



Building a better
working world

Jak lze pomocí blockchainu vybudovat důvěru?

EY Blockchain Analyzer:
SmartContract and Token Review

The better the question. The better the answer. The better the world works.

Často kladené otázky

EY Blockchain Analyzer: Smart Contract & Token Review (SC&TR) je řešení, jehož cílem je zajistit důvěru v transakce prováděné na blockchainu. Kontrolou základního kódu chytrých smluv pomáhá SC&TR identifikovat běžné bezpečnostní zranitelnosti, ověřit soulad kódu s obchodní logikou a zvýšit efektivitu a kvalitu kódu.

Co je chytrá smlouva?

Chytrá smlouva (neboli Smart Contract) je samovykonatelný počítačový program, který automaticky vynucuje podmínky dohody mezi dvěma i více stranami. Chytré smlouvy pracují samostatně bez zprostředkovatelů a jsou postaveny na blockchainu, díky čemuž jsou bezpečné a transparentní. Chytré smlouvy mají využití v rámci široké škály aplikací od finančních transakcí až po řízení dodavatelského řetězce.

Proč by měly být chytré smlouvy revidovány?

Chytré smlouvy je třeba revidovat, aby se snížila míra rizika případných chyb, zranitelností a dalších problémů, které by mohly ohrozit jejich bezpečnost a vlastní funkčnost. Identifikací potenciálních rizik a příležitostí ke zlepšení kódu, revize pomáhají snižovat dopady nákladných chyb, podvodů a pokusů o „hacknutí“. Takovéto revize mohou zainteresovaným stranám pomoci posoudit, zda chytrá smlouva funguje tak, jak byla zamýšlena, což je zásadní pro aplikace, které zahrnují citlivá data nebo transakce s vysokou hodnotou.

Co je vlastně řešení „Smart Contract & Token Review“?

Řešení SC&TR dodává organizacím jistotu při nasazování a interakci s chytrými smlouvami. Pomáhá uživatelům spouštět stovky standardních i vlastních testovacích scénářů. Zároveň poskytuje podrobné výsledky související s účelem a logikou každého testu. Výsledky testů pomáhají uživatelům pochopit chyby a nekonzistence, které chytrá smlouva obsahuje.

Jaké typy blockchainu podporuje?

V EY věříme, že veřejné blockchainy jsou jedinou dlouhodobě životaschopnou možností, a proto se zaměřujeme na Ethereum blockchain.

Jakým způsobem SC&TR funguje?

Poskytnutý kód je naskenován, zkompilován s příslušnou verzí solidity kompilátoru a odeslán do našeho testovacího enginu. Testovací engine provádí statickou analýzu kódu prostřednictvím zdrojového kódu i AST a customizovaná Ethereum Virtual Machine (EVM) dynamicky simuluje různé testovací scénáře.

Proč SC&TR používat?

Řešení využívají především odborníci EY pracující na klientských projektech. Může být ovšem použito i přímo klienty, osobami nebo organizacemi, které potřebují zrevidovat chytrou smlouvu (v závislosti na případném schválení ze strany EY). Evidujeme rovněž zájem ze strany technických specialistů, vývojářů, auditorů, compliance a riskových týmů.

Jaké bezpečnostní testy poskytuje?

Řešení pokrývá běžné bezpečnostní zranitelnosti, jako je přetečení nebo podtečení, nebezpečné změny stavu chytrých smluv, používání zastaralých nebo nebezpečných klíčových slov, krátké adresy a další. Seznam bezpečnostních testů průběžně aktualizujeme společně s dalším výzkumem a vývojem řešení. V rámci každé zakázky jsou automatizované kontroly odborně revidovány a doplněny o kontroly manuální tak, aby bylo zajištěno plné pokrytí kódu.

Co je funkční testování?

Náš výzkum a zkušenosti ukazují, že k většině zneužití chytrých smluv dochází prostřednictvím neočekávaného chování chytré smlouvy a manipulace s krajními případy. Z toho důvodu provádíme funkční testy, které mají za cíl snížit toto riziko ověřením, zda se chytrá smlouva chová dle očekávání. Funkčnost je ověřena jak kontrolou požadované syntaxe, tak simulací různých scénářů, které jsou součástí základní funkcionality standardu ERC-20.

Kdy by se mělo řešení SC&TR používat?

Řešení SC&TR poskytne největší užitek při použití před nasazením, jako součást procesu vývoje nebo k revizi kódu před nasazením smlouvy na Mainnet. Jakmile je chytrá smlouva nasazena, je již neměnná, což znamená, že ve většině případů již nelze chyby a zranitelnosti opravit.

Proč je tým EY v ideální pozici pro podporu klientů při revidování a testování chytrých smluv?

Hlavní činností týmů EY je poskytovat byznysovým ekosystémům důvěru a jistotu. Tímto se zabýváme jak v rámci oddělení auditu, tak v rámci naší poradenské činnosti. V EY disponujeme robustní metodologií a standardy zajišťujícími nejvyšší kvalitu služeb, jenž pomáhají zainteresovaným stranám získat větší důvěru v technologie, které používají.

Pokračujme v konverzaci

Pokud se chcete o řešení EY Blockchain Analyzer: Smart Contract & Token Review dozvědět více a zjistit, jak může pomoci Vaší organizaci, kontaktujte náš tým:



Jakub Tesař

Vedoucí týmu inovací, digitálních řešení a nových technologií
jakub.tesar@cz.ey.com



Jan Pich

Vedoucí týmu Kybernetické bezpečnosti
jan.pich@cz.ey.com

EY | Building a better working world

EY je předním celosvětovým poskytovatelem odborných poradenských služeb v oblasti auditu, daní, transakčního a podnikového poradenství. Znalost problematiky a kvalita služeb, které poskytujeme, přispívají k posilování důvěry v kapitálové trhy i v ekonomiky celého světa. Výjimečný lidský a odborný potenciál nám umožňuje hrát významnou roli při vytváření lepšího prostředí pro naše zaměstnance, klienty i pro širší společnost.

Název EY zahrnuje celosvětovou organizaci a může zahrnovat jednu či více členských firem Ernst & Young Global Limited, z nichž každá je samostatnou právnickou osobou. Ernst & Young Global Limited, britská společnost s ručením omezeným garancí, služby klientům neposkytuje. Informace o tom, jak EY shromažďuje a používá osobní údaje, a popis práv, která mají fyzické osoby podle právních předpisů o ochraně osobních údajů, jsou k dispozici na adrese ey.com/privacy. Pro podrobnější informace o naší organizaci navštivte prosím naše webové stránky ey.com.

© 2020 Ernst & Young, s.r.o. | Ernst & Young Audit, s.r.o. | E & Y Valuations s.r.o. | EY Law advokátní kancelář, s.r.o. Všechna práva vyhrazena.

Tento materiál má pouze všeobecný informační charakter, na který není možné spoléhat se jako na poskytnutí účetního, daňového ani jiného odborného poradenství. V případě potřeby se prosím obraťte na svého konkrétního poradce.

ey.com