BME–s kutatók mutattak rá az Ethereum kriptovaluta sebezhetőségére

Az ELTE-s kollégáikkal közösen írt tanulmányt a világ egyik legrangosabb informatikai konferenciáján mutathatják be.

A BME és az ELTE közös kutatásának eredményeit összefoglaló tanulmányt fogadtak be az ACM Conference on Computer and Communications Security (CCS) nevű konferenciára. Az amerikai alapítású ACM az egyik legismertebb, ma már leginkább ernyőszervezetként működő oktatási-tudományos társaság az informatika területén. Konferenciája, a világ egyik legnagyobb presztízsű informatikai biztonsági fóruma **magyar intézményből körülbelül 10 évente fogad el tudományos közleményt**.

A publikáció két szerzője a BME részéről a Távközlési és Mesterséges Intelligencia Tanszék egyetemi tanára, Tapolcai János, valamint a tanszék tudományos munkatársa, Ladóczki Bence (BME), az ELTE részáról pedig Nagy Ábel és Seres István András. Tanulmányuk az Ethereum blokklánc – a Bitcoin után a második legnagyobb piaci kapitalizációjú kriptovaluta – egy kritikus sebezhetőségére hívja fel a figyelmet.

Számos elméleti munka korábban már rámutatott arra, hogy a blokklánc-technológia egyik Achilles-sarka az elosztott véletlenszám-generálás, amely meghatározza, hogy ki javasolhatja a következő blokkot. A Bitcoin ezt a folyamatot hatalmas energiafelhasználással teszi biztonságossá – évente Magyarország teljes villamosenergia-felhasználásához mérhető mértékben. Az Ethereum ezzel szemben egy korszerűbb, energiatakarékosabb megközelítést alkalmaz: kriptográfiai algoritmus segítségével választja ki a validátort. Bár ez hatékonyabb, a szakértők már korábban is kifejezték aggodalmukat a megoldás biztonságosságával kapcsolatban.

Izgalom az Ethereum-közösségben

A BME-s kutatók munkája (*Forking the RANDAO: Manipulating Ethereum's Distributed Randomness Beacon*) elsőként igazolja, hogy a jelenlegi Ethereum-protokollban használt algoritmus kritikus mértékben manipulálható, megerősítve ezzel a korábbi sejtéseket. A tanulmány nyomán vita bontakozott ki az Ethereum közösségében arról, bevezethető-e a közelgő hard-forkok (szoftverfrissítés az elosztott hálózat résztvevői számára) egyikében olyan protokollmódosítás, amely képes megelőzni a támadást.

Az ACM CCS a számítástechnikai konferenciákat rangsoroló Computing Research and Education Association of Australasia (CORE) rendszerében A* besorolású, vagyis a kiemelkedően színvonalas tudományos fórumok közé tartozik – mindössze 63 ilyen konferencia létezik az egész világon. A CORE A* rendezvényeken szakterületenként az év legjelentősebb tudományos eredményeit mutatják be, amelyek nagy figyelmet kapnak az akadémiai és az ipari szereplők részéről is. A BME kutatói évente átlagosan 2–3 ilyen jelentőségű publikációval képviseltetik magukat ezeken a fórumokon, a világ vezető egyetemeinek társaságában.

Az idei CCS Tajpejben lesz október 13. és 17. között.

Sajtókapcsolat:

- Kommunikációs Igazgatóság
- +36 1 463 2250

- kommunikacio@bme.hu

Eredeti tartalom: Budapesti Műszaki és Gazdaságtudományi Egyetem

Továbbította: Helló Sajtó! Üzleti Sajtószolgálat

Ez a sajtóközlemény a következő linken érhető el:
https://hellosajto.hu/?p=24406