Побудова оцінки імовірності атаки подвійної витрати у протоколі консенсусу Proof of Stake за наявності чекпоінтів

Коломієць Андрій Юрійович

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Фізико-технічний інститут

Науковий керівник: д.т.н., проф. кафедри ММЗІ Ковальчук Л.В.

24 червня 2022 р.

Актуальність дослідження

- Популяризація блокчейн технології в криптовалютах.
- Покращення безпеки блокчейн мережі до протидії атаки подвійної витрати з проколом консенсусу Proof of Stake.
- Безпека мережі блокчейну, що містить у собі механізм чекпоінтів, який можливо за недоведеними припущеннями протидіятиме атаці подвійної витрати з протоколом консенсусу Proof of Stake.

Мета та завдання дослідження

Метою дослідження є оцінка імовірності атаки подвійної витрати у блокчейнах з протоколом консенсусу Proof of Stake при наявності контрольних точок.

Завдання дослідження:

- огляд літератури за зазначеною тематикою;
- знайомство з протоколами консенсусу Proof of Work та Proof of Stake, та атаками, що можуть відбутися у кожній консенсусній моделі;
- знаходження явного виразу імовірності для атаки подвійної витрати на протокол консенсусу Proof of Stake за умови існування чекпоінтів;
- отримати чисельні результати за доведеною формулою, та переконатися, що вони підтверджують адекватність отриманої формули.

Об'єкт і предмет дослідження

Об'єктом дослідження є процес функціювання блокчейну з протоколом консенсусу Proof of Stake за умови наявності чекпоінтів.

Предметом дослідження є аналіз стійкості блокчейну до атаки подвійної витрати у протоколі консенсусу Proof of Stake за наявності чекпоінтів.

Поняття блокчейну

Блокчейн — це цифровий реєстр стійкий до несанкційованого доступу, реалізований розподіленим чином без центрального органу керування, підтримується та керується спільно розподіленою групою учасників. В системі відсутня централізація у вигляді фінансових установ, банків чи довірених осіб.

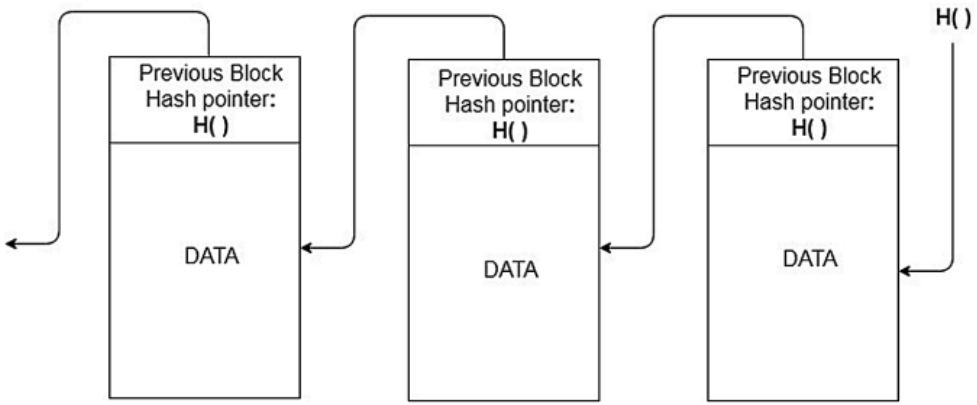

Рис.: Блокчейн

Протоколи консенсусу

Proof of Work – це протокол консенсусу, що заснований на доведенні виконаної роботи.

Proof of Stake – це модель протоколу консенсусу, котра залежить від того скільки коштів у вигляді криптовалюти інвестував кожен користувач в систему.

Поняття чекпоінту

Контрольні точки або чекпоінти – це коли хеш-значення блоку до певного моменту часу жорстко закодовано в офіційному клієнті Bitcoin. Клієнт сприймає всі транзакції, підтверджені до контрольної точки, як незворотні.

Приклади криптовалют з чекпоінтами:

- Bitcoin (1000 blocks);
- Bitcoin Cash (10 blocks);
- Ethereum 2.0 (64 slots);
- Polkadot (64 slots);
- Cardano and Solana (432 000 slots or 5 days);

Класична атака подвійної витрати у протоколі консенсусу Proof of Stake

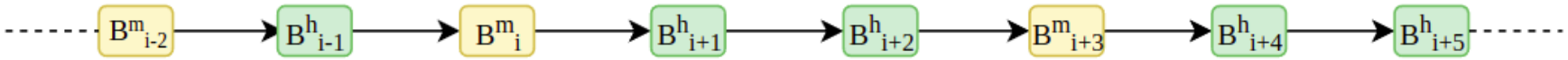

Рис.: Блокчейн у вигляді послідовності часових слотів.

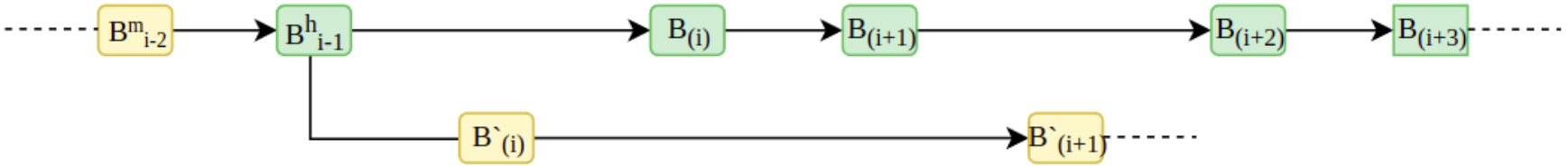

Рис.: Візуалізація атаки.

Атака відбувається успішно, якщо зловмисникам вдалося побудувати довший або принаймні однаковий за кількістю блоків ланцюг у порівнянні з ланцюгом чесних майнерів.

Явний вираз для імовірності атаки подвійної витрати у протоколі консенсусу Proof of Stake

Theorem

$$P(A(z)) = \sum_{k=z}^{\infty} p^z q^k C_{k+z-1}^k + \sum_{k=0}^{z} \left(\frac{q}{p}\right)^{z-k} p^z q^k C_{k+z-1}^k =$$

$$= 1 - \sum_{k=0}^{z} \left(p^z q^k - p^k q^z\right) C_{k+z-1}^k,$$

де

p – *частка чесних майнерів;*

q – *частка зловмисних майнерів;*

z – *кількість блоків підтвердження побудовані чесними майнерами;*

k – *кількість блоків побудованих зловмисником.*

Атака подвійної витрати у протоколі консенсусу Proof of Stake з чекпоінтами

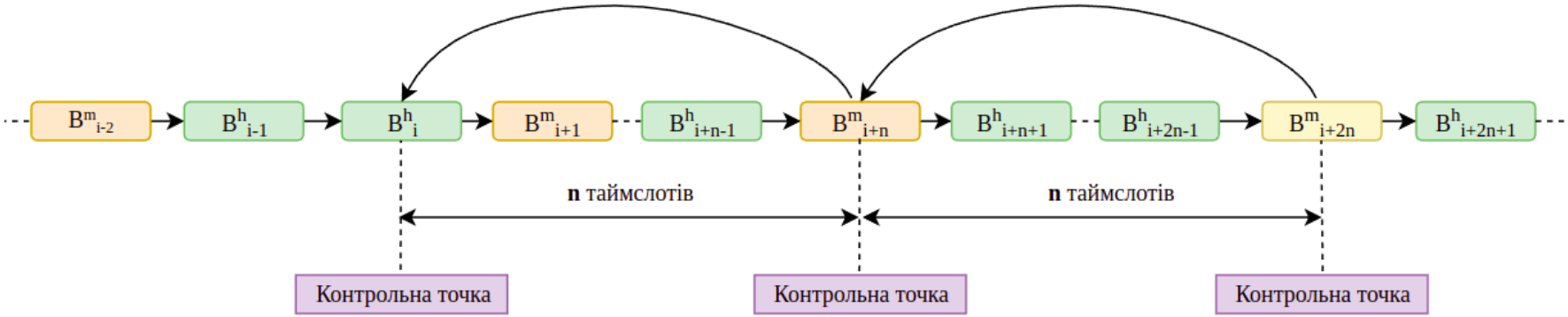

Рис.: Блокчейн ланцюг у вигляді послідовності часових слотів.

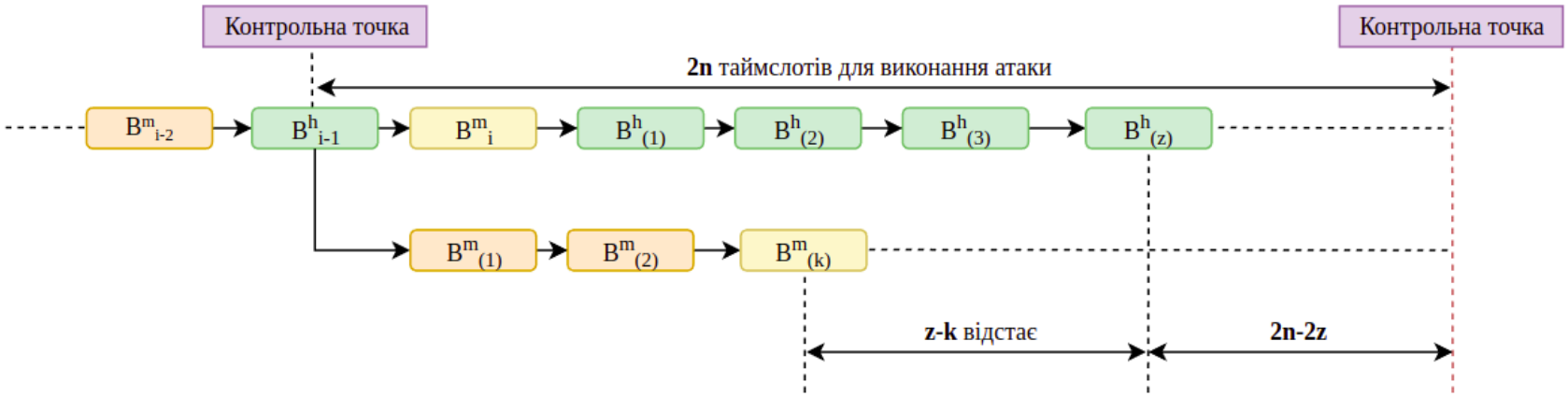

Рис.: Візуалізація атаки.

Явний вираз для імовірності атаки подвійної витрати у протоколі консенсусу Proof of Stake з чекпоінтами

Theorem

$$P(A(z)) = \sum_{k=0}^{z-1} C_{z+k-1}^{k} p^z q^k \sum_{i=0}^{n-z} p_i + \sum_{k=z}^{2n-z} C_{z+k-1}^{k} p^z q^k,$$

де :

$$p_i = \left(C_{z-k+2i}^{i} p^i q^{z-k+i} - \sum_{j=0}^{i-1} p_j C_{2i-2j}^{i-j} (pq)^{i-j} \right),$$

p – *частка чесних майнерів;*
q – *частка зловмисних майнерів;*
z – *кількість блоків підтвердження побудовані чесними майнерами;*
n – *відстань між двома чекпоінтами, що вимірюється у тайм слотах.*
k – *кількість блоків підтвердження, що побудували зловмисні майнери.*

Результати для порівняння

Табл.: Мінімальна кількість блоків підтвердження для класичного випадку атаки, при якій $P_z \leq 10^{-3}$

q	**0.10**	**0.15**	**0.20**	**0.25**	**0.30**	**0.35**	**0.40**	**0.45**
$P(A(z)) \leq 10^{-3}$	0,00000785976466	0.000288	0.000284	0.000748	0.0033027	0.000788	0.00047	0.00099
z	10	10	15	20	25	60	150	540

Табл.: Мінімальна кількість блоків підтвердження для випадку атаки з чекпоінтами, при якій $P_z \leq 10^{-3}$

q	**0,1**	**0,15**	**0,2**	**0,25**	**0.3**	**0,35**	**0,4**	**0,45**
$P(A(z)) < 10^{-3}$	0,00000785976465	0,000287	0,000284	0,000747	0,003303	0,000787	0,000471	0,000847
z	10	10	15	20	25	60	150	500

Результати для порівняння

Табл.: Порівняльна таблиця з кількістю блоків підтвердження та ймовірностями здійснення атаки подвійної витрати в класичній блокчейн-системі, та блокчейн-системі з чекпоінтами.

	Частка	Класичний випадок блокчейн-системи		Блокчейн-система, що містить чекпоінти	
n	**q**	**z**	**Імовірності атаки**	**z**	**Імовірності атаки**
50	0,1	6	0,000591412160000	6	0,00059141216000
	0,15	9	0,000590058017484	9	0,00059005801748
	0,2	13	0,000738096069111	13	0,00073809606849
	0,25	20	0,000747285192981	20	0,00074728135353
	0,3	32	0,000875915224973	32	0,00087305341156
	0,35	50	0,002188394725421	50	0,00145056147656
	0,4	50	0,043860884260170	50	0,02709919775701
	0,45	50	0,317304397874194	50	0,18272818468614
100	0,1	6	0,000591412160000	6	0,00059141216000
	0,15	9	0,000590058017484	9	0,00059005801748
	0,2	13	0,000738096069111	13	0,00073809606911
	0,25	20	0,000747285192981	20	0,00074728519298
	0,3	32	0,000875915224973	32	0,00087591508657
	0,35	58	0,000965098041430	58	0,00096385710585
	0,4	100	0,004320189876101	100	0,00263540335618
	0,45	100	0,156775865424405	100	0,08870061556165
150	0,1	6	0,000591412160000	6	0,00059141216000
	0,15	9	0,000590058017484	9	0,00059005801748
	0,2	13	0,000738096069111	13	0,00073809606911
	0,25	20	0,000747285192981	20	0,00074728519298
	0,3	32	0,000875915224973	32	0,00087591522496
	0,35	58	0,000965098041430	58	0,00096509262566
	0,4	133	0,000994204554214	131	0,00099269100223
	0,45	150	0,082748003254018	150	0,04647043929210
200	0,1	6	0,000591412160000	6	0,00059141216000
	0,15	9	0,000590058017484	9	0,00059005801748
	0,2	13	0,000738096069111	13	0,00073809606911
	0,25	20	0,000747285192981	20	0,00074728519298
	0,3	32	0,000875915224973	32	0,00087591522497
	0,35	58	0,000965098041430	58	0,00096509801118
	0,4	133	0,000994204554214	133	0,00098816813374
	0,45	200	0,045094107137097	200	0,02521789162552

Практичні результати для класичної атаки

Табл.: Імовірності класичної атаки подвійної витрати на блокчейн без чекпоінтів.

$\frac{q}{z}$	0.10	0.15	0.20	0.25	0.30	0.35	0.40	0.45
5	0,001781840	0,011257326	0,039162880	0,097854614	0,197617320	0,343438571	0,533135360	0,757158109
10	0,000007860	0,000288000	0,003158241	0,017806559	0,065106714	0,174947201	0,372184042	0,657928176
15	0,000000039	0,000008220	0,000284000	0,003568523	0,023307658	0,095273444	0,272425900	0,586064960
20	0,000000000	0,000000248	0,000026800	0,000748000	0,008673864	0,053573446	0,204117260	0,528630060
25	0,000000000	0,000000008	0,000002580	0,000160600	0,003302727	0,030712034	0,155151124	0,480591320
30	0,000000000	0,000000000	0,000000256	0,000035000	0,001276000	0,017837342	0,119104008	0,439334368
35	0,000000000	0,000000000	0,000000025	0,000007760	0,000500000	0,010458206	0,092100486	0,403281240
40	0,000000000	0,000000000	0,000000003	0,000001730	0,000196600	0,006176008	0,071620620	0,371386020
45	0,000000000	0,000000000	0,000000000	0,000000388	0,000078000	0,003667923	0,055944968	0,342909560
50	0,000000000	0,000000000	0,000000000	0,000000088	0,000031000	0,002188395	0,043860884	0,317304398
55	0,000000000	0,000000000	0,000000000	0,000000020	0,000012440	0,001310000	0,034492480	0,294150380
60	0,000000000	0,000000000	0,000000000	0,000000005	0,000005000	0,000788000	0,027195754	0,273115940
65	0,000000000	0,000000000	0,000000000	0,000000001	0,000002020	0,000474000	0,021490666	0,253933500
70	0,000000000	0,000000000	0,000000000	0,000000000	0,000000814	0,000286000	0,017015502	0,236383140
75	0,000000000	0,000000000	0,000000000	0,000000000	0,000000330	0,000173400	0,013495322	0,220281280
80	0,000000000	0,000000000	0,000000000	0,000000000	0,000000134	0,000105000	0,010719656	0,205472840
85	0,000000000	0,000000000	0,000000000	0,000000000	0,000000054	0,000063800	0,008526426	0,191825200
90	0,000000000	0,000000000	0,000000000	0,000000000	0,000000022	0,000038800	0,006790194	0,179224060
95	0,000000000	0,000000000	0,000000000	0,000000000	0,000000009	0,000023600	0,005413464	0,167569980
100	0,000000000	0,000000000	0,000000000	0,000000000	0,000000004	0,000014400	0,004320190	0,156775866

Практичні результати для атаки з чекпоінтами

Табл.: Ймовірність атаки подвійної витрати для випадку блокчейну з чекпоінтами (відстань між чекпоінтами $n = 50$).

$\frac{q}{z}$	**0,1**	**0,15**	**0,2**	**0,25**	**0,3**	**0,35**	**0,4**	**0,45**
5	0,001781840000	0,011257326211	0,039162880000	0,097854612690	0,197616568315	0,343366854001	0,531145103303	0,736413569802
10	0,000007859765	0,000287014738	0,003158241098	0,017806556239	0,065105579550	0,174839299040	0,369204504278	0,627152503143
15	0,000000039252	0,000008223010	0,000283612898	0,003568520213	0,023306178834	0,095133228086	0,268576820035	0,546718896697
20	0,000000000207	0,000000247918	0,000026719163	0,000747281354	0,008672035230	0,053400794201	0,199411374949	0,481104058216
25	0,000000000001	0,000000007694	0,000002587264	0,000160530298	0,003300515949	0,030504447776	0,149542482626	0,424755943188
30	0,000000000000	0,000000000243	0,000000255042	0,000035064297	0,001274219556	0,017589772354	0,112489488954	0,374627975893
35	0,000000000000	0,000000000008	0,000000025457	0,000007746013	0,000495855528	0,010161694293	0,084295808643	0,328605502108
40	0,000000000000	0,000000000000	0,000000002563	0,000001720610	0,000192684196	0,005813829872	0,062289707195	0,284728899621
45	0,000000000000	0,000000000000	0,000000000258	0,000000376758	0,000072734569	0,003202204285	0,044362536086	0,240079435059
50	0,000000000000	0,000000000000	0,000000000021	0,000000066385	0,000022060913	0,001450561477	0,027099197757	0,182728184686

Практичні результати для атаки з чекпоінтами

Табл.: Ймовірність атаки подвійної витрати для випадку блокчейну з чекпоінтами (відстань між чекпоінтами $n = 100$).

$\frac{q}{z}$	0,1	0,15	0,2	0,25	0,3	0,35	0,4	0,45
5	0,001781840000	0,011257326211	0,039162880000	0,097854614258	0,197617319954	0,343438321777	0,533026948061	0,750981309932
10	0,000007859765	0,000287014738	0,003158241098	0,017806558608	0,065106713695	0,174946834914	0,372025224891	0,648915747834
15	0,000000039252	0,000008223010	0,000283612899	0,003568523309	0,023307657785	0,095272982480	0,272225848899	0,574761678960
20	0,000000000207	0,000000247918	0,000026719163	0,000747285193	0,008673864168	0,053572896683	0,203879890103	0,515280022075
25	0,000000000001	0,000000007694	0,000002587265	0,000160534957	0,003302727045	0,030711401183	0,154878258430	0,465321943483
30	0,000000000000	0,000000000243	0,000000255043	0,000035069920	0,001276875697	0,017836627246	0,118796330599	0,422210583042
35	0,000000000000	0,000000000008	0,000000025459	0,000007752863	0,000499069008	0,010457407562	0,091757892283	0,384327196904
40	0,000000000000	0,000000000000	0,000000002565	0,000001729199	0,000196669843	0,006175123556	0,071242358545	0,350595018840
45	0,000000000000	0,000000000000	0,000000000260	0,000000388347	0,000078000807	0,003666948763	0,055529709603	0,320248210685
50	0,000000000000	0,000000000000	0,000000000027	0,000000087697	0,000031095400	0,002187324453	0,043406656003	0,292713530736
55	0,000000000000	0,000000000000	0,000000000003	0,000000019893	0,000012448799	0,001309453887	0,033996596291	0,267543330029
60	0,000000000000	0,000000000000	0,000000000000	0,000000004529	0,000005001348	0,000786156665	0,026654644160	0,244374188848
65	0,000000000000	0,000000000000	0,000000000000	0,000000001035	0,000002015247	0,000472983873	0,020899594928	0,222898912685
70	0,000000000000	0,000000000000	0,000000000000	0,000000000237	0,000000814006	0,000284915421	0,016368115609	0,202845003099
75	0,000000000000	0,000000000000	0,000000000000	0,000000000054	0,000000329401	0,000171616688	0,012782876401	0,183954443437
80	0,000000000000	0,000000000000	0,000000000000	0,000000000013	0,000000133406	0,000103139991	0,009929598364	0,165958383907
85	0,000000000000	0,000000000000	0,000000000000	0,000000000003	0,000000053942	0,000061585235	0,007639526511	0,148533054078
90	0,000000000000	0,000000000000	0,000000000000	0,000000000001	0,000000021620	0,000036191476	0,005773676084	0,131193297540
95	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000008367	0,000020386502	0,004198822974	0,112911933986
100	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000002596	0,000009459338	0,002635403356	0,088700615562

Практичні результати для атаки з чекпоінтами

Табл.: Ймовірність атаки подвійної витрати для випадку блокчейну з чекпоінтами (відстань між чекпоінтами $n = 150$).

$\frac{q}{z}$	0,1	0,15	0,2	0,25	0,3	0,35	0,4	0,45
5	0,001781840000	0,011257326211	0,039162880000	0,097854614258	0,197617320000	0,343438569794	0,533127123407	0,754773785784
10	0,000007859765	0,000287014738	0,003158241098	0,017806558608	0,065106713763	0,174947198906	0,372172064464	0,654469017168
15	0,000000039252	0,000008223010	0,000283612899	0,003568523309	0,023307657870	0,095273441874	0,272410928363	0,581753083020
20	0,000000000207	0,000000247918	0,000026719163	0,000747285193	0,008673864270	0,053573442967	0,204099653380	0,523571123530
25	0,000000000001	0,000000007694	0,000002587265	0,000160534957	0,003302727162	0,030712030645	0,155131072523	0,474846654674
30	0,000000000000	0,000000000243	0,000000255043	0,000035069920	0,001276875829	0,017837338878	0,119081631302	0,432942556691
35	0,000000000000	0,000000000008	0,000000025459	0,000007752863	0,000499069156	0,010458202267	0,092075853856	0,396267032667
40	0,000000000000	0,000000000000	0,000000002565	0,000001729199	0,000196670007	0,006176003848	0,071593760704	0,363764863631
45	0,000000000000	0,000000000000	0,000000000260	0,000000388347	0,000078000988	0,003667918727	0,055915903620	0,334689980429
50	0,000000000000	0,000000000000	0,000000000027	0,000000087697	0,000031095600	0,002188389886	0,043829597665	0,308489455084
55	0,000000000000	0,000000000000	0,000000000003	0,000000019893	0,000012449019	0,001310622620	0,034458940574	0,284738500816
60	0,000000000000	0,000000000000	0,000000000000	0,000000004529	0,000005001589	0,000787439125	0,027159914395	0,263101381344
65	0,000000000000	0,000000000000	0,000000000000	0,000000001035	0,000002015513	0,000474393995	0,021452459940	0,243306556750
70	0,000000000000	0,000000000000	0,000000000000	0,000000000237	0,000000814301	0,000286472154	0,016974843658	0,225130148831
75	0,000000000000	0,000000000000	0,000000000000	0,000000000054	0,000000329731	0,000173346614	0,013452108304	0,208384513280
80	0,000000000000	0,000000000000	0,000000000000	0,000000000013	0,000000133779	0,000105082216	0,010673758914	0,192910072478
85	0,000000000000	0,000000000000	0,000000000000	0,000000000003	0,000000054372	0,000063801596	0,008477689316	0,178569294172
90	0,000000000000	0,000000000000	0,000000000000	0,000000000001	0,000000022133	0,000038791893	0,006738429983	0,165242110603
95	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000009022	0,000023614677	0,005358449010	0,152822307815
100	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000003682	0,000014390588	0,004261646304	0,141214548436
105	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000001505	0,000008776967	0,003388445050	0,130331757346
110	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000615	0,000005356346	0,002692059485	0,120092608596
115	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000252	0,000003269544	0,002135636294	0,110418789446
120	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000103	0,000001994958	0,001690047596	0,101231526554
125	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000042	0,000001215453	0,001332167366	0,092446372814
130	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000017	0,000000737932	0,001043493568	0,083963955252
135	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000007	0,000000444609	0,000808974238	0,075650425020
140	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000003	0,000000263378	0,000615786122	0,067286308260
145	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000001	0,000000149443	0,000451083376	0,058379001691
150	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000069932	0,000286034141	0,046470439292

Практичні результати для атаки з чекпоінтами

Табл.: Ймовірність атаки подвійної витрати для випадку блокчейну з чекпоінтами (відстань між чекпоінтами $n = 200$).

$\frac{q}{z}$	0,1	0,15	0,2	0,25	0,3	0,35	0,4	0,45
5	0,001781840000	0,011257326211	0,039162880000	0,097854614258	0,197617320000	0,343438571047	0,533134636576	0,756125866792
10	0,000007859765	0,000287014738	0,003158241098	0,017806558608	0,065106713763	0,174947200730	0,372182994672	0,656435021106
15	0,000000039252	0,000008223010	0,000283612899	0,003568523309	0,023307657870	0,095273444155	0,272424592626	0,584209512729
20	0,000000000207	0,000000247918	0,000026719163	0,000747285193	0,008673864270	0,053573445654	0,204115734146	0,526460282281
25	0,000000000001	0,000000007694	0,000002587265	0,000160534957	0,003302727162	0,030712033708	0,155149391919	0,478135966926
30	0,000000000000	0,000000000243	0,000000255043	0,000035069920	0,001276875829	0,017837342300	0,119102083945	0,436612451479
35	0,000000000000	0,000000000008	0,000000025459	0,000007752863	0,000499069156	0,010458206039	0,092098379011	0,400305913040
40	0,000000000000	0,000000000000	0,000000002565	0,000001729199	0,000196670007	0,006176007966	0,071618328652	0,368166634922
45	0,000000000000	0,000000000000	0,000000000260	0,000000388347	0,000078000988	0,003667923191	0,055942508364	0,339452717950
50	0,000000000000	0,000000000000	0,000000000027	0,000000087697	0,000031095600	0,002188394698	0,043858252923	0,313614658360
55	0,000000000000	0,000000000000	0,000000000003	0,000000019893	0,000012449019	0,001310627788	0,034489677678	0,290230687739
60	0,000000000000	0,000000000000	0,000000000000	0,000000004529	0,000005001589	0,000787444658	0,027192781458	0,268967902899
65	0,000000000000	0,000000000000	0,000000000000	0,000000001035	0,000002015513	0,000474399905	0,021487521977	0,249557573293
70	0,000000000000	0,000000000000	0,000000000000	0,000000000237	0,000000814301	0,000286478457	0,017012183522	0,231778741347
75	0,000000000000	0,000000000000	0,000000000000	0,000000000054	0,000000329731	0,000173353331	0,013491828441	0,215446923563
80	0,000000000000	0,000000000000	0,000000000000	0,000000000013	0,000000133779	0,000105089370	0,010715984023	0,200406082166
85	0,000000000000	0,000000000000	0,000000000000	0,000000000003	0,000000054372	0,000063809215	0,008522570119	0,186522768372
90	0,000000000000	0,000000000000	0,000000000000	0,000000000001	0,000000022133	0,000038800014	0,006786148445	0,173681751227
95	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000009022	0,000023623341	0,005409225536	0,161782689041
100	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000003682	0,000014399848	0,004315749784	0,150737548857
105	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000001505	0,000008786888	0,003446207120	0,140468572918
110	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000615	0,000005367011	0,002753895343	0,130906651512
115	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000252	0,000003281061	0,002202076154	0,121990001609
120	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000103	0,000002007468	0,001761786403	0,113663077579
125	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000042	0,000001229156	0,001410148124	0,105875658468
130	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000017	0,000000753117	0,001129058337	0,098582068548
135	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000007	0,000000461730	0,000904169640	0,091740495599
140	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000003	0,000000283242	0,000724094503	0,085312375427
145	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000001	0,000000173836	0,000579782387	0,079261811431
150	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000106732	0,000464030860	0,073554993616
155	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000065549	0,000371100901	0,068159569658
160	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000040259	0,000296413404	0,063043895474
165	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000024720	0,000236308961	0,058176040304
170	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000015166	0,000187856792	0,053522307927
175	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000009287	0,000148701272	0,049044771061
180	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000005664	0,000116935587	0,044696627996
185	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000003427	0,000090990050	0,040412107221
190	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000002038	0,000069509188	0,036079746521
195	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000001161	0,000051108631	0,031444076792
200	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000545	0,000032584987	0,025217891626

Висновки

- Було здійснено огляд літератури за зазначеною тематикою дослідження;
- Ознайомилися з протоколами консенсусу Proof of Work та Proof of Stake, та атаками, що можуть відбутися у кожній консенсусній моделі;
- Отримано явний вираз імовірності для атаки подвійної витрати на протокол консенсусу Proof of Stake за умови існування чекпоінтів;
- Отримано чисельні результати за доведеною формулою, та переконалися, що вони підтверджують адекватність отриманої формули.

Дякую за увагу!