Date: 9th February-2026

MARKAZLASHMAGAN BLOKCHEYN TIZIMIDA SHIFRLASH ALGORITMLAR TADQIQI

Ahmadov Ulug‘bek Said o‘g‘li
Muxammad al – Xorazmiy nomidagi TATU “Kiberxavfsizlik va kriminalistika” kafedrasi stajyor o‘qituvchisi
Oripov Asilbek Baxtiyor o‘g‘li
Saidov Ozodbek Alisher o‘g‘li
Xayriddinov Shaxboz Shavkatovich
Muxammad al – Xorazmiy nomidagi TATU talabalari

Annotatsiya: Ushbu maqolada markazlashmagan blokcheyn tizimlarida qo‘llaniladigan asosiy kriptografik (shifrlash) algoritmlar va ularning ishlash prinsiplari tahlil qilinadi. Blokcheyn texnologiyasi ma’lumotlarning o‘zgarmasligi (immutability), yaxlitligi (integrity) va autentifikatsiyasini ta’minlash uchun zamonaviy kriptografik mexanizmlarga asoslanadi. Tadqiqot davomida xesh funksiyalar, ochiq va yopiq kalitli shifrlash (asymmetric cryptography), raqamli imzo algoritmlari hamda konsensus mexanizmlarida qo‘llaniladigan kriptografik usullar ko‘rib chiqiladi.

Kalt so‘zlar: Blokcheyn, kriptografiya, SHA-256, ECDSA, Keccak-256, raqamli imzo, ochiq kalit, yopiq kalit, xesh funksiya, konsensus algoritmi, ma’lumotlar yaxlitligi.

Kriptografiya blokcheyn texnologiyasining muhim tarkibiy qismi bo‘lib, tranzaktsiyalar xavfsizligini va blokcheynda saqlanadigan maxfiy ma’lumotlarning maxfiyligini ta’minlash uchun ishlatiladi. Kriptografiya ma’lumotlarni kodlash va dekodlash uchun matematik algoritmlardan foydalanadi, bu esa uni tegishli shifrlash kalitiga ega bo‘lganlardan tashqari hech kim o‘qib bo‘lmaydi. Bu blokcheynda saqlangan ma’lumotlarga ruxsatsiz kirish va manipulyatsiyani oldini olishga yordam beradi.

Kriptografiya turlari

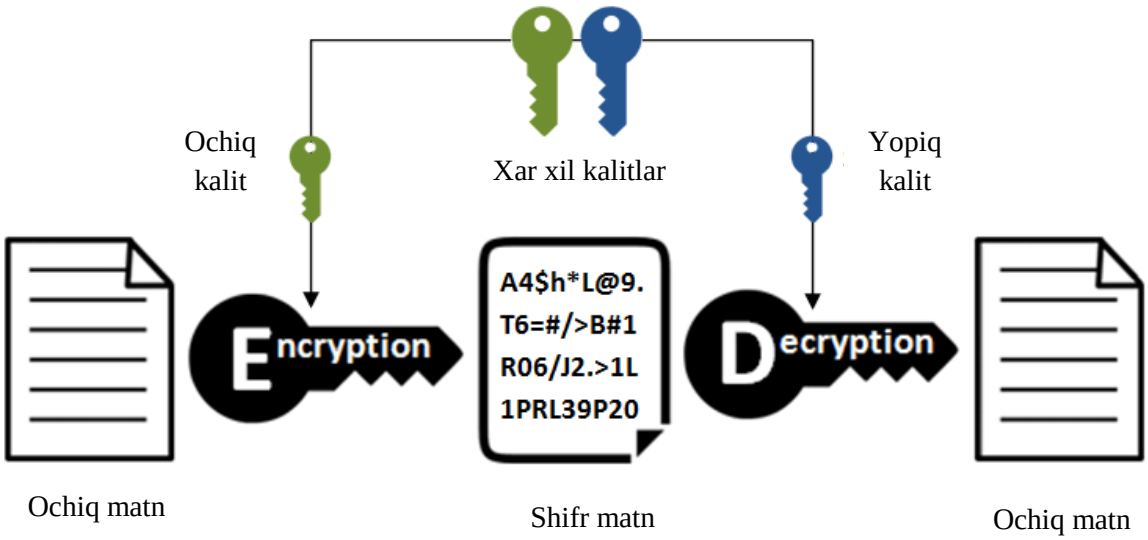
Blokcheyn texnologiyasida ishlatiladigan kriptografik algoritmlarning bir necha xil turlari mavjud, ular orasida simmetrik kalitli kriptografiya, assimetrik kalitli kriptografiya va xesh funksiyalari mavjud.

Simmetrik kalitli kriptografiya: Yashirin kalit kriptografiyasi deb ham ataladigan simmetrik kalitli kriptografiya ham shifrlash, ham shifrni ochish uchun bir xil kalitdan foydalanadi. Simmetrik kalitlar algoritmiga misol sifatida nozik ma’lumotlarni himoya qilish uchun keng qo‘llaniladigan Kengaytirilgan shifrlash standarti (AES) hisoblanadi.

Asimmetrik kalitli kriptografiya: Ochiq kalit kriptografiyasi sifatida ham tanilgan assimetrik kalitli kriptografiya shifrlash va shifrni ochish uchun ikki xil kalitdan foydalanadi. Shifrlash kaliti hamma uchun ochiq bo‘ladi, shifrni ochish kaliti esa maxfiy saqlanadi. Bu foydalanuvchilarga faqat mo‘ljallangan qabul qiluvchi tomonidan parolini hal qilish mumkin bo‘lgan xabarlarni shifrlash imkonini beradi. Asimmetrik kalitli algoritmga misol sifatida RSA algoritmini keltirish mumkin, u odatda xavfsiz aloqa va raqamli imzolar uchun ishlatiladi.

Blockchain-da kriptografiya

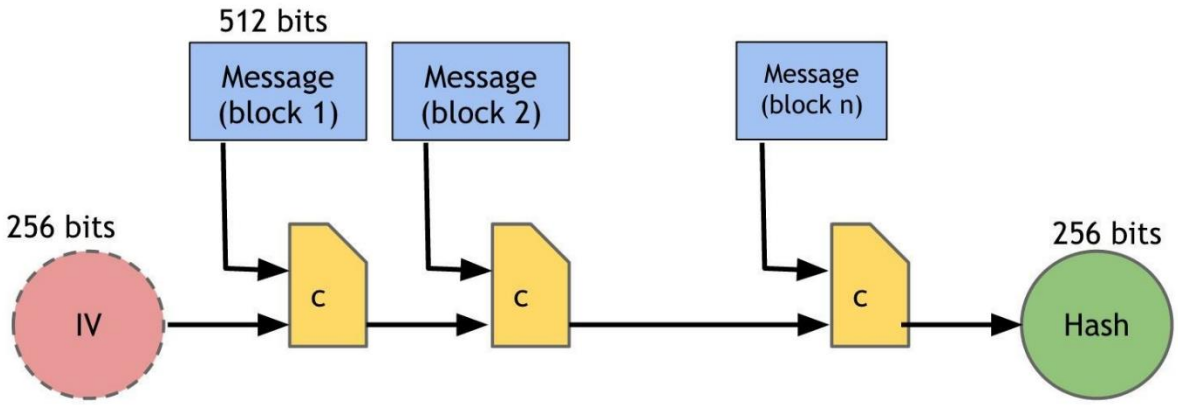
Blokcheynda eng ko‘p ishlatiladigan kriptografik usullar assimetrik kalitli kriptografiya va xesh funktsiyalari hisoblanadi. Raqamli imzolarni yaratish uchun assimetrik kalitli kriptografiya qo‘llaniladi, ular tranzaktsiyalarning haqiqiyligini isbotlash uchun ishlatiladi. Xesh funktsiyalari blokcheynda saqlangan ma’lumotlarning yaxlitligini ta’minlash va blok zanjirida bloklarni bir-biriga bog‘laydigan xeshlarni himoya qilish uchun ishlatiladi.



1.1-rasm. Assimmetrik shifrlash algoritmi

Blokcheyn dunyosida eng ko‘p ishlatiladigan kriptografik algoritmlarga SHA-256, Ethash va Elliptic Curve Digital Signature Algoritm (ECDSA) kiradi. SHA-256 ma’lumotlarni xeshlash va tekshirish uchun ishlatiladi, Ethash esa Ethereum blokcheynida qazib olish algoritmi sifatida ishlatiladi. Boshqa tomondan, ECDSA tranzaktsiyalarni ta’minlash va egalik huquqini tasdiqlovchi hujjatni taqdim etish uchun raqamli imzolar uchun ishlatiladi. Bundan tashqari, Advanced Encryption Standard (AES) ham tez-tez blokcheyndagi ma’lumotlarni shifrlash va dekodlash uchun ishlatiladi. Blokcheynda eng ko‘p ishlatiladigan kriptografiya algoritmi har bir blokcheyn tarmog‘ining o‘ziga xos qo‘llanilishi va talablariga bog‘liq.

SHA-256, shuningdek, Secure Hash Algoritm 256-bit nomi bilan ham tanilgan, blokcheyn texnologiyasida keng qo‘llaniladigan kriptografiya algoritmidir. Bu har qanday uzunlikdagi har qanday kirishni qabul qiladigan va 256 bitlik qattiq uzunlikdagi chiqishni ishlab chiqaradigan xesh funksiyasi. Ushbu algoritm blokcheyn-da turli maqsadlarda, jumladan, ma’lumotlarning yaxlitligini tekshirish, xavfsiz raqamli imzolar va tranzaktsiyalarni tasdiqlash uchun ishlatiladi.



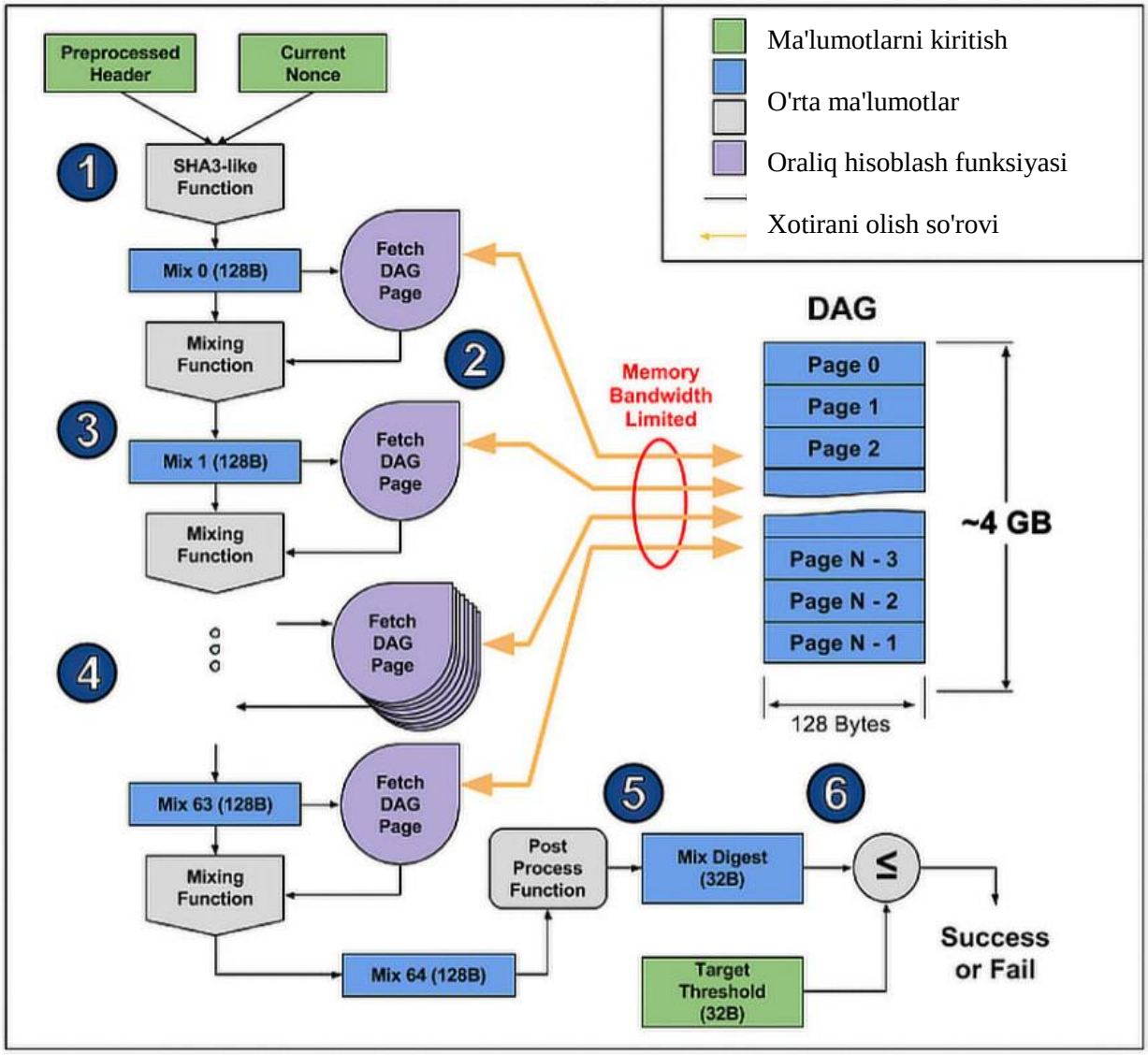
1.2-rasm. SHA-256 hesh algoritmi

SHA-256 bir tomonlama funktsiyadir, ya'ni xesh funktsiyasi jarayonini teskari hisoblash va xeshli chiqishdan asl kirishni olish hisoblash mumkin emas. Bu SHA-256 ni blokcheyndagi ma'lumotlarning xavfsizligi va maxfiyligini ta'minlash uchun muhim vositaga aylantiradi. Bundan tashqari, kiritilgan ma'lumotlarning har qanday o'zgarishi butunlay boshqacha xesh qiymatiga olib keladi, bu esa dastlabki ma'lumotlarga har qanday o'zgartirish yoki o'zgarishlarni aniqlashni osonlashtiradi.

SHA-256 ning yana bir muhim xususiyati uning to'qnashuvga chidamliligidir. Ikki xil kirish bir xil xesh qiymatini hosil qilganda, xesh to'qnashuvi sodir bo'ladi. Blockchain-da bu xavfsizlikning sezilarli zaifliklariga olib kelishi mumkin, chunki bu tajovuzkorga asl ma'lumotlarni shunday o'zgartirishi mumkinki, u hali ham bir xil xesh qiymatini yaratadi. SHA-256 algoritmi to'qnashuvga chidamli bo'lib ishlab chiqilgan bo'lib, uni blokcheyn ilovalarida foydalanish uchun xavfsiz variantga aylantiradi.

Ethash

Ethash - bu Ethereum blokcheyn tarmog'ida ishlatiladigan Proof of Work (PoW) qazib olish algoritmi. U ASIC-ga chidamli bo'lishi uchun ishlab chiqilgan, ya'ni u maxsus kon uskunalaridan farqli o'laroq, oddiy kompyuter yoki grafik karta bilan qazib olinishi mumkin bo'lgan ma'noda yanada demokratik bo'lishga mo'ljallangan. Bu tog'-kon mukofotlarini tarmoq ishtirokchilari o'rtasida teng ravishda taqsimlashga va markazlashuvning oldini olishga yordam beradi.



1.3-rasm. Ethash algoritmi

Ethashning asosiy xususiyatlaridan biri bu har bir davr uchun (30 000 blok) ishlab chiqariladigan va qazib olish uchun asos bo‘lib xizmat qiluvchi DAG (yo‘naltirilgan asiklik grafik) dan foydalanishdir. DAG xotirada saqlanadi va qazib olish jarayoni uchun kirish sifatida ishlatiladi, bu blok sarlavhasi bilan birlashganda kerakli qiyinchilik maqsadiga javob beradigan xesh qiymatiga olib keladigan nonce (tasodifiy raqam) topishni o‘z ichiga oladi. Yechimni birinchi bo‘lib topgan konchi Ethereum tarmog‘ida ishlatiladigan kriptovalyuta Eter bilan taqdirlanadi.

Ethash-da DAG-dan foydalanish konchilik jarayonini xotirani qattiqroq qilishga yordam beradi, bu esa Ethereum qazib olish uchun maxsus apparat (ASIC) ishlab chiqishda qiyinchiliklarni oshiradi. Bu tarmoqni markazsizlashtirishni saqlab qolish va qazib olish quvvatining bir nechta shaxslar yoki tashkilotlarning qo‘lida kontsentratsiyasini oldini olishga yordam beradi. Bundan tashqari, Ethash shuningdek, kon qazish jarayonida tasodifiylikni ta’minlaydi, bu konchilar uchun natijalarni bashorat qilishni va qazib olish ishlarini optimallashtirishni qiyinlashtiradi.

XULOSA

Xulosa qilib aytganda, markazlashmagan blokcheyn tizimlarida shifrlash algoritmlari asosiy xavfsizlik mexanizmi hisoblanadi. Xesh funksiyalar bloklarning o‘zgarmasligini ta’minlaydi, ochiq va yopiq kalitli kriptografiya esa tranzaksiyalarni xavfsiz amalga oshirish imkonini beradi.

Bitcoin va Ethereum kabi tizimlarda qo‘llaniladigan SHA-256, Keccak-256 va ECDSA algoritmlari blokcheyn xavfsizligining fundamental asosini tashkil etadi. Kelajakda kvant kompyuterlar rivojlanishi bilan post-kvant kriptografiya algoritmlarini joriy etish dolzarb masalaga aylanishi mumkin.

Shu sababli blokcheyn tizimlarida kriptografik algoritmlarni chuqur o‘rganish va ularni takomillashtirish axborot xavfsizligini ta’minlashda muhim ahamiyat kasb etadi.

ADABIYOTLAR RO‘YXATI:

1. Castells, M. *The Rise of the Network Society*. Oxford: Blackwell Publishers, 2010.
2. Boyd, D., Ellison, N. Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication*, 2007.
3. Wasserman, S., Faust, K. *Social Network Analysis: Methods and Applications*. Cambridge University Press, 1994.
4. Kaplan, A.M., Haenlein, M. Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons*, 2010.
5. O‘zbekiston Respublikasi “Axborotlashtirish to‘g‘risida”gi Qonuni.
6. O‘zbekiston Respublikasi “Axborot erkinligi prinsiplari va kafolatlari to‘g‘risida”gi Qonuni.