

Smart contracts

Andrej Adamčík
9.máj 2018



HILLBRIDGES

Téma smart contracts na blockchain-e, ich právneho významu a účinkov je zatiaľ v plienkach.

Ranná fáza ich aplikácií a absencia právnej úpravy šitej priamo na tento koncept interakcie v digitálnom prostredí zatiaľ bránia vysloveniu definitívnych právnych záverov, či všeobecne platných a trvalých právd.

Obsah dnešnej prednášky a príspevky do diskusie preto prosím berte ako moje aktuálne a rámcové názory.

Odpovede na konkrétne právne otázky bude (aj v tejto oblasti) naďalej potrebné hľadať formou zodpovedného posúdenia jednotlivých prípadov a ich súvislostí.

Možnosti právnej úpravy pri inováciách:

- tvorbou a zavedením nových právnych noriem
- interpretáciou existujúcich právnych noriem v nových súvislostiach

Komplikácie v prípade právnej regulácie smart contracts (a používania blockchain-u všeobecne):

- rozdielnosť slovníka programátorov a regulátora/právnikov
- rôznorodosť možných (aj nemožných) aplikácií
- celosvetová použiteľnosť = globálna aréna a viac rozhodcov
- priama naviazanosť na kryptomeny

Smart contracts ľudskou rečou (1)

- počítačový program
- zapísaný v bytecode, s ktorým daný blockchain pracuje
- tvorí súčasť daného blockchain-u
- obsahuje jedno alebo viacero „if-then“ pravidiel a prípadne aj nejaký vnútorný register informácií (čokoľvek, čo smart contract vie „udržať“)

Smart contracts ľudskou rečou (2)

- spustenie smart contract-u vyvolá následok (podľa „if-then“ pravidiel) – odoslanie určitej informácie na jednu alebo viac stanovených adries na blockchain-e (prípadne inam)
- po úspešnom spustení smart contract-u teda dôjde k zmene stavu na blockchain-e, čiže k transakcii, ktorá môže predstavovať prevod alebo distribúciu vecí, práv alebo iných hodnôt zastúpených zápismi v danom blockchain-e

Právne významné znaky (1)

- smart contract je elektronický zápis podmienok transakcie na blockchain-e
- častokrát neobsahuje všetky podmienky zmluvy a nemusí spĺňať ani formálne požiadavky povinné pre niektoré zmluvy
- niekedy vôbec nemusí obsahovať podmienky zmluvy
- bytecode smart contract-u je pre človeka nečitateľný
- zdrojový kód (po prevedení z bytecode) je zrozumiteľný len pre programátora
- bez ďalšieho kontextu sú „strany“ smart contract-u anonymné

Právne významné znaky (2)

- smart contract vzniká (t.j. jeho podmienky sa sfinalizujú) pred umiestnením na blockchain; kedy vzniká zmluva, ktorej podmienky zachytáva a kde?
- transakciu na blockchain-e nevykoná samotný smart contract, ale virtuálny počítač „bežiaci“ na blockchain-e – fyzicky teda nodes blockchain-u
- k uskutočneniu transakcie podľa smart contract-u teda fyzicky dochádza na viacerých miestach naraz, v závislosti od povahy blockchain-u aj vo viacerých krajinách; v skutočnosti dokonca postupne v rámci tvorby konsenzu, nie nevyhnutne v rovnakej chvíli u všetkých nodes...

Výhody konceptu smart contracts

- smart contract je nielen zápis podmienok transakcie, ale v spojení s virtuálnym počítačom aj prostriedkom jej realizácie a zaznamenania zmeneného stavu – automatizácia a vynechanie prostredníkov
- + blockchain effects:
- vylúčenie double-spendingu
- nemennosť - ochrana pred zmenou podmienok bez konsenzu
- auditovateľnosť (trvácnosť a podľa okolností aj publicita)

- sťažená čitateľnosť a zrozumiteľnosť
 - len čiastočný zápis podmienok
 - nedostatočnosť formy / závislosť od iných úkonov
- + blockchain effects:
- deterministická povaha virtuálneho počítača
 - nemennosť – problematická aktualizácia, oprava
 - potreba virtuálneho počítača na realizáciu
 - zraniteľnosť rozhrania s externalitami (oracles, externé databázy a registre, aplikácie, a pod.)
 - otázky dôvernosti

Protizákonnosť a „nezvratnosť“

- nezákonná transakcia, hoci aj zrealizovaná a zachytená na blockchain-e, je neplatná; neplatná môže byť napr. aj transakcia vykonaná v omyle alebo pri nesplnení požiadaviek formy
- celý katalóg následkov neplatných transakcií: právo na vrátenie do predošlého stavu, možnosť uloženia sankcií (finančných, trestných), atď.
- transakcie na blockchain-e je prakticky možné zvrátiť (spätný prevod, hard fork)
- prekážky vynútiteľnosti zvrátenia (anonymita, nedostatok konsenzu, nemajetnosť mimo blockchain-u, zapojenie rôznych jurisdikcií)

- zodpovednosť za správnosť technologického riešenia smart contract-u (blockchain, naprogramovanie, komunikácia s klientom, výstupná kontrola produktu)
- možná zodpovednosť za výber správnej externality
- ochrana tvorcu
- ochrana zadávateľa

Tvorba smart contracts aplikácií

- všetko, čo sa vzťahuje na tvorbu smart contracts
- zodpovednosť za zákonnosť transakcií
- zodpovednosť za náklady transakcií
- kto s kým uzatvára zmluvu a o čom



Vďaka

kontakt: andrej.adamcik@hillbridges.com