

## POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Student: Bc. Matěj Vaculík

Oponent: Ing. Aleš Ryška

Studijní program: Informační technologie

Specializace: Kybernetická bezpečnost

Akademický rok: 2024/2025

Téma diplomové práce: **Bezpečnostní rizika smart kontraktů na blockchainu**

Diplomová práce Bc. Matěje Vaculíka s názvem "Bezpečnostní rizika smart kontraktů na blockchainu" se systematicky zabývá aktuální a vysoce relevantní problematikou kybernetické bezpečnosti v prostředí decentralizovaných aplikací. Stanovený cíl práce (body zadání) byl naplněn v plném rozsahu a na adekvátní odborné úrovni.

Práce je strukturována logicky a přehledně, což usnadňuje orientaci v textu. Jazykové zpracování je na velmi vysoké úrovni. To práci klasifikuje jako vhodný materiál, jak pro začínající, tak i pro pokročilé čtenáře se v oblasti vývoje a výzkumu v oblasti smart kontraktů. Formální úprava práce splňuje veškeré požadavky, s adekvátním využitím odkazů na literární a elektronické zdroje. Je nutno zdůraznit vhodné užití obrázků, tabulek a příloh, které doplňují textový obsah.

Teoretická část poskytuje důkladný základ v oblasti smart kontraktů a blockchainových technologií. Autor prokázal schopnost identifikovat a klasifikovat klíčové bezpečnostní zranitelnosti, což reflektuje hluboké pochopení problematiky a vysokou míru přehledu v aktuálním dění.

Praktická část je charakterizována aplikačním přístupem, který významně přispívá k hodnotě práce, posouvá ji na velmi kvalitní a vysokou úroveň. V rámci této části autor provedl simulace širokého spektra útoků na smart kontrakty v testovacím prostředí. Následně byly navrženy a implementovány mitigační strategie, jejichž účinnost byla verifikována opakovaným testováním. Tento iterativní metodologický postup (analýza zranitelností, simulace útoku, návrh mitigace, implementace a ověření) podtrhuje úroveň a praktickou aplikovatelnost dosažených výsledků a vyspělost autora.

Celkově práce demonstruje vysokou úroveň odborných znalostí a analytických schopností autora v dané oblasti. Její přínos spočívá v komplexním a prakticky ověřeném popisu problematiky bezpečnosti smart kontraktů, což ji předurčuje k využití jako relevantní zdroj informací pro další výzkum a vývoj. Všechny požadavky zadání diplomové práce byly splněny.

Kvalita předložené práce indikuje výjimečné nadání autora pro řešení komplexních technických problémů, což je předpoklad pro úspěšnou kariéru v dynamickém prostředí kybernetické bezpečnosti.

Na základě předloženého obsahu a zpracování se diplomová práce jeví jako plně vyhovující stanoveným cílům. Práci doporučuji k obhajobě s hodnocením **A (výborně)**.

**Doporučené dotazy k obhajobě:**

- Narazil student během vypracování práce na zranitelnosti “in the wild”, tedy zranitelnosti, které jsou aktuální?
- Jak student vnímá z hlediska bezpečnosti trend “vibecodingu” v oblasti smart contractů?

**Celkové hodnocení práce:**

Známku uvede oponent dle svého uvážení dle klasifikační stupnice ECTS:

A – výborně, B – velmi dobře, C – dobře, D – uspokojivě, E – dostatečně, F – nedostatečně.

Stupeň F znamená též „nedoporučuji práci k obhajobě“.

**Předloženou diplomovou práci k obhajobě a navrhuji hodnocení**

**A**

**V případě hodnocení stupněm „F – nedostatečně“ uveďte do připomínek a slovního vyjádření hlavní nedostatky práce a důvody tohoto hodnocení.**

Datum 8.6.2025

Podpis oponenta diplomové práce