A csoport
Név:
Neptun:

A helyes válaszok bejelölését kérjük. Feladatonként több válasz is lehet helyes. Helytelen válaszért részpont-levonás jár, de csak az adott feladatra nézve vett nulla pontig. A pontszámok nem állnak közvetlen korrelációban a helyes válaszok számával.

I DLT (11p)

I/1 A DLT feloldása (1p):

- ☐ Distributed Link Technology
- ☐ Distributed Ledger Technology
- ☐ Domain Ledger Technology

I/2 DLT és Blockchain viszonya (2p):

- ☐ A DLT mintát a Blockchain technológiák valósítják meg
- ☐ A DLT minta Blockchain technológiával is megvalósítható
- ☐ A Blockchaint DLT segítségével valósítjuk meg
- ☐ A Blockchain minta DLT-vel is megvalósítható
- ☐ A DLT minta fő megvalósítását ma Blockchain alapú technológiák adják
- ☐ A Blockchain minta fő megvalósítását ma DLT-k adják

I/3 A Blockchain általános adatszerkezetre igaz általánosságban (2p):

- ☐ A blokkok egyértelműen sorrendezett tranzakciókat tárolnak
- ☐ A blokkok kriptográfiailag láncoltak
- ☐ A blokkok láncolását jellemzően nyilvános kulcsú titkosítással végezzük
- ☐ A blokkok láncolása irányított aciklikus gráfot definiál
- ☐ Az első blokkot konvencionálisan origin blokknak nevezzük
- ☐ Az első blokkot konvencionálisan genesis blokknak nevezzük
- ☐ Az első blokkot konvencionálisan root blokknak nevezzük

I/4 A Blockchain technológiák az általuk reprezentált “főkönyv” következő tulajdonságait biztosítják általánosan (2p):

- ☐ Immutabilitás
- ☐ Elosztott (P2P csomópontok között szinkronizált) tárolás
- ☐ Tranzakciók titkossága
- ☐ Megosztott főkönyv - tipikusan több vagy minden csomóponton
- ☐ Kriptográfiailag autentikus, nem letagadható tranzakciók
- ☐ Tranzakciót igénylő természetes vagy jogi személy egyértelmű azonosíthatósága
- ☐ Anoním tranzakciók

I/5 Az okos szerződésekre (amennyiben egy Blockchain technológia támogatja őket) általánosságban igaz, hogy… (2p)

- ☐ Jogi erővel rendelkeznek
- ☐ Segítségükkel a tranzakció-logika “programozhatóvá” válik
- ☐ Létrehozásuk önmagában egy Blockchain-tranzakció
- ☐ A szerződés maga is tárolásra kerül a főkönyvön
- ☐ A csomópontok közötti, blokkonkénti konszenzus-mechanizmusnak az okos szerződések hívási sorrendje tárgyát képezi
- ☐ A csomópontok közötti, blokkonkénti konszenzus-mechanizmusnak az okos szerződések végrehajtásának eredménye tárgyát képezi
- ☐ Végrehajtásukhoz mellékhatás-mentes (csak olvasó) kód esetén is lefuttatandó a rendszerszintű konszenzus-mechanizmus

I/6 Az okos szerződésekre (amennyiben egy Blockchain technológia támogatja őket) általánosságban igaz, hogy… (2p)

- ☐ A Blockchainre telepített okos szerződés kód módosítása a rendszerszintű konszenzus-mechanizmus segítségével történik
- ☐ Az okos szerződésből az azt tranzakcióként létrehozó fél “kizárhatja” magát
- ☐ Okos szerződés támogatás kialakítása csak kriptopénzzel rendelkező rendszerekben lehetséges
- ☐ Egy okos szerződés nyelv a megállási probléma (halting problem) eldönthetetlensége miatt nem lehet Turing-teljes
- ☐ Az okos szerződés nyelvek lehetnek Turing teljesek; a véges és korlátos futásidőt (megállást) tranzakciós díj, vagy végrehajtási időkorlát biztosítja

II Bitcoin (13p)

II/1 A Bitcoinra, mint kriptopénzre a következők igazak (2p):

- Elemi, tovább nem bontott egysége a Bitcoin
- Elemi, tovább nem bontott egysége a Satoshi
- Elemi, tovább nem bontott egysége a Wei
- Központi szereplő nem gyakorol felette monetáris kontrollt, a P2P rendszer bocsátja ki algoritmikusan
- A P2P rendszer üzemeltetőinek többségi döntésével a kibocsátás logikája megváltozhat a jövőben

II/2 A Bitcoin tranzakció-gráfjára a következőek igazak (3p):

- Minden tranzakció több bemenettel és több kimenettel is rendelkezhet, melyek egy-egy, a rendszer által könyvelt kriptopénz-mennyiséget reprezentálnak.
- Minden kimenet egyben bemenet is.
- Az "el nem költött" kimenetek rövidítése: UTXO
- Az "el nem költött" kimenetek rövidítése: UTRO
- A gráf összefüggő abban az értelemben, hogy minden tranzakció-pár között vezet legalább egy irányított út.
- "Coinbase" tranzakciónak hívjuk azokat a tranzakciókat, melyek során felhasználóként hozzájutunk a coin-kereskedő oldalakon vásárolt kriptopénzünkhöz.
- A tranzakció-gráf egy blokkosított, láncolt lista (ezért hívjuk a Bitcoint az első Blockchain technológiának).

II/3 A Bitcoin "pay to public key hash" tranzakció-típusára a következők igazak (3p):

- A kimenetek valamely fogadó, "továbbköltési jogosultsággal rendelkező" fél számára "címzettek"
- A Bitcoin "cím" (address) egy privát kulcs kriptográfiailag erős hash-e
- A továbbköltő fél digitális aláírással bizonyítja egy kimenet bemenetként alkalmazása feletti jogát
- A tranzakciók pszeudonimitása azt jelenti, hogy a tranzakciós gráf ismeretében sem lehet felfedni a "küldő" és "fogadó" felek identitását

II/4 "Proof of Work" / Nakamoto-style consensus (2p):

- A Bitcoin peer to peer hálózat (illetve a BTC ledger) csomópontjai a beérkezett tranzakciókból beérkezési sorrendben próbálnak blokkot képezni.
- A blokk-képzés során a csomópontok versenyeznek, hogy egy "nonce" mező módosításával ki talál előbb egy elég nagy SHA256 hash-ű blokkot.
- A blokk-képzés üteme az idő előrehaladtával előre meghatározott módon gyorsul, hogy a Bitcoin népszerűségének növekedését tranzakció-kapacitásban kövesse.
- Az átlagos blokkidő jelenleg ~10 perc.
- A "lezárt" tranzakció-blokkokat a csomópontok P2P stílusban terjesztik szét, így a tárolt "blokklánc" valójában átmenetileg "blokkfa" is lehet a csomópontokon.

II/5 "Proof of Work" / Nakamoto-style consensus (3p):

- A további bányászás tekintetében a csomópontok az ágak között a "legtöbb már elvégzett munka" elv alapján döntenek.
- A további bányászás tekintetében a csomópontok az ágak között a "legfrissebb utolsó blokk" elv alapján döntenek.
- A tranzakciók akkor véglegesek, amikor 6 blokk mélységbe kerültek; formálisan bizonyítható, hogy ezután a tranzakciók visszagörgetése, illetve a "dupla költés" (double spending) lehetetlen.
- A mechanizmus attól "Proof of Work", hogy egy kellő nehézségű blokk létezése valószínűségi értelemben bizonyítja kellő mennyiségű eredménytelen próbálgatás megtörténtét.
- A PoW megközelítés a Bitcoin sajátja; a többi Blockchain hálózat tipikusan más konszenzus-mechanizmust használ (pl. Proof of Stake, Proof of Elapsed Time, Practical Byzantine Fault Tolerance).
- Mivel az SHA256 hash "törése" célhardverrel jól támogatható feladat, az eredeti célokkal ellentétben a Bitcoin "bányászás" messze nem annyira demokratikusan elosztott, mint az eredeti szándék volt.

III Ethereum (7p)

III/1 Alapok és okos szerződések (3p):

- Az Ethereumban, csakúgy, mint a Bitcoinban, a "címtérbe" (address space) publikus-privát kulcspárok publikus része képződik le.
- Az Ethereumban, csakúgy, mint a Bitcoinban, az egyes "címeknek" nincs explicit egyenlege; az adott címhez kapcsolódó, költhető Ether-mennyiséget a hálózat klienseinek kell kiértékelnie.
- Az Ethereum okos szerződések fejlesztésének nyelve a Solidity.

- Az Ethereum okos szerződésekkel az ETH főkönyv felett saját definiálású és kibocsátású tokenek “főkönyveit” is létrehozhatjuk.
- Az okos szerződések támogathatják ezen tokenek natív kriptopénz (Ether) alapú adásvételét.
- Az Ethereum “world computer” interpretációja azt jelenti, hogy a tokenek segítségével gépidőt vásárolhatunk a világméretű peer to peer hálózat gépein, így férve hozzá nagymennyiségű erőforráshoz.

III/2 Tokenizáció (2p)

- A pénzért való tokenkibocsátás “Initial Coin Offering” (ICO) formájában az Európai Unióban illegális tevékenység.
- A tokenek segítségével alternatív gazdasági modellek hozhatóak létre, pl. “körkörös gazdaság” időhöz kötött autóhasználati jogot reprezentáló tokennel.
- Létrehozható olyan okos szerződés, mely egyértelműen (nem csak pszeudoním módon) azonosít token-tulajdonosokat, de nem ez a jellemző minta.
- A Decentralized Autonomous Organization, mint okos szerződés minta működésképtelenségét a “The DAO” kezdeményezés bukása egyértelműen bizonyította.

III/3 Cégünk biztosítói innovációt hajt végre, de magát a biztosítótársaságot nem akarja felszámolni (azaz nem “crowdsurance” forgatókönyvről beszélünk). Mely funkciókat lehet indokolt az Ethereum Blockchainre telepíteni - központosított rendszer, vagy privát/konzorciális Blockchain helyett? (2p)

- Kifizetés kriptopénzben külső, megbízható forrás (oracle) által bizonyított káresemény esetén (pl. repülőgép késése)
- Káresemény-piactér a szervízeknek
- Kockázatbecslés- és árazás
- Egyedi árazáshoz személygépkocsiba épített szenzorok méréseinek rögzítése
- Ügyféltörzs-adatbázis

IV Jogosultságkezelt rendszerek (15p)

IV/1 A privát/konzorciális, jogosultságkezelt Blockchain-ek fő előnyei a publikus rendszerekkel szemben... (3p)

- A főkönyvet nem az “egész világ”, csak az érdekelt felek látják
- Jellemzően magasabb áteresztőképesség
- Jellemzően magasabb átlagos késleltetés
- Jóval magasabb hibatűrés (a csomópontok kiesésének hatása kisebb)
- A Proof of Work konszenzus kisebb rendszerben hatékonyabb az alacsonyabb fogyasztás miatt
- Mivel nem a kriptopénzben javadalmazás adja a részvétel hajtóerejét, a főkönyvnek nem kell mindenképp kriptopénzt könyvelnie, egyszerűsödhet a programozási modell
- Magasabb profit érhető el bányászással
- A publikus rendszerekkel szemben a klasszikus PKI alapú autentikáció és autorizáció támogatása jellemzően megoldott

IV/2 Hyperledger Fabric: a szabadon hagyott helyen ábrával szemléltesse és ismertesse a szervezetek, csomópontok, főkönyvek/csatornák és okos szerződések (“chaincode”) kapcsolatát! (3p)

IV/3 Hyperledger Fabric: a szabadon hagyott helyen ábrával szemléltesse és ismertesse a tranzakció-vegrehajtás fő lépéseit! (3p)

IV/4 Hyperledger Fabric/Composer: lehet-e ezekben a technológiákban UTXO stílusú kriptopénzt okosszerződésként megvalósítani? Miért nincs a felvetésnek általánosságban értelme? Van-e olyan alkalmazás, ahol eseti jelleggel mégis felmerülhet egy “Fabric alapú coin” (vagy pénzért vehető token) bevezetése? (3p)

IV/5: Érveljen amellett, hogy a jogosultságkezelt rendszerek (pl. a Hyperledger Fabric) is “valódi” Blockchain technológiák, azaz minőségileg többet nyújtanak, mint egy egyszerű szinkronizált adatbázis – még ha kriptopénzt nem is nyújtanak! (3p)

V. Integráció (3p)

V/1. Az okos szerződések jellemzően zárt világot feltételeznek; a végrehajtó környezetből “kihívás” (pl. külső szolgáltatások hívása) tipikusan nem támogatott. Miért? (3p)