Зборник радова Факултета техничких наука, НовиСад

УДК: 4.9
ДОИ: https://doi.org/10.24867/34BE32Kacanski

Анализа и имплементација Тендерминт консензус алгоритма и његових варијација

Analysis and Implementation of the Tendermint Consensus Algorithm and Its Variations

Данило Кањански, *Факултет техничких наука, Нови Сад*

Студијски програм – РАЧУНАРСТВО И АУТОМАТИКА

Кратак садржај – *Овај рад се бави анализом и имплементацијом Тендерминт консензус алгоритма и његових варијација, које су настале као његове надоградње. У првом делу рада описане су теоријске основе, механизам постизања консензуса и варијације Тендерминта, док се други део рада односи на његову експерименталну симулацију. Добијени резултати показују да Тендерминт задржава кључне особине чак и у присуству византијских валидатора, чиме се потврђује примењивост у савременим blockchain системима.*

Кључне речи (три до пет): *Тендерминт консензус, Византијска толеранција на грешке, Дистрибуирани системи, Blockchain*

Abstract – *This paper focuses on the analysis and implementation of the Tendermint consensus algorithm and its variations, which have emerged as extensions of it. The first part of the paper describes the theoretical foundations, the mechanism of achieving consensus, and the variations of Tendermint, while the second part is dedicated to its experimental simulation. The obtained results demonstrate that Tendermint preserves its key properties even in the presence of the Byzantine validators, thereby confirming its applicability in modern blockchain systems.*

Keywords: (three to five): *Tendermint consensus, Byzantine fault tolerance, Distributed systems, Blockchain*

НАПОМЕНА: Овај рад проистекао је из мастер рада чији ментор је био др Дарко Чапко, ред. проф.

1. УВОД

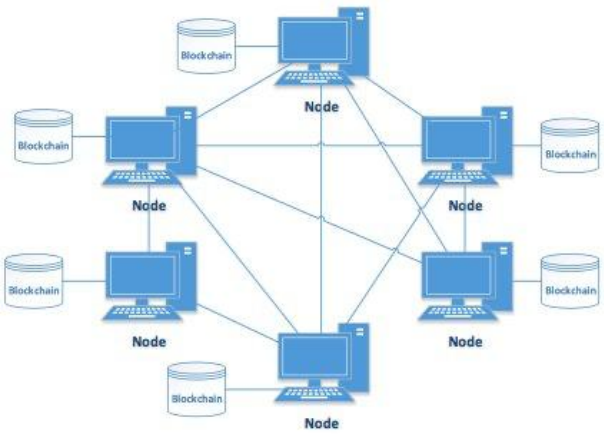
Постизање договора око неке вредности је одувек био један од **главних проблема у дистрибуираним системима**. Развитком технологије и настанком *blockchain* система, овај проблем добија још једну димензију. Сада је број валидатора за неколико реда величина већи, не припадају истом административном домену и прети опасност од злонамерних (византијских). Алгоритми који су се претходно користили, као што су *Paxos* и *Raft*, нису више примењиви због ових нових проблема који доносе *blockchain* системи. Управо из тог разлога су развијени *BFT (Byzantine Fault Tolerant)* алгоритми који омогућавају консензус, чак и када се део валидатора понаша злонамерно [6].

Једно од најпознатијих *BFT* решења је **Тендерминт**, алгоритам који започиње предлогом за додавање блока од стране лидера, и наставља се гласањем кроз даље фазе. За разлику од осталих приступа, Тендерминт омогућава додавање валидних блокова са високом отпорношћу на византијске валидаторе. Његова једноставност и могућност примене у *Proof-of-Stake* системима учинили су га **основом за велики број модерних *blockchain* мрежа** [1].

Осим **анализе** и **имплементације Тендерминт консензус алгоритма**, дат је и **преглед његових варијација**, које су настале ради превазиласка неких од његових недостатака [5,7,8]. Помоћу експерименталне симулације која је имплементирана, могуће је испитивање најважнијих особина Тендерминта и његово тестирање под различитим комбинацијама параметара мреже и валидатора.

2. ТЕНДЕРМИНТ АЛГОРИТАМ

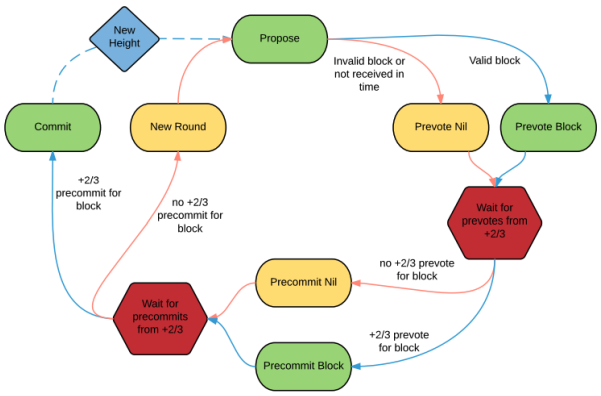
Тендерминт је дизајниран тако да обезбеди **детерминистичку финалност** блока, другим речима једном када је блок прихваћен, он више не може бити опозван [1].



Слика 1. Мрежа валидатора у *blockchain* систему [2]

Структуриран је тако да се на свакој висини, по потреби понавља кроз рунде. У свакој рунди бира се један лидер који предлаже нови блок, док остали валидатори гласају у више фаза како би одредили да ли ће предлог бити прихваћен.
Основне фазе Тендерминта су:

Propose → Prevote → Precommit → Commit → NewHeight



Слика 2. Главне фазе Тендерминт консензуса [4]

У случају да у некој рунди не дође до прихватања блока (на пример због кашњења порука или неактивног лидера), покреће се нова рунда са новим лидером. Оваква структура алгоритма гарантује прогресивност, јер се рунде настављају све док се не постигне консензус.
У фази *Propose*, лидер предлаже нови блок, који садржи скуп трансакција и хеш претходног блока. Током *Prevote* фазе сваки валидатор гласа за предложени блок или за *nil* (уколико га сматра неважећим).
Ако се више од две трећине валидатора сложи око истог блока, систем прелази у наредну фазу *Precommit,* у којој се гласови потврђују и валидатори закључавају на ту вредност.
Када више од две трећине валидатора пошаље *precommit* за исти блок, он се сматра потврђеним (*Commit*) и додаје у *blockchain.*
Да би све ово постигао, Тендерминт користи систем тајмера који спречава да било која од наведених фаза траје неограничено. Уколико време истекне, чворови прелазе у нову рунду, тајмер се експоненцијално увећава, чиме се гарантује прогресивност и финалност у неком тренутку, чак и у делимично синхроним условима.

3. БЕЗБЕДНОСТ и ПРОГРЕСИВНОСТ

Најважнија карактеристика Тендерминта јесте његова гаранција **безбедности** (*safety*) и **прогресивности** (*liveness*) [1]. Безбедност значи да ниједна два исправна чвора неће потврдити различите блокове на истој висини, док прогресивност осигурава да ће систем, без обзира на застоје и губитке порука, пре или касније доћи до консензуса.
Механизам који омогућава ове две особине је **закључавање блокова**. Када валидатор током *Precommit* фазе пошаље глас за неки блок, он се онда закључава на исти, и не може да подржи ниједан други на истој висини док не добије потврду да је систем напредовао. На овај начин се спречава појава конфликтних потврда и одржава конзистентност *blockchain*-а.
Детаљније, да би се прогресивност обезбедила, сваки валидатор има локалне промењиве *validRound* и *validValue*, у којима се чува последња рунда и вредност за коју је добијена двотрећинска већина у *Prevote* фази. Лидер ове информације користи у наредним рундама како би предложио блок са којим је задовољна већина валидатора без додатног гласања. Због тога се знатно смањује стагнација, и систем напредује чак и у делимично синхроном окружењу.
Да би се решио случај када нека фаза траје предуго, уводи се **систем тајмера** (*timeoutPropose, timeoutPrevote, timeoutPrecommit*). Време трајања се увећава експоненцијално, тако да и у случају да поруке касне пуно, консензус се постиже по истеку времена стабилизације мреже.
Тендерминт помоћу овакве структуре осигурава да се може донети само једна одлука, и да се процес не може трајно зауставити, а управо тиме истовремено гарантује и безбедност и прогресивност.

4. ВАРИЈАЦИЈЕ И НАДОГРАДЊЕ ТЕНДЕРМИНТА

Развој Тендерминта је подстакао настанак више варијанти и надоградњи које су имале за циљ да побољшају његове различите аспекте. У почетним фазама развоја, **фокус** је био на **формалним доказима исправности** Тендерминта, као што је приказано у раду *Correctness of Tendermint-Core Blockchains* [6], док су каснији радови попут *Lock-free Enhanced Tendermint* [7], *Tenderbake* [5] и *TenderTee* [8] направили **конкретна** и **практична побољшања**.
Ове три варијације у већој или мањој мери модификују Тендерминт, уводећи нове механизме за избор валидатора, убрзавање консензуса и повећање безбедности, тако да ће у наставку бити нешто више речи о њима.

4.1. LOCK-FREE ENHANCED TENDERMINT

Прва модификација, представљена у раду *Fair and Trustworthy: Lock-free Enhanced Tendermint Blockchain Algorithm* [7], се односи на низ побољшања усмерених ка **пропусности** система и **избегавања застоја** у комуникацији.
Најважнија модификација је увођење *lock-free* приступа, чиме се уклања закључавање током фаза гласања. Као што је већ напоменуто, у Тендерминту се валидатори закључавају на вредност блока, док се у овој верзији фазе гласања извршавају паралелно, док се само *Commit* фаза извршава секвенцијално. Овим приступом се смањује време потребно за достизање консензуса, и постиже се линеаризабилност, тј. особина да су резултати добијени конкурентним извршавањем програма идентични као и код секвенцијалног извршавања.
Друга иновација се односи на **динамичко одређивање скупа валидатор**а, али тако да се број валидатора подешава помоћу нивоа поузданости и осетљивости података. У случају да је поверење у мрежи високо

мањи број валидатора је довољан, док се у критичним ситуацијама користи већи скуп валидатора.
Наредно побољшање је **фер избор валидатора** помоћу стохастичког алгоритма *random walk*, којим се смањује вероватноћа пристрасности и повећава униформност добијања награда.
За крај, последња модификација ове варијације је *wait-freedom* механизам. Он након истека дефинисаног времена, све поруке које нису пристигле третира као *nil* гласове. Због тога се консензус увек завршава у коначном времену, чиме се постиже још већи степен прогресивности.

4.2. TENDERBAKE

Наредна варијација је *Tenderbake*, који се не бави само формалном теоријом, већ проналази и своју **примену** и *Tezos blockchain*-у [5].
Он уводи концепт **динамичког поновљеног консензуса** (*Dynamic Repeated Consensus - DRC*), где се састав валидатора може мењати кроз сваку рунду, али не као у претходној верзији кроз подскупове, већ додавањем и уклањањем валидатора, који су купили и продали токен задужен за расподелу гласачке снаге. Како аутори рада наводе основна својства која сваки *DRC* мора задовољити (*Agreement*, *Validity* и Progress) обезбеђују да се све одлуке доносе конзистентно и да *blockchain* расте континуирано.
Друга модификације је увођење *best-effort broadcast*-а, помоћу ког се елиминише потреба за поузданим слањем порука. Овако се толерише губитак порука без утицаја на сигурност система, а истовремено се и мрежно оптерећење значајно смањује.
Трећа иновација је употреба **кворум сертификата** (*Quorum Certificates - QC*) који представљају агрегиране криптографске потписе валидатора. Захваљујући њима, *Tenderbake* постиже консензус у највише $f + 2$ рунде (где је f број византијских валидатора), што је велико побољшање у односу на Тендерминт где је таква гаранција била могућа тек у случају када се прођу сви валидатори.
Захваљујући овим изменама, *Tenderbake* доноси брже и ефикасније доношење одлука у делимично синхроном окружењу и као што је већ наведено успешно је интегрисан у *Tezos blockchain*, што потврђује његову примену у пракси.

4.3. TENDERTEE

Последња обрађена варијација јесте *TenderTee*, и усмерена је ка **повећању безбедности** и **отпорности** на византијске валидаторе [8]. За разлику од претходних приступа који су имали друге предмете оптимизације, *TenderTee* **помера границу толеранције** на византијске валидаторе са $f < \frac{n}{3}$ на $f < \frac{n}{2}$, што представља значајан корак у детерминистичким *PBFT* протоколима.
Ово је постигнуто увођењем **хардверске компоненте** *Attested Append-Only Memory (A2M)*, која гарантује да ће свака порука бити јединствено забележена и непромењива. Такође изразито битна ствар је то што *A2M* гарантује да валидатор не може послати две различите поруке у истој рунди, чиме се елиминише најгора верзија византијског понашања *equivocation*.
Сем тога, свака порука садржи и **дигиталан потпис**, који је заснован на систему јавних кључева, што омогућава да се сваки корак консензуса криптографски провери. На овај начин уз помоћ *A2M* се ствара **двострука заштита**, комбинацијом хардверског и софтверског слоја.
За крај, *TenderTee* даје и формално дефинисање **поновљеног консензуса**, који осигурава да ће сви исправни валидатори имати идентичан *blockchain* и након произвољно великог броја итерација, за разлику од осталих приступа који су помоћу индукције гарантовали ову особину. На овај начин се обезбеђује детерминистичка финалност и непромењивост одлуке, што је кључно за примену у реалним *blockchain* системима.

4.4. ЗАКЉУЧАК

Приказане варијације показују **континуирану еволуцију Тендерминта**, бавећи се унапређивањем његових различитих карактеристика. *Lock-free Enhanced Tendermint* [5] повећава ефикасност и флексибилност, *Tenderbake* [7] формализује динамички консензус и смањује број потребних рунди, док *TenderTee* [8] проширује границе безбедности и уводи хардверску заштиту од византијског понашања.
Све три варијације имају исту суштину, а свака уноси додатни степен сигурности, скалабилности или правичности, што чини Тендерминт темељем савремених *PBFT* протокола који се налазе иза модерних *Proof-of-Stake* система.

5. ИМПЛЕМЕНТАЦИЈА

Имплементација је реализована у програмском језику **Go**, због изразите подршке за конкурентно програмирање и једноставног управљања асинхроним догађајима у мрежи. Главни циљ имплементације је био да се изгради симулација која представља експериментално окружење у којем се може испитати понашање Тендерминта у различитим мрежним и византијским условима [1]. Систем је подељен на три нивоа: **консензус језгро**, **мрежни слој** и **конфигурациони интерфејс**.
Консензус језгро симулира све фазе алгоритма (*Propose*, *Prevote*, *Precommit* и *Commit*) и прати кључне промењиве као што су *lockedValue*, *lockedRound*, *validValue* и *ValidRound* које служе да би се обезбедила безбедност и прогресивност консензуса. Лидер се бира насумично, пропорционално гласачкој снази, док се процес гласања одвија кроз рунде са временским ограничењима. Уколико дође до истека времена, помоћу система тајмера, рунда се аутоматски понавља са новим лидером, без чега не би било могуће гарантовати завршетак алгоритма, тј. прогресивност.
Мрежни слој је заснован на *in-memory gossip* протоколу који омогућава симулацију реалних услова у мрежи, укључујући кашњења, губитке порука и насумичне поремећаје (*jitter*). Сваки валидатор спроводи комуникацију преко посебних канала, а поруке бивају потписане и верификоване од стране *Ed25519* алгоритма. Поред стандардних подешавања мрежа подржава моделовање различитих врста византијског понашања као што су ћутање, намерно

гласање за *nil* или слање контрадикторних порука. На овај начин могуће је тестирање свих особина протокола, под свим могућим условима.
На највишем нивоу се налази **конфигурациони слој**, који омогућава покретање једне или више симулација са различитим параметрима. Корисник може дефинисати број валидатора, расподелу гласачке снаге, понашање сваког од њих, топологију мреже, трајање свих кључних промењивих, итд. Резултати се аутоматски чувају у *.csv* форматима и садрже све кључне метрике потребне за даљу анализу.
Додатно, реализовани су различити **тестни сценарији**, чију израду и интеграцију пружа језик *Go*. Окружење је дефинисано тако да испитује кључне особине Тендерминта и његову исправност у различитим условима. Тестови се извршавају без кашњења и насумичних одступања, да би се обезбедило њихово детерминистичко извршавање. У оквиру тестног модула се испитују случајеви као што су постизање консензуса уз присуство византијских валидатора, прекид рада симулације у случају прекорачења прага броја византијских валидатора (преузето из практичних решења) и стабилност у случају ограничене комуникације. Овакав модул за тестирање омогућава брзу проверу исправности протокола и његових особина, као и лако проширење новим тестовима. Захваљујући томе, након сваке веће промене симулатора, може се лако написати нови тестни случај, и на брз и коректан начин проверити исправност Тендерминта са новим проширењима.

6. ЗАКЉУЧАК

Рад је представио **теоријску анализу Тендерминта** [1], **његове варијације** и **практичну имплементацију**, који данас чини основу за велики број *Proof-of-Stake blockchain*-ова. Нагласак овог рада јесте на повезивању теоријских принципа са практичним механизмима примене, како би се истакла практична вредност Тендерминта у реалним условима имплементације децентрализованих мрежа, које захтевају висок ниво поузданости. Кроз приказ основног алгоритма и његових варијација (*Lock-Free Enhanced Tendermint*, *Tenderbake* и *TenderTee* [5, 7, 8]), показано је како се исти концепт развијао од почетног *PBFT* решења, до напредних система који обезбеђују већу ефикасност, флексибилност и отпорност на византијске валидаторе.
Развијена имплементација доказује да је могуће детерминистички и експериментално утврдити понашање Тендерминта у контролисаном окружењу, као и пратити утицај свих подесивих хиперпараметара мреже и валидатора. На основу симулација је потврђено да Тендерминт задржава своје кључне особине, безбедност и прогресивност, чак и у граничним случајевима што се тиче броја византијских валидатора и непропусности мреже.
Симулатор представља **добру основу** за даљу **квантитативну анализу** Тендерминта и **његова проширења**. Проширења која се природно настављају на већ имплементиран алгоритам јесу увођење реалног *ABCI* слоја, динамички избор валидатора и права *P2P* комуникација. Након тога би такође било занимљиво пробати неке од техника које варијације Тендерминта користе.
Овим рад заокружује целу причу око развоја и практичне примене Тендерминт консензус алгоритма, који је један од најзначајнијих ослонаца модерних *PBFT blockchain* система.

7. ЛИТЕРАТУРА

[1] Buchman, Ethan, Jae Kwon, and Zarko Milosevic. "*The latest gossip on BFT consensus.*" arXiv preprint arXiv:1807.04938 (2018).

[2] Koteska, Bojana, Elena Karafiloski, and Anastas Mishev. "*Blockchain implementation quality challenges: a literature*." In SQAMIA 2017: 6th workshop of software quality, analysis, monitoring, improvement, and applications, vol. 11, p. 2017. 2017.

[3] Bounceur, Ahcène, Ahmed-Sami Berkani, Hamouma Moumen, and Saber Benharzallah. "*The Transparency Challenge in Blockchain-Enabled Sustainable Development Goals Applications: Exploring Privacy-Preserving Techniques and Emerging Platforms.*" IEEE Access (2025).

[4] Lagaillardie, Nicolas, Mohamed Aimen Djari, and Önder Gürcan. "*A computational study on fairness of the tendermint blockchain protocol."* Information 10, no. 12 (2019): 378.

[5] Aştefanoaei, Lăcrămioara, Pierre Chambart, Antonella Del Pozzo, Thibault Rieutord, Sara Tucci, and Eugen Zălinescu. "*Tenderbake--A Solution to Dynamic Repeated Consensus for Blockchains.*" arXiv preprint arXiv:2001.11965 (2020).

[6] Amoussou-Guenou, Yackolley, Antonella Del Pozzo, Maria Potop-Butucaru, and Sara Tucci-Piergiovanni. "*Correctness of tendermint-core blockchains.*" In 22nd International Conference on Principles of Distributed Systems (OPODIS 2018), pp. 16-1. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2019.

[7] Assiri, Basem, and Wazir Zada Khan. "*Fair and trustworthy: Lock-free enhanced tendermint blockchain algorithm.*" TELKOMNIKA (Telecommunication Computing Electronics and Control) 18, no. 4 (2020): 2224-2234.

[8] Beltrando, Lionel, Maria Potop-Butucaru, and Jose Alfaro. "*TenderTee: Secure Tendermint.*" Cryptology ePrint Archive (2022).

Кратка биографија:

Данило Каћански рођен је у Новом Саду 2001. год. Мастер рад на Факултету техничких наука из области Електротехнике и рачунарства одбранио је 2025. год.
Контакт:
kacanski.ra26.2020@gmail.com