BEMSZ TECHNOLÓGIAI PLATFORM

Ismeret bővítés belső ellenőrök számára

Mik azok a smart contractok?

A smart contractok egyszerűen egy blokkláncon tárolt programok, amelyek előre meghatározott feltételek teljesülése esetén futnak. Általában egy megállapodás végrehajtásának automatizálására használják őket, hogy minden résztvevő azonnal biztos lehessen a végeredményben, közvetítő közreműködése és időveszteség nélkül. Automatizálhatnak egy munkafolyamatot is, a feltételek teljesülése esetén elindítva a következő műveletet.

Az intelligens szerződések egyszerű "ha/amikor...akkor..." utasításokat követve működnek, amelyeket a blokklánc kódjába írnak. A számítógépek hálózata hajtja végre a műveleteket, ha az előre meghatározott feltételek teljesülnek és ellenőrizve vannak. Ez a művelet lehet például pénzeszközök felszabadítása a megfelelő felek számára, egy jármű regisztrálása, értesítések küldése vagy egy jegy kiállítása. A blokklánc frissül, amikor a tranzakció befejeződik. Ez azt jelenti, hogy a tranzakciót nem lehet megváltoztatni, és csak azok a felek láthatják az eredményeket, akiknek engedélyt adtak rá.

Kinek van szükséges smart contract auditra?

Elsősorban a kriptotőzsdéknek.

Egyre többen követelik meg a tokencsapatoktól, hogy a token tőzsdére való bevezetése előtt átessenek egy okosszerződés-ellenőrzésen.

Miért fontos a biztonság a kriptotőzsdék számára?

Ha egy szerződés nincs biztonságosan megírva, akkor bárkinek, aki rosszindulatú szándékkal és megfelelő ismeretekkel rendelkezik a szerződések természetéről, lehetősége van arra, hogy bármely szerződésből eszközöket vagy pénzt szipolyozzon ki a saját számlájára, pénzügyi és reputációs veszteséget okozva.

A megnövekedett pénzeszközök megnövelték a kiberbűnözők érdeklődését. Pl:

- Az EXMO a jelek szerint 10,5 millió dollár értékű pénzeszközt veszített el. - 2020. december
- Több mint 280 millió dollárt szivattyúztak le a KuCoin kriptotőzsdei tőzsdei hackelés során. - 2020. szeptember
- Az UPbit kriptopénz tőzsde ma bejelentette, hogy közel 50 millió dollár értékű étert (ETH) veszített el egy nyilvánvaló biztonsági rés során. - 2019. november
- A dél-koreai kriptopénz tőzsde egy feltételezett bennfentes munka áldozata lett - 2019. április

Smart contract audit módszertan

Csapatunk kidolgozott egy Smart Contract Security Verification Standardot az OWASP APPLICATION SECURITY VERIFICATION STANDARD v4.0 alapján. Többek közt ezekre a területekre tér ki: Tervezési, végrehajtási és tesztelési minőség, hozzáférés-ellenőrzés, kommunikáció, "biztonságos matematika", megbízható harmadik féltől származó komponensek, titkos adatok biztonságos tárolása, gázhasználattal kapcsolatos kockázatok, tokenek megvalósítása.

Statikus elemzés: A legkorszerűbb statikus kódelemző eszközöket használjuk.

Láncon belüli felügyelet: Manuálisan ellenőrizzük a szerződést a ténylegesen használt blokkláncon, hogy lássuk, milyen konfigurációs hibák, logikai problémák lehetnek, valamint milyen hatással lenne egy esetleges támadás a rendszerre.

Kézi felülvizsgálat: Kódellenőrzés (ha lehetséges, interjúval segítve), hogy kiszúrjuk a lehetséges logikai és kódolási hibákat.

Speciális eszközök:

- Securify - Python alapú kódelemző és sebezhetőség-kezelő.
- SmartCheck - Statikus kódelemző és biztonsági sebezhetőség-ellenőrző program.
- Mythril - intelligens szerződés sebezhetőségi elemző eszköz.
- Solidity Visual auditor

Készítette: Smohay Ferenc és Nagy Tamás

ABT Treuhand csoport