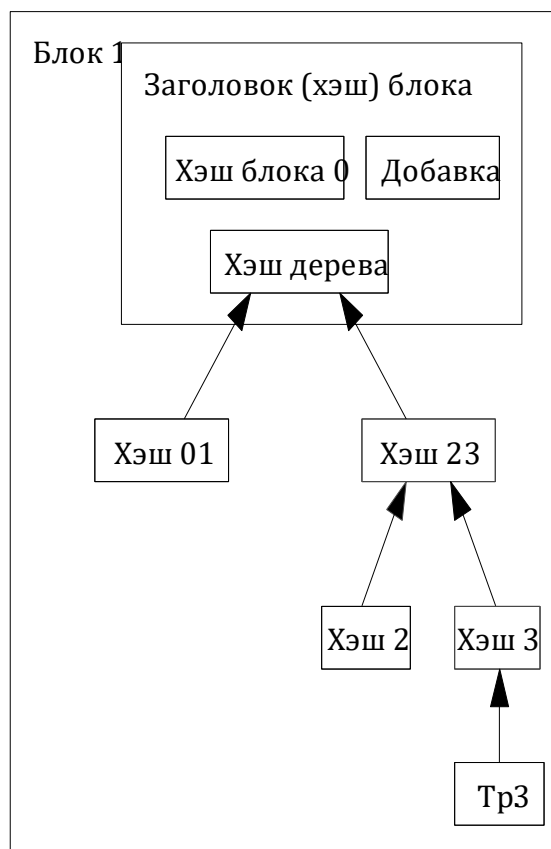
calculate_hash генерирует хэш
блока на основе его данных.

create_genesis_block создает
первый блок (генезис) в цепочке.

create_new_block создает
новый блок на основе предыдущего
блока и новых данных.



Все транзакции в дереве Меркле



После обрезки Тр.0-2 из Блока 1

Этот код добавляет функцию
merkle_tree для создания дерева
Меркле и display_merkle_tree для
отображения информации о дереве
Меркле в текстовом поле GUI. При

добавлении нового блока в
блокчейн, дерево Меркле
обновляется, и вывод в GUI также
обновляется.

Список использованной литературы:

1. Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). *Blockchain technology: Beyond bitcoin*. *Applied Innovation Review*, 2, 6–10.
2. Mougayar, W. (2016). *The Business Blockchain: Promise, Practice, and the Application of the Next Internet Technology*. Wiley.
3. Zhang, R., & Xue, R. (2019). *Security and Privacy on Blockchain*. *ACM Computing Surveys*, 52(3), Article 51.

Ingliz tili muharriri: Nosirova Nargiza Jamoliddin qizi
Musahhih: Vahobova Marfua Mirkamalovna
Sahifalovchi va dizayner: Zoirov Sardor Ziyodin o'g'li

1-maxsus son

© Materiallar ko'chirib bosilganda **"Management and Economics Scientific Research Journal"** jurnali manba sifatida ko'rsatilishi shart. Jurnalda bosilgan material va reklamalardagi dalillarning aniqligiga mualliflar ma'sul. Tahririyat fikri har vaqt ham mualliflar fikriga mos kelamasligi mumkin. Tahririyatga yuborilgan materiallar qaytarilmaydi.

Mazkur jurnalda maqolalar chop etish uchun quyidagi havolalarga maqola, reklama, hikoya va boshqa ijodiy materiallar yuborishingiz mumkin.
Materiallar va reklamalar pullik asosda chop etiladi.

El. pochta: journals@timeedu.uz

Tel.: [+998 95 651 90 00](tel:+998956519000)

"Management and Economics Scientific Research Journal" jurnali 19.09.2024-yildan O'zbekiston Respublikasi Prezidenti Adminstratsiyasi huzuridagi Axborot va ommaviy kommunikatsiyalar agentligi tomonidan 404368-son reyestr raqami tartibi bo'yicha ro'yxatdan o'tkazilgan. Litsenziya raqami: C-5669639
PNFL: 308906510

Manzilimiz: Toshkent shahar, Yakkasaroy tumani
Shota Rustaveli ko'chasi, 114