Smart Contracts: Programování peněz

Smart Contract je digitální protokol nebo program, který automatizuje provádění, kontrolu a dokumentaci událostí podle podmínek smlouvy. Běží na blockchainu, což znamená, že po nasazení (deploymentu) je kód nezměnitelný a nepodplatitelný.

1. Jak Smart Contract funguje?

Fungování chytrých smluv se často přirovnává k prodejnímu automatu na nápoje:

```
1. **Vstup:** Vložíte peníze a zvolíte kód nápoje.
2. **Logika:** Automat ověří, zda je částka dostatečná a zda je nápoj skladem.
3. **Výstup:** Pokud jsou podmínky splněny, automat vydá nápoj a případně vrátí drobné. Není potřeba žádný prodavač (prostředník).
```

—

2. Klíčové vlastnosti

- **Autonomie:** Smlouva se vykoná sama. Jakmile je v síti, nikdo (ani autor) ji nemůže zastavit nebo změnit.
- **Důvěra:** Data jsou uložena v distribuované síti. Všichni účastníci vidí pravidla a výsledek.
- **Bezpečnost:** Šifrování a distribuce uzlů činí nabourání smlouvy extrémně náročným.
- **Rychlost a úspora:** Odpadá nutnost papírování, notářů a bankovních poplatků.

—

3. Programovací jazyky a platformy

Nejpoužívanějším prostředím pro chytré smlouvy je **EVM (Ethereum Virtual Machine)**.

- **Solidity:** Nejoblíbenější jazyk pro Ethereum. Syntaxí připomíná JavaScript nebo C++, ale je navržen specificky pro práci s financemi a bezpečností.
- **Rust:** Používá se na moderních rychlých blockchainech jako Solana nebo Polkadot (díky své bezpečnosti v oblasti paměti).
- **Move:** Nový jazyk (původně od Meta/Facebooku) navržený s důrazem na digitální aktiva jako na fyzické objekty, které nelze omylem zkopírovat.

—

4. Praktické příklady využití

Oblast	Využití
Financování	Automatické uvolňování splátek hypotéky po potvrzení katastrem.
Logistika	Platba dodavateli se odešle v momentě, kdy senzor v kamionu potvrdí doručení do skladu.
Hlasování	Transparentní a nezfalšovatelné volby v rámci **DAO** (Decentralizovaných organizací).
NFT	Automatické vyplácení autorských honorářů (royalty) umělci při každém přeprodeji díla.

—

5. Orákula (Oracles): Most do reality

Smart kontrakty jsou uzavřeny v blockchainu a „nevidí“ ven. Aby se mohly rozhodovat na základě reálných dat (např. cena zlata, výsledek fotbalu, počasí), potřebují **Orákula**.

- **Příklad:** Chytrá pojistka na zpoždění letu automaticky vyplatí odškodné, pokud orákulum (např. Chainlink) potvrdí zpoždění v databázi letiště.

—

6. Rizika: "Code is Law"

Filozofie „Kód je zákon“ znamená, že chyba v kódu je považována za vlastnost systému.

- **Reentrancy attack:** Klasická chyba, kdy útočník stihne vybrat peníze několikrát dříve, než smlouva stihne aktualizovat váš zůstatek.
- **Auditování:** Před nasazením smlouvy s miliony dolarů je nezbytný externí audit kódu bezpečnostními firmami.

Související články:

- Blockchain: Jak funguje databáze
- DeFi a automatizované půjčky
- Ethereum: Počítač celého světa

Tagy: it smart-contracts solidity ethereum programming fintech blockchain