ТӘУЕЛСІЗДІК ЖЫЛДАРЫ ҚАЗАҚСТАН

РУХАНИ ЖАҢҒЫРУ

Фараби оқулары

Қазақстан 2050

ӘЛ-ФАРАБИ АТЫНДАҒЫ ҚАЗАҚ ҰЛТТЫҚ УНИВЕРСИТЕТІ
КАЗАХСКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ ИМЕНИ АЛЬ-ФАРАБИ
AL-FARABI KAZAKH NATIONAL UNIVERSITY

АҚПАРАТТЫҚ ТЕХНОЛОГИЯЛАР ФАКУЛЬТЕТІ
ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
FACULTY OF INFORMATION TECHNOLOGY

«ФАРАБИ ӘЛЕМІ»

атты студенттер мен жас ғалымдардың
халықаралық ғылыми конференция

МАТЕРИАЛДАРЫ

Алматы, Қазақстан, 6-8 сәуір 2021 жыл

МАТЕРИАЛЫ

международной научной конференции
студентов и молодых ученых

«ФАРАБИ ӘЛЕМІ»

Алматы, Казахстан, 6-8 апреля 2021 года

MATERIALS

International Scientific Conference
of Students and Young Scientists

«FARABI ALEMI»

Almaty, Kazakhstan, April 6-8, 2021

P2P ЭЛЕКТРОНДЫҚ ТӨЛЕМ ЖҮЙЕСІНДЕ ПАЙДАЛАНУШЫЛАРДЫҢ ҚҰПИЯЛЫЛЫҒЫН САҚТАУ

Бекетова А., Кубаев К.Е.

P2P электронды төлем жүйесі кейбір қорғаныс қасиеттеріне ие болуы керек, атап айтқанда, қол жетімділік, авторизация, тұтастық, теріске шығару, аутентификация және құпиялылық. Қазіргі уақытта электронды төлемдердегі қауіпсіздік мәселелері, қазіргі Интернеттегі қауіпсіздік мәселелеріне қарағанда өте көп талап етіледі.

Биткойн экожүйесі анонимді және бақыланбайды деп болжанады. Алайда, Биткойн іс жүзінде әлсіз анонимділікті ұсынады. Пайдаланушылар үшін құпиялылық мәселелерін Биткойн жүйесінің жалған аты көтереді.

Көптеген зерттеулер көрсеткендей, Bitcoin пайдаланушы мекен-жайы мен нақты тұлға арасындағы байланыс транзакцияны талдаудан алынуы мүмкін, бірнеше шабуыл режимдеріне атап өтсек:

1) заңды тұлғаларға нақты шабуыл – пайдаланушының жеке ақпаратын ашатын банк немесе биржа. Пайдаланушыларға Биткойн көмегімен физикалық тауарларды сатып алу немесе биткойнды фиаттық ақшаға айырбастау керек. Бұл жағдайда пайдаланушының мекен-жайын, байланыс ақпаратын және шынайы тұлғасын білу қажет.

2) жалпы сауда паттернері – Биткойнның кейбір сауда петтернері пайдаланушылардың құпиялығын ашуына әкеп соғады.

3) дақты шабуыл – бір битокин пайда болған сәттен бастап барлық тиісті транзакция туралы ақпарат пен мекен-жайлар сыртқы әлемде белгілі болуы мүмкін. Бұл мекенжайлар жоғары корреляция қасиетіне ие және шабуылдаушы тиісті талдау арқылы пайдаланушы туралы толық ақпаратты ала алады.

4) желілік деңгейдегі шабуыл – Биткойн желілік деңгейге қарағанда қолданбалы деңгейде құпиялылықты сақтай алады, ал шабуылшыларға желілік деңгейде шабуыл жасау оңай болып табылады [1].

Бұл жұмыста Биткойнның криптовалюта транзакцияларында пайдаланушылардың жеке басын және транзакциялық сәйкестігін сақтауға назар аударылды. Ұсынылған схема теориялық тұрғыдан талданып және бағаланып, Bitcoin транзакцияларында пайдаланушылардың құпиялылығын сақтау үшін олардың қауіпсіздігі мен сенімділігін дәлелдеді. Биткойнның қазіргі архитектурасына ешқандай өзгеріс енгізбестен сәйкес келетінін көрсетеді[2].

Әдебиеттер тізімі:

1. Koshy, P., Koshy, D., McDaniel, P.: An analysis of anonymity in Bitcoin using p2p network traffic. In: International Conference on Financial Cryptography and Data Security. Springer, Berlin, pp. 469–485 2014).

2. Conti, M., Kumar, S., Lal, C., A survey on security and privacy issues of Bitcoin. In: IEEE Communications Surveys & Tutorials (2018).