TESIS

PENYELESAIAN TRILEMMA UNTUK SKALABILITAS & KEAMANAN BLOCKCHAIN MENGGUNAKAN ALGORITMA TERKINI

Disusun oleh:

Nama : **Nur Arifin Akbar**
NIM : **19.77.1233**
Konsentrasi : **Informatics Technopreneurship**

PROGRAM STUDI S2 TEKNIK INFORMATIKA
PROGRAM PASCASARJANA UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2021

TESIS

PENYELESAIAN TRILEMMA UNTUK SKALABILITAS & KEAMANAN BLOCKCHAIN MENGGUNAKAN ALGORITMA TERKINI

SOLVING A TRILEMMA FOR BLOCKCHAIN SCALABILITY & SECURITY USING NOVEL ALGORITHM

Diajukan melalui Jalur Lomba dengan Publikasi
untuk memenuhi salah satu syarat memperoleh derajat Magister

Disusun oleh:

Nama : **Nur Arifin Akbar**
NIM : **19.77.1233**
Konsentrasi : **Informatics Technopreneurship**

PROGRAM STUDI S2 TEKNIK INFORMATIKA
PROGRAM PASCASARJANA UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2021

HALAMAN PENGESAHAN

PENYELESAIAN TRILEMMA UNTUK SKALABILITAS & KEAMANAN BLOCKCHAIN MENGGUNAKAN ALGORITMA TERKINI

SOLVING A TRILEMMA FOR BLOCKCHAIN SCALABILITY & SECURITY USING NOVEL ALGORITHM

Dipersiapkan dan Disusun oleh

Nur Arifin Akbar

19.77.1233

Telah Diujikan dan Dipertahankan dalam Sidang Ujian Tesis
Program Studi S2 Teknik Informatika
Program Pascasarjana Universitas AMIKOM Yogyakarta
pada hari Senin, 07 Juni 2021

Tesis ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Magister Komputer

Yogyakarta, 07 Juni 2021
Rektor

Prof. Dr. M. Suyanto, M.M.
NIK. 190302001

HALAMAN PERSETUJUAN

PENYELESAIAN TRILEMMA UNTUK SKALABILITAS & KEAMANAN BLOCKCHAIN MENGGUNAKAN ALGORITMA TERKINI

SOLVING A TRILEMMA FOR BLOCKCHAIN SCALABILITY & SECURITY USING NOVEL ALGORITHM

Dipersiapkan dan Disusun oleh

Nur Arifin Akbar

19.77.1233

Telah Diujikan dan Dipertahankan dalam Sidang Ujian Tesis
Program Studi S2 Teknik Informatika
Program Pascasarjana Universitas AMIKOM Yogyakarta
pada hari Senin, 07 Juni 2021

Pembimbing Utama

Dr. Andi Sunyoto M.Kom
NIK. 190302052

Pembimbing Pendamping

M. Rudyanto Arief M.T
NIK. 190302098

Anggota Tim Penguji

Prof. Dr. Ema Utami, S.Si., M.Kom
NIK. 190302037

Dr. Kusrini M.Kom
NIK. 190302106

Dr. Andi Sunyoto M.Kom
NIK. 190302052

Tesis ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Magister Komputer

Yogyakarta, 07 Juni 2021
Direktur Program Pascasarjana

Dr. Kusrini, M.Kom.
NIK. 190302106

HALAMAN PERNYATAAN KEASLIAN TESIS

Yang bertandatangan di bawah ini,

Nama mahasiswa : Nur Arifin Akbar
NIM : 19.77.1233
Konsentrasi : Informatics Technopreneurship

Menyatakan bahwa Tesis dengan judul berikut:
Penyelesaian Trilemma Untuk Skalabilitas & Keamanan Blockchain Menggunakan Algoritma Terkini

Dosen Pembimbing Utama : Dr. Andi Sunyoto, M.Kom
Dosen Pembimbing Pendamping : M. Rudyanto Arief, M.T.

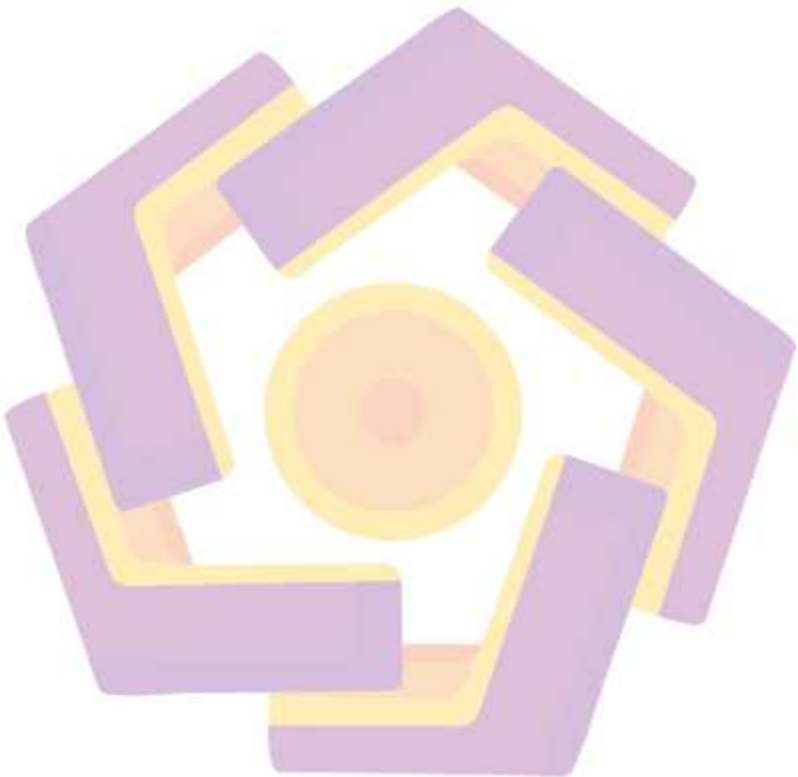
1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Tim Dosen Pembimbing
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi

Yogyakarta, 05 Juni 2021
Yang Menyatakan,

Nur Arifin Akbar

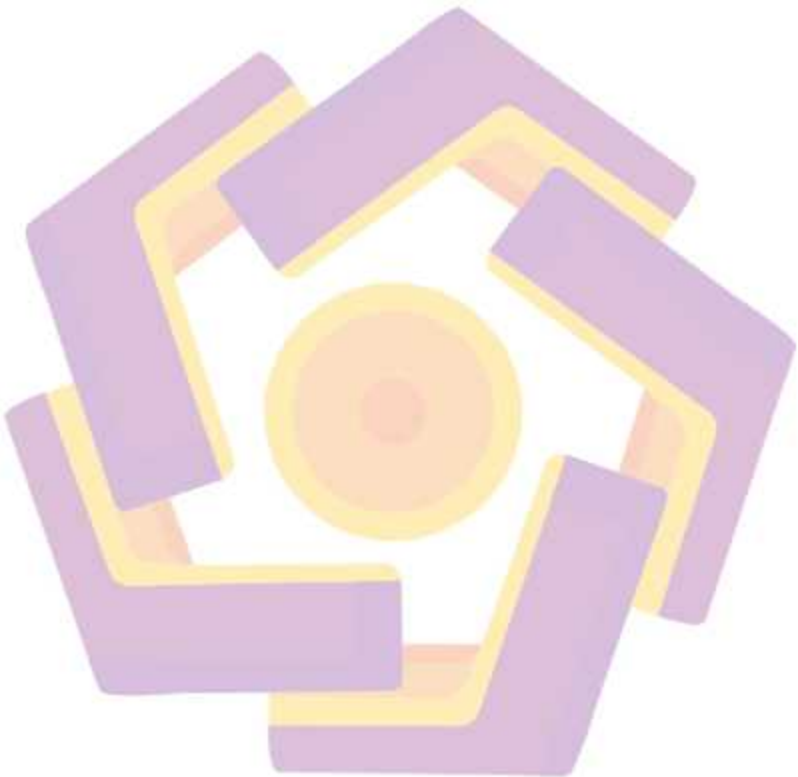
HALAMAN PERSEMBAHAN

Tesis ini saya persembahkan untuk keluarga besar yang telah memberikan dukungan kepada saya, kepada tim Plasma Nation yang telah bekerja keras dalam pengembangan produk Plasmanation dan kepada Bapak/Ibu pembimbing yang telah membimbing saya dalam pengembangan produk Plasmanation dan dalam pelaksanaan prosesi Tesis.



HALAMAN MOTTO

Lampu Hijau Itu Kehadirannya Sangat Ditunggu-tunggu, Tapi Begitu Dia Muncul Langsung Ditinggalkan



KATA PENGANTAR

Dengan memanjatkan puji dan syukur ke hadirat Allah SWT atas segala rahmat dan karunia-NYA, akhirnya penulis dapat menyelesaikan penyusunan tesis yang berjudul: Penyelesaian Trilemma Untuk Skalabilitas & Keamanan Blockchain Menggunakan Algoritma Terkini (*Solving a Trilemma for Blockchain Scalability & Security Using Novel Algorithm*). Tesis ini ditulis dalam rangka memunuhi sebagian persyaratan untuk memperoleh gelar Magister Teknik Informatika di program Pascasarjana Universitas AMIKOM Yogyakarta.

Penulis menyadari bahwa tesis ini dapat diselesaikan berkat dukungan dan bantuan dari berbagai pihak. Oleh karena itu, penulis berterimakasih kepada semua pihak yang secara langsung dan tidak langsung memberikan kontribusi dalam penyelesaian tesis ini. Secara khusus pada kesempatan ini penulis menyampaikan terima kasih kepada: Dr. Andi Sunyoto M.Kom selaku pembimbing I dan M. Rudyanto Arief, M.T. selaku Pembimbing II, yang telah membimbing dari awal hingga tesis ini dapat diselesaikan.

Kiranya penulis berharap tesis ini dapat memberi manfaat bagi dunia pendidikan dan masyarakat.

Banyumas, Juni 2021

Penulis

BAB I

DESKRIPSI KARYA LOMBA

1.1. Uraian Tentang Karya

Wabah virus corona (COVID-19) pada akhir 2019 menyebabkan keadaan darurat kesehatan global di seluruh dunia [1]. Hanya dalam waktu tiga bulan, jumlah kasus baru virus corona telah meningkat menjadi lebih dari satu juta di seluruh dunia. Penularan virus yang cepat menyebabkan kasus-kasus baru dilaporkan secara global per jam. Secara bersamaan, jumlah kematian dan infeksi terus meningkat dengan cepat. Akibatnya, pandemi COVID-19 telah memberlakukan lockdown dan pedoman jarak sosial yang mempengaruhi ekonomi global secara negatif. Ini telah menyebabkan pembatalan banyak kegiatan penting dunia, termasuk acara olahraga seperti Olimpiade Tokyo [2] dan Dubai Expo [3]. Akibatnya, pejabat pemerintah dan ilmuwan di seluruh dunia telah bekerja keras untuk mengembangkan penyembuhan dan memprediksi potensi lintasan pertumbuhan virus sejak beberapa kasus pertama yang dilaporkan ke Organisasi Kesehatan Dunia (WHO).

Selain memperkirakan korban dan pertumbuhan kasus COVID19, banyak laporan juga menghitung kasus aktif dan pulih yang dikumpulkan dari badan kesehatan pemerintah nasional dan negara bagian bersama dengan laporan media lokal.

Beberapa organisasi bahkan telah mengembangkan dasbor berbasis peta untuk melacak informasi penyebaran covid. Memahami dinamika pandemi membutuhkan data yang baik untuk memprediksi seberapa cepat penyakit menyebar, apakah penanggulangan efektif atau tidak, dan dampaknya terhadap kehidupan orang. Namun, data yang tersedia secara online mungkin tidak sempurna karena rentan terhadap manipulasi data.

Oleh karena itu, teknologi inovatif seperti deep learning, machine learning, kecerdasan buatan (AI), dan blockchain dapat membantu memerangi krisis. Secara khusus, teknologi blockchain memiliki potensi untuk merevolusi berbagai industri, termasuk keuangan, supply chain, dan bidang kesehatan. Blockchain adalah

teknologi terdesentralisasi dengan fitur yang berbeda seperti tamper-proof, secure-encrypted, immutable. Ini adalah buku besar terdistribusi yang berisi rantai blok. Platform terdesentralisasi Blockchain tidak dapat dirusak karena teknologi kriptografi yang mendasarinya, yang digunakan untuk mengautentikasi participant dalam jaringan. Selain itu, membutuhkan banyak sumber daya untuk dapat memodifikasi transaksi yang ditambahkan ke jaringan blockchain karena setelah transaksi divalidasi dan diverifikasi, maka transaksi tersebut akan dicocokan ke transaksi sebelumnya dengan hash yang unik. Oleh karena itu, memanipulasi satu transaksi akan mengubah hash ini, dan semua member akan di broadcast sehingga hampir mustahil untuk memperbarui atau menghapus data. Selanjutnya, data yang disimpan di blockchain tersedia untuk semua member jaringan, memastikan transparansi di antara para member.

Sehingga, dibuatlah sebuah platform berbasis blockchain untuk recovery ekonomi khususnya pada pandemic. Pada kali ini, penulis beserta team hackathon di Garudahacks membuat PoC (Proof of Concept) terkait dengan aplikasi Blockchain based Economy, dimana pada pandemic ini khususnya covid, mutasi pada virus masih kerap terjadi sehingga vaksin dianggap belum cukup efektif untuk menangani kasus tersebut, aplikasi ini akan dikhususkan untuk membuat sistem insentif donor plasma dengan ekonomi sekitar dengan nama Plasma Nation.

Plasma Nation adalah aplikasi donor plasma & darah yang diperuntukan khusus untuk untuk recovery plasma covid-19 serta donor darah pada umumnya. Cara kerja aplikasi ini menghubungkan berdasarkan radius-based, dimana user dapat mencari bank darah terdekat, serta push notification menggunakan one-signal. Adapun kedepannya aplikasi ini akan di hubungkan ke rewarding based berbasis blockchain, pre-assessment dengan parameter kesehatan baik dengan AI, serta reward yang didasarkan pada komunitas dikarenakan perekonomian yang anjlok akibat pandemic covid-19.

1.2. Latar Belakang Pengembangan

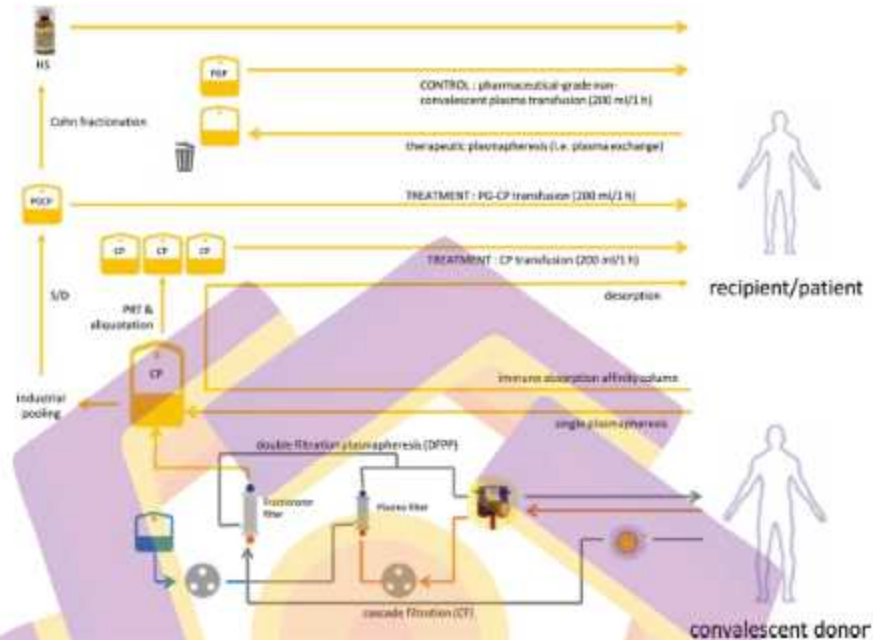
Meski banyak pasien Covid-19 sembuh, tapi sejauh ini belum ada obat khusus untuk mengobati orang yang terinfeksi virus corona. Salah satu metode pengobatan

yang efektif adalah dengan terapi dari donor darah plasma konvalesen.. Latar belakang dibuatnya aplikasi Plasmanation adalah dimana pada saat pandemic Covid-19, hampir seluruh masyarakat menerapkan social distancing, hal ini juga terjadi pada sektor kesehatan dimana pasien akan dibatasi di faskes itu sendiri khususnya pada aktivitas donor darah maupun plasma, dimana Social Distancing membatasi gerakan sehingga terjadilah kekurangan baik untuk terapi plasma convalescent maupun stock bank darah itu sendiri.

Plasma konvalesen adalah plasma darah yang diambil dari pasien Covid-19 yang telah sembuh, dan kemudian diproses agar dapat diberikan kepada pasien yang sedang dalam masa pemulihan setelah terinfeksi. Jadi, donor darah plasma konvalesen adalah donor darah dari penyintas Covid-19 untuk membantu pasien lain yang belum sembuh dari corona.

Terapi plasma konvalesen diberikan dengan cara mengambil plasma darah yang mengandung antibodi dari donor, kemudian ditransfusikan kepada pasien yang membutuhkan. Terapi plasma darah selama ini dinilai cukup aman digunakan untuk pasien COVID-19. Pasalnya, terapi ini juga sudah berjalan cukup lama dan digunakan untuk menangani SARS, MERS, Ebola dan Influenza H5N1.

Terapi plasma konvalesen dalam hal Covid-19, acuannya adalah penyintas penyakit itu diharapkan sudah membentuk antibodi. Plasma penyintas Covid-19 itu kemudian diberikan kepada orang lain yang sedang menghadapi infeksi virus corona. Secara sederhana, terapi plasma konvalesen bisa dipahami sebagai transfer antibodi antara penyintas suatu infeksi kepada orang yang sedang menghadapi infeksi.Terapi plasma konvalesen diberikan dengan cara mengambil plasma darah yang mengandung antibodi dari donor, kemudian ditransfusikan kepada pasien yang membutuhkan.



Gambar 1.1 Ilustrasi Donor Plasma Convalescent

1.3. Keunikan dan Value

Adapun Value dari Aplikasi Plasmanation adalah

a. Compliance dengan GDPR

GDPR adalah singkatan dari General Data Protection Regulation, sebuah peraturan tentang Data Privacy (perlindungan data) yang diterapkan bagi seluruh perusahaan di dunia yang menyimpan, mengolah atau memproses personal data penduduk dari 28 negara yang tergabung dalam EU (Uni Eropa). Dimana peraturan ini telah disetujui oleh otoritas Eropa sejak April 2016 dan akan berlaku secara efektif di seluruh dunia pada tanggal 25 May 2018. Fungsi utama dari GDPR adalah memberikan kontrol kepada konsumen atas data pribadi mereka yang dikumpulkan oleh perusahaan.

b. Push Notification

Ada Filtur Push Notification sebagai reminder dan news atas berita yang dikeluarkan oleh pihak Backend.

c. Radius-Based Optimization

Filtur dimana pendonor dan calon penerima melakukan transaksi di bank darah terdekat bedasarkan radius google maps.

d. History

Akan terdapat history dimana sang pendonor akan terlibat berapa kali pendonor dan reminder untuk donor darah secara rutin.

e. Pre-Assessment Module

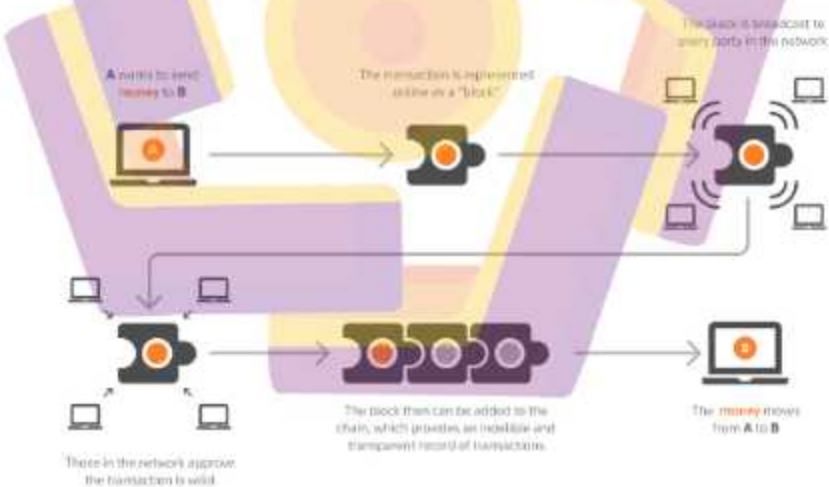
Tidak semua orang dapat dikategorikan sebagai donor plasma, oleh karena itu menurut informasi UDD PMI, ada 15 kriteria inklusi untuk memenuhi syarat donor plasma konvalesen, yaitu :

1. Berusia 18 sampai 60 tahun
2. Berat badan minimal 55 kg (sebab, pengambilan darah konvensional dengan kantong 450 ml)
3. Pemeriksaan tanda vital yang normal yakni tekanan darah systole 90-160 mmHg, tekanan darah diastole 60-100 mmHg, denyut nadi sekitar 50 sampai 100 kali per menit, dan suhu tubuh kurang dari 37 derajat celsius.
4. Terdiagnosis Covid-19 sebelumnya dengan real time PCR
5. Sudah dinyatakan sembuh oleh rumah sakit
6. Memiliki kadar Hemoglobin lebih dari 13.0 g/dL untuk pria dan lebih dari atau sama dengan 12.5 g/dL untuk wanita
7. Tidak leukopenia, limfopenia, trombositopenia, neutrofil lymphocyte ratio (NLR) kurang dari atau sama dengan 3,13.
8. Konsentrasi protein darah total lebih dari 6 g/dL atau albumin darah normal lebih dari 3,5 d/dL
9. Hasil uji saring IMTL terhadap sifilis, hepatitis B dan C serta HIV dengan CLIA/Elisa non-reakif

10. Hasil uji saring terhadap hepatitis B dan C serta HIV dengan NAT non-reaktif
11. Hasil skrining terhadap antibodi golongan darah negative
12. Hasil pemeriksaan Golongan Darah ABO dan rhesus dapat ditentukan
13. Tidak memiliki riwayat transfusi sebelumnya
14. Bersedia untuk menjalani prosedur plasmaferesis
15. Untuk donor wanita dipersyaratkan belum pernah hamil dan tidak memiliki antibodi anti-HLA/anti-HNA (namun tidak telalu direkomendasikan).

f. Blockchain Based Incentives (Upcoming)

Filtur ini memungkinkan transparency pada donor maupun unit donor darah yang menerima donor dari plasma itu sendiri, serta pemodelan decentralized pada ekosistem yang terkait.



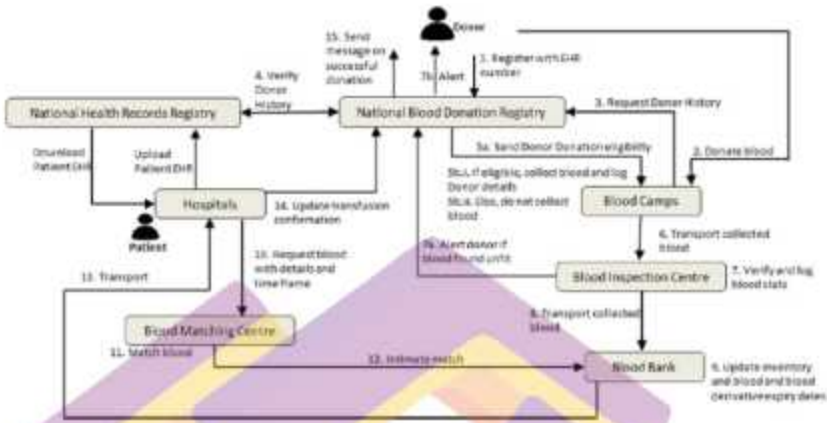
Gambar 1.2 Ilustrasi Blockchain

1.4. Fungsi, Fitur, dan Kegunaan

Adapun filtur yang terdapat pada plasmanation antara lain :

a. *Home Screen*
b. *Add Blood Donor*
c. *View Blood Donors*
d. *Call the donor*
e. *Add Blood Request*
f. *View Blood Requests*
g. *View Blood Banks*
h. *Call Function*
i. *Locate Function*
j. *Edit/Delete Blood Requests added by User*
k. *Edit/Delete Blood Donors added by User*
l. *Add Blood Donation Reminder*
m. *Settings*
n. *Send notification through admin panel*
o. *Manage Ad details from Admin panel*
p. *Manage Notifications from Admin panel*

Hal diatas adalah basic features dari program untuk donor berdasarkan lokasi, sedangkan untuk rewarding antara lain berupa token issue, business parter sign-up, serta listing UDD.



Gambar 1.3 Blood Donor dengan EHR systems

1.5. Inovasi, dan Implementasi atau Potensi

Innovasi ini berhasil menjuarai Garuda Hacks, dan mendapat award dari social team of the year dari script foundation untuk aplikasi plasmanation, sehingga aplikasi ini kedepannya diharapkan akan dapat terus sustain baik untuk donor plasma konvalesen ketika ada pandemi maupun donor darah secara rutin dengan memperhatikan rewarding yang sesuai untuk ekonomi local menggunakan blockchain.

Sedangkan untuk Backend stack yang digunakan antara lain :

Smart contract: a key aspect of Blockchain

Frontend: a React JS web client based on which Material UI is used.

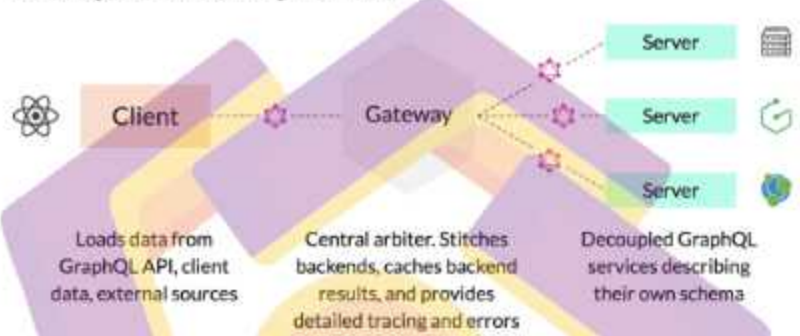
Hasura: A PostgresDB-based autogenerated GraphQL API.

API : a NodeJS back-end account management service, integration of wallet services and the synchronization of postgreSQL blockchain tables.

Digital wallet: All private keys are being saved and transactions signed by a service.

Nginx : a Web server that is also used to redirect external traffic to suitable services as a reverse proxy.

Potensi pada pengembangan blockchain pada saat ini masih terbatas, dikarenakan teknologinya belum terlalu mature, sedangkan kebanyakan aplikasi decentralized application berbasis pada Ethereum, dimana hal tersebut tidak efisien. Oleh karena itu, pada BAB 2, penulis akan membahas beberapa cara untuk menyelesaikan masalah scaling pada blockchain serta kemungkinan untuk menerapkan protocol baru di layer tertentu secara pseudocode.



Gambar 1.4 Backend Stack

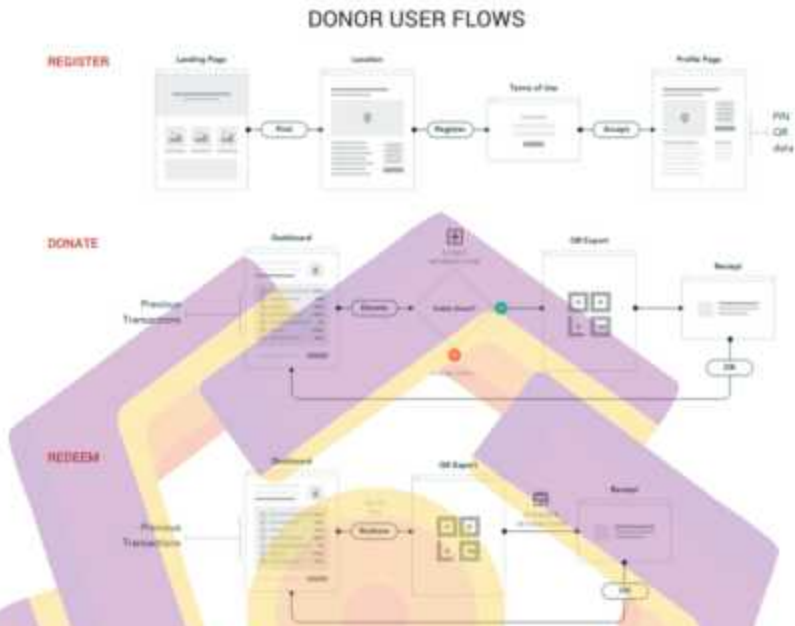
1.5.1 Mekanisme Donor Plasma

a. Donor telah memenuhi kriteria pada pre-skrining yang sudah dilakuan sehari sebelumnya. Pre-skrining yakni kondisi memiliki antibodi dan hasil negatif terhadap beberapa pemeriksaan keamanan darah, serta memenuhi standar pemeriksaan laboratorium sesuai dengan persyaratan.

b. Pengambilan plasma konvalesen dengan metode apheresis sebanyak 400 sampai 600 ml pada hari selanjutnya.

c. Adapun pengambilan plasma konvalesen dapat dilakukan sesuai petunjuk teknik BPOM. Namun, jika UDD PMI belum memiliki alat apheresis dan belum tersertifikasi CPOB, maka pengambilan dapat dilakukan dengan cara konvensional atau menggunakan kantong 450 ml.

d. Dalam pengambilan plasma konvalesen, petugas tetap memperhatikan kualitas dan keamanan yang dapat dipertanggungjawabkan.



Gambar 1.5 Ilustrasi Donor Plasma Convalescent

1.5.2 Mekanisme Permintaan Plasma di Faskes

Berikut rincian masing-masing tahap alur permintaan plasma konvalesen:

a. Pasien yang membutuhkan transfusi plasma konvalesen.

Untuk tahap ini, pasien yang membutuhkan transfusi plasma konvalesen harus mendapatkan surat permintaan plasma konvalesen dari dokter yang merawat. Kemudian, pihak yang bersangkutan membawa sampel pasien.

b. UDD PMI

Selanjutnya petugas rumah sakit atau keluarga pasien menuju front desk khusus pelayanan plasma konvalesen di UDD PMI/loket khusus. Sebelum melakukan transfusi, pihak keluarga sebaiknya menghubungi petugas rumah sakit untuk menanyakan ketersediaan plasma konvalesen di setiap

UDD PMI. Langkah berikutnya yakni penerimaan petugas khusus di UDD PMI. Kemudian, melakukan pemeriksaan uji kecocokan dan menyerahkan plasma konvalesen untuk ditransfusikan.

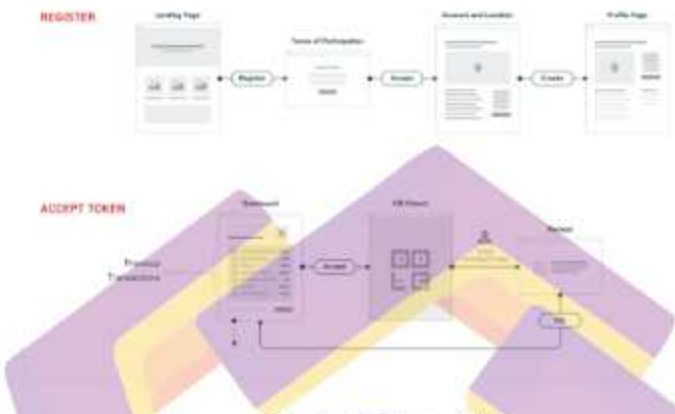
c. Rumah sakit

Setelah selesai melakukan proses tertentu di UDD PMI, petugas rumah sakit atau keluarga pasien membawa plasma konvalesen yang sudah disiapkan dan dicocokkan untuk pasien. Kemudian, dilakukan pencairan plasma oleh petugas kesehatan tertentu. Jika sudah siap, proses transfusi plasma konvalesen dilaksanakan di bangsal rumah sakit.

Gambar 1.6 Ilustrasi Faskes

1.5.3 Mekanisme Redeem Token dari Sponsor

Apabila terjadi transaksi antara pendonor dan penerima (match), maka dari sistem akan mengeluarkan token dengan jumlah sesuai skala prioritas, dari angka 1-3, semakin urgent maka akan semakin tinggi. Dari pendonor bisa meredeem point dengan ditukar pada sponsor terdekat untuk mendapatkan reward.



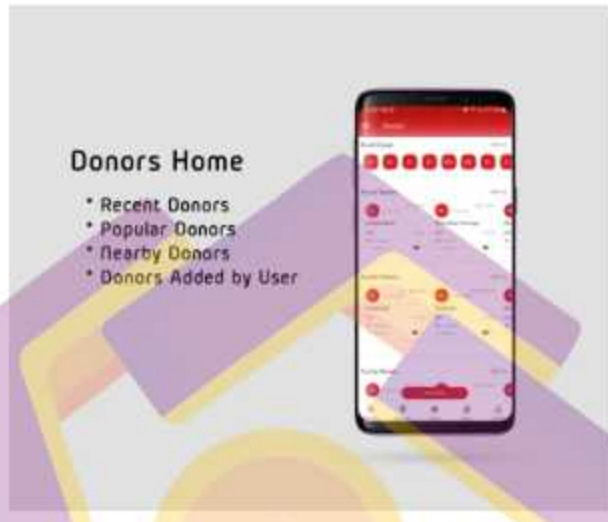
Gambar 1.7 Ilustrasi Sponsor

1.5.4 Blockchain Scaling Potential

Ada beberapa cara untuk menscaling aplikasi pada blockchain, namun pada kasus ini penulis akan menggunakan layer HTTP sehingga tidak perlu redeploy pada smart contract yang mengakibatkan kemungkinan data hilang pada blockchain yang berbasis non-upgradable contracts.

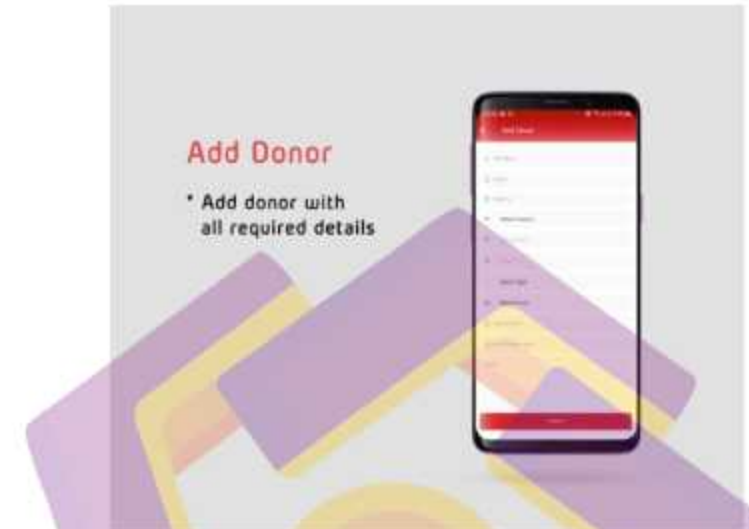
Gambar 1.8 Solusi Existing pada Scaling

1.6. Screenshot

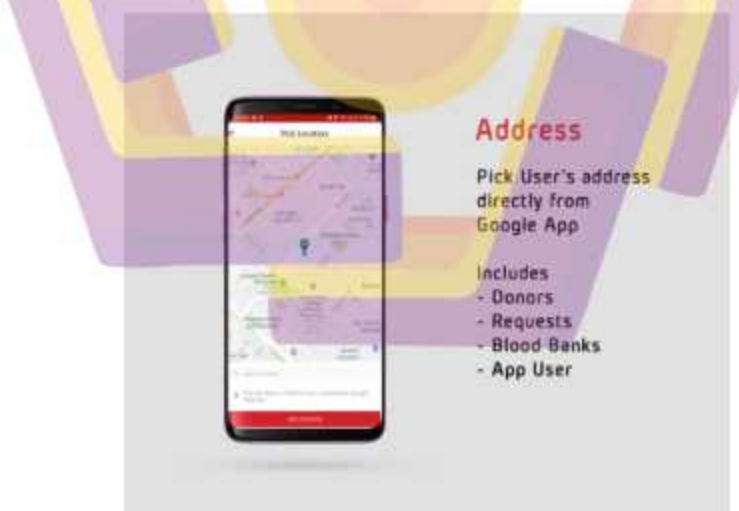


Gambar 1.9 Halaman Utama

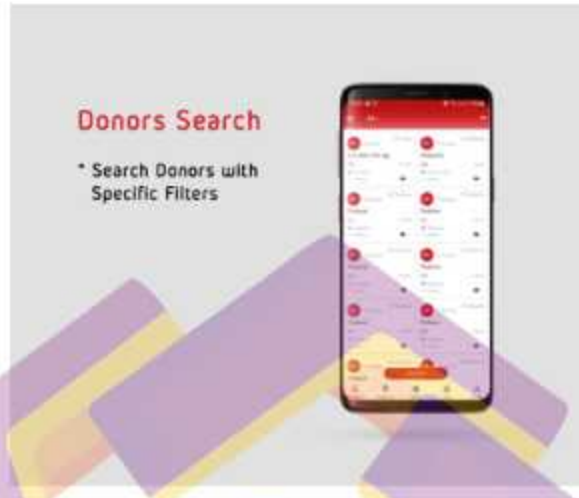
Gambar 1.10 Detil Donor



Gambar 1.11 Menambah Donor



Gambar 1.12 Autocomplete Address

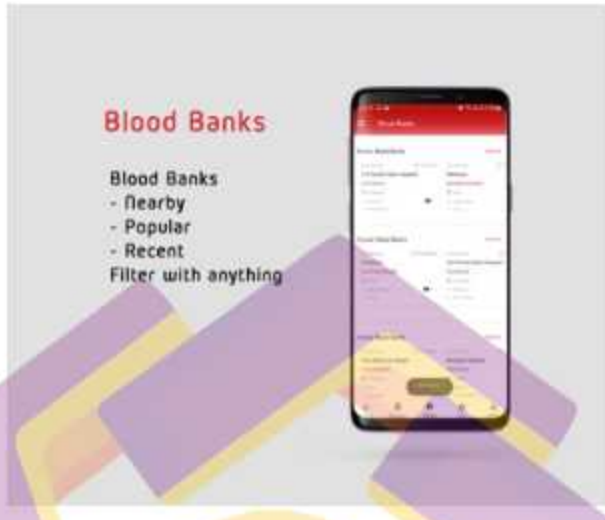


Gambar 1.13 Mencari Donor

Gambar 1.14 Filter Donor

Gambar 1.15 Left Navigation

Gambar 1.16 Reminder Donasi



Gambar 1.17 Lokasi Unit Donor Darah

BAB II

PUBLIKASI

2.1 Penjelasan Publikasi

Hasil penelitian pengembangan produk Plasmanation telah diterima dalam artikel ilmiah sesuai dengan Notifikasi Email dari Open Journal Sistem sebagaimana terlampir pada Lampiran , dengan detail sebagai berikut :

Nama Penulis	: Nur Arifin Akbar, Andi Sunyoto, M. Rudyanto Arief, Wahyu Caesarendra
Institusi	: Universitas Amikom Yogyakarta Fakultas/Prodi
	: Magister Teknik Informatika
Judul Makalah	: Reducing Overhead Of Self-stabilizing Byzantine Agreement Protocols For Blockchain Using Http/3 Protocol : A Perspective View
Nama Jurnal	: Sinergi
Kode Makalah	: #10585
Website	: https://publikasi.mercubuana.ac.id/index.php/sinergi
ISSN	: (p) 1410-2331, (e) 2460-1217
Akreditasi	: Sinta 2

2.2 Abstrak (In English)

Today, there is a tendency to reduce the dependence on local computation in favor of cloud computing. However, this inadvertently increases the reliance upon distributed fault-tolerant systems. In a condition that forced to work together, these systems often need to reach an agreement on some state or task, and possibly even in the presence of some misbehaving Byzantine nodes. Although non-trivial, Byzantine Agreement (BA) protocols now exist that are resilient to these types of faults. However, there is still a risk for inconsistencies in the application state in practice, even if a BA protocol is used. A single transient fault may put a node into an illegal state, creating a need for new self-stabilizing BA protocols to recover from illegal states. As self-stabilization often comes with a cost, primarily in the form of communication overhead, a potential lowering of latency - the cost of each message - could significantly impact how fast the protocol behaves overall. Thereby, there is a need for new network protocols such as QUIC, which, among other things, aims to reduce latency. In this paper, we survey current state-of-the-art agreement protocols. Based on previous work, some researchers try to implement pseudocode like QUIC protocol for Ethereum blockchain to have a secure network, resulting in slightly slower performance than the IP-based blockchain. We focus on consensus in the context of blockchain as it has prompted the development and usage of new open-source BA solutions that are related to proof of stake. We also discuss extensions to some of these protocols, specifically the possibility of achieving self-stabilization and the potential integration of the QUIC protocol, such as PoS and PBFT. Finally, further challenges faced in the field and how they might be overcome are discussed.

2.3 Korelasi Penelitian

Pada tahap pengembangan berikutnya di aplikasi Plasmanation, akan digunakan sistem blockchain sebagai bentuk reward yang terjadi atas transaksi atas donor dan pasien. Sistem Blockchain akan mengeluarkan token sesuai urgensi dari pendonor tersebut, adapun pemodelannya adalah sebagaimana berikut :

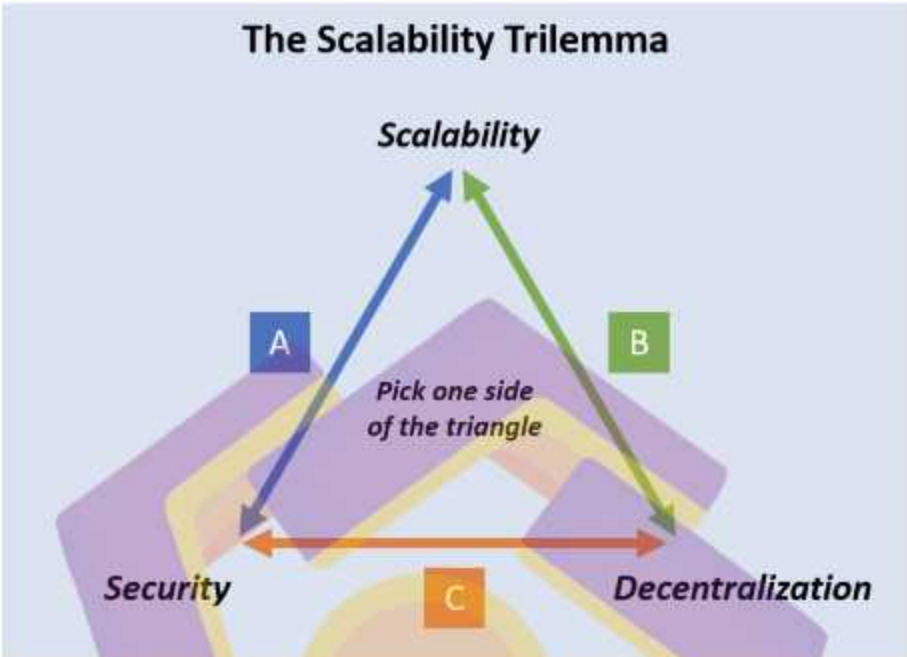
Tabel 2.1 Token Issuance Model

Urgency Level	Tokens Issued
1 - Low	1
2 - Medium	2
3 - High	3

Dalam ranah teknologi blockchain ada yang disebut sebagai "trilema", yakni tiga tantangan dalam hal meningkatkan derajat desentralistik, keamanan dan skalabilitas. Hingga saat ini dua tantangan pertama praktis telah terjawab, namun tidak untuk persoalan skalabilitas, yang utamanya mengacu pada peningkatan kecepatan transaksi per detik. Namun, selayaknya persoalan yang dilematis, skalabilitas yang tinggi tidak boleh mengorbankan karakter desentralistik blockchain.

Menyelesaikan trilema itu adalah syarat utama agar teknologi blockchain dapat diadopsi secara luas di berbagai sektor kehidupan sehingga menjadi mainstream, terpadu dengan sejumlah teknologi lainnya. Skalabilitas misalnya juga terkait dengan masalah interoperability (kesalingterhubungan) antar blockchain yang berbeda.

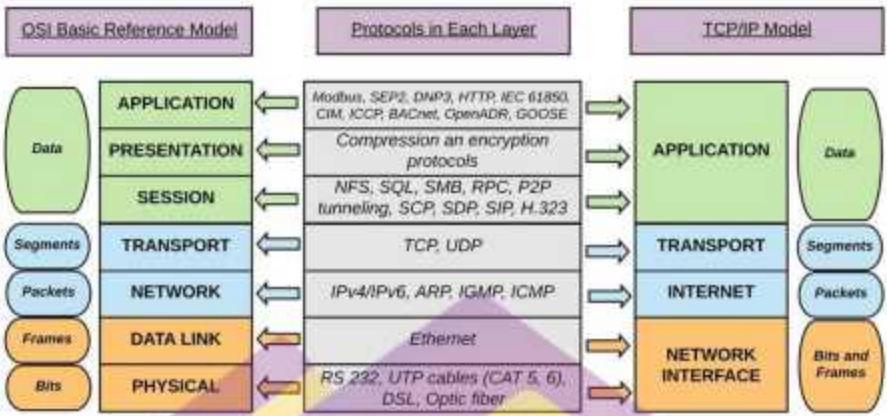
Sebagai blockchain pengembangan dApp yang paling lama dan paling banyak diadopsi, Ethereum mewakili blockchain yang paling desentralistik dan aman. Namun Ethereum juga terkenal tertinggal dalam hal skalabilitas. Karena keterbatasan infrastruktur, saat ini Ethereum hanya mampu menangani 10-20 transaksi per detik, bahkan setelah 5 tahun pengembangan. Para developer memastikan bahwa perlu waktu hingga dua tahun sebelum Ethereum 2.0 yang telah lama ditunggu-tunggu mencapai skalabilitas. Pada generasi kedua ini nanti, Ethereum akan menganut algoritma konsensus Proof-of-Stake (PoS), meninggalkan Proof-of-Work (PoW). Tetapi hal tersebut baru akan terlaksana sekitar tahun 2023 untuk full migration pada networknya.



Gambar 2.1 Blockchain Trillema

Pada penelitian sebelumnya, beberapa peneliti telah melakukan pendekatan untuk menyelesaikan Blockchain Trillema dengan beberapa method, antara lain scaling pada beberapa layer, baik layer-1 maupun layer-2, serta pembuatan consensus baru baik existing blockchain maupun varian blockchain baru agar lebih scalable.

Adapun kebaharuan yang ditulis dalam paper berjudul "Reducing Overhead Of Self-stabilizing Byzantine Agreement Protocols For Blockchain Using Http/3 Protocol : A Perspective View" dengan Judul Thesis "Penyelesaian Trilemma Untuk Skalabilitas & Keamanan Blockchain Menggunakan Algoritma Terkini" adalah pembahasan untuk kemungkinan pendekatan teknologi hybrid UDP dan TCP pada OSI Layer yang sebelumnya diterapkan pada protocol HTTP/3 (Quic) pada teknologi blockchain.



Gambar 2.2 OSI vs TCP Layer

2.4 Dasar Teori

2.4.1 Konsensus pada Blockchain

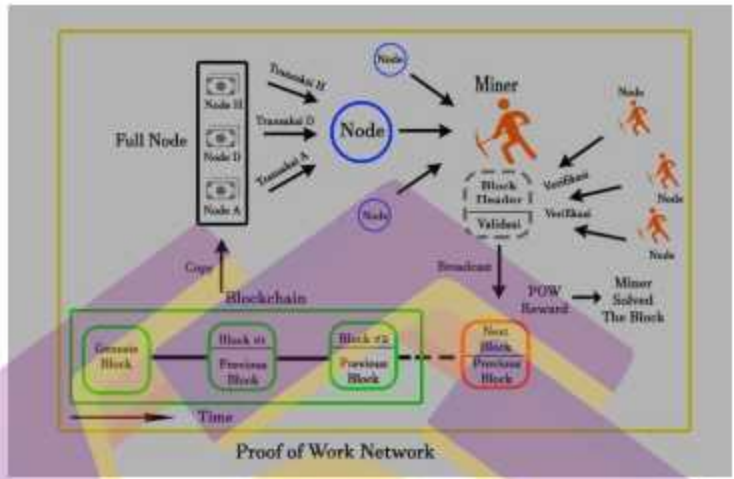
Konsesus merupakan kemampuan untuk mencapai kesepakatan bersama. Konsensus dalam *Blockchain* adalah suatu proses perhitungan rumit untuk menghasilkan kesepakatan bersama tentang validasi suatu transaksi. Dengan kata lain konsensus dimaksudkan untuk menghasilkan sistem yang ketat tanpa aturan penguasa. Tidak ada satu orang, organisasi atau kelompok yang bertanggungjawab atau lebih tepatnya kekuatan dan kontrol tersebar di seluruh

jaringan peserta. Kemampuan untuk mencapai konsensus di seluruh jaringan terdistribusi dibawah kondisi persaingan dan tanpa kontrol yang bersifat sentral merupakan prinsip inti dari *public blockchain*. Berikut merupakan beberapa algoritma konsensus yang digunakan untuk memvalidasi transaksi pada *blockchain*.

1. *Proof of Work / Nakamoto Consensus*

   Proof of Work merupakan sebuah protokol yang mempunyai fungsi untuk mencegah aktifitas serangan *cyber* (DDos), yang dapat melumpuhkan/melemahkan suatu sumber daya sistem komputer. Konsep POW pertama kali dikenalkan oleh Cynthia Dwork & Moni Naor pada tahun 1993 dan baru di implementasikan oleh Markus Jakobsson (mata uang Shell) pada tahun 2009. Dalam teknologi *Blockchain*, POW digunakan oleh Satoshi Nakamoto sebagai algoritma konsensus dan Bitcoin sendiri sebagai Mata Uang dari konsensus *Proof of Work*. Persyaratan utama dalam konsensus POW adalah proses kegiatan mining (proses komputasi dari CPU, GPU, ASIC, FPGA) yang berfungsi sebagai penemu, pencari solusi dan memvalidasi setiap masalah (*hash*) kedalam sebuah *block* dan akan didistribusikan ke dalam sebuah buku besar (*ledger*) yang disebut dengan *Blockchain[11][12][13]*.

   Untuk mencapai sebuah konsensus, sebuah transaksi harus melewati beberapa proses yang juga melibatkan adanya proses komputasi yang dilakukan oleh beberapa miners, sehingga bisa tercipta sebuah *Block* yang valid.[14] Sistem distribusi konsensus *proof of work* dapat dilihat pada pada Gambar 2.3.



Gambar 2.3 *Proof of Work Network*

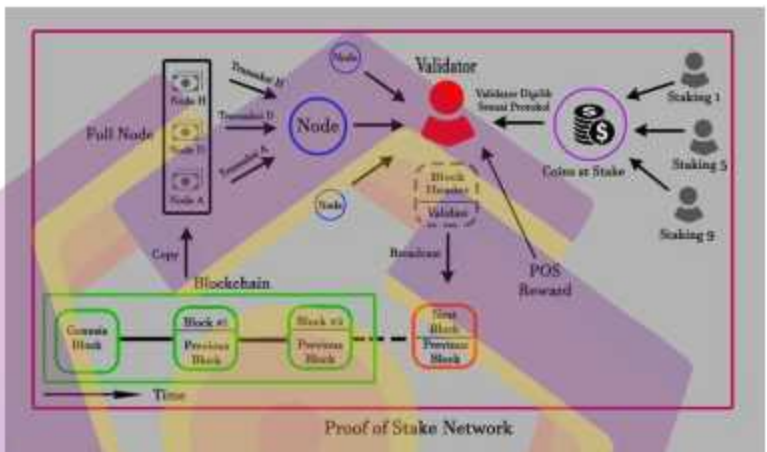
Berikut merupakan penjelasan dari *Proof of Work Network*:

a. Suatu (beberapa) transaksi yang muncul dari sebuah *wallet* yang bertindak sebagai *Full Node* (salinan *Blockchain*) akan di *publish* pada jaringan (P2P).
b. Transaksi-transaksi ini akan tehubung ke sebuah jaringan yg juga terhubung dengan node *Miners*.
c. Miner akan melakukan proses komputasi (*hash function*) untuk menyelesaikan persoalan matematika rumit ini ke dalam sebuah *block*.
d. Jumlah maksimal transaksi dalam setiap *block* tergantung dari protokol yang berlaku.
e. Setelah masalah (*hash*) terpecahkan, maka miner yang pertama kali memecahkan masalah ini akan mem-broadcast *block* baru ke jaringan (P2P).
f. *Node* (*miner*) lainnya yang menerima *block* ini akan melakukan proses verifikasi (validasi).
g. Setelah *block* mendapat validasi, maka *block* ini akan di distribusikan ke dalam *blockchain* sebagai *Block* baru yang valid.
h. *Miners* yang bertindak sebagai pembuat *block* valid akan menerima reward.

2. *Proof Of Stake / Byzantine Agreement*

Algoritma konsensus Proof of *Stake* (PoS) pertama kali dikenalkan oleh Sunny King dan Scott Nadal pada tahun 2012. Penggunaan metode ini diharapkan dapat mengatasi besarnya daya yang dibutuhkan untuk melakukan proses komputasi pada konsensus PoW. Secara garis besar, proses Staking ialah mengunci beberapa jumlah coin (*cryptocurrency*) sebagai jaminan, didalam sebuah *wallet* yang menjalankan *Full Node* dari sebuah *blockchain*. Jaminan ini sebagai bukti kepemilikan seorang pemegang koin (tokens holder) sebagai fungsi node, dalam berkontribusi didalam jaringan konsensus PoS dengan proses yang dinamakan *Forging* (menempa koin)[14][15][16].

Berbeda dengan konsensus PoW yang membutuhkan proses komputasi menggunakan peralatan-peralatan dengan sumber daya *listr*ik. Pada metode PoS, untuk mencapai sebuah konsensus hanya dibutuhkan sebuah *Full Node* (*Wallet*) dengan token/koin didalamnya. Dan setiap token/koin holder yang senantiasa terhubung dengan jaringan (*node*) *blockchain*, mempunyai peluang untuk menjadi seorang *staker/forger* dengan memenuhi syarat sesuai dengan protokol yang berlaku. Oleh karena itu didalam konsensus PoS ini, tidak dibutuhkan banyak sumber daya energi (*listr*ik) dalam proses pencapaian suatu konsensus. Sistem distribusi konsensus *proof of work* dapat dilihat pada pada Gambar 2.4.



Gambar 2.4 *Proof of Stake Network*

Berikut merupakan penjelasan dari *Proof of Stake Network*:

a. Untuk bisa melakukan *forging* (*minting*), maka pemegang token/koin harus mengunci sejumlah koin didalam *wallet*nya (*Full Node*) yg terhubung dengan jaringan *blockchain*.

b. Pada saat sebuah/beberapa transaksi masuk ke dalam jaringan (P2P). Pembuatan sebuah *block* (validasi transaksi) dipilih secara *Pseudorandom* berdasarkan jumlah koin yang di *stake* dan berapa lama koin tersebut sudah di *stake*.

c. *Token/Coin Holder* dengan jumlah *Staking Coin* yang besar dan waktu (umur) *staking* yang lama, mempunyai peluang (kesempatan) lebih tinggi untuk melakukan proses *forging* pada

block berikutnya.

d. Setelah proses pembuatan *block* dan proses validasi selesai, maka *block* ini akan didistribusikan ke dalam jaringan *blockchain* sebagai *block* baru yang valid.

e. *Forger* (*staker*) akan menerima *reward* dari hasil kerjanya dan untuk umur *staking coinnya* akan direset ulang.

3. *Practical Byzantine Fault Tollerance*

Practical Byzantine Fault Tolerance (PBFT) adalah protokol BFT pertama yang diterapkan pada aplikasi blockchain. Protokol ini menerapkan teknik kriptografi public-key untuk mencegah pemalsuan pesan (spoofing). Protokol ini menggunakan konsep state machine replication (SMR), yaitu konsep bahwa satu service yang sama diproses oleh beberapa server (replika) untuk mengantisipasi adanya fault pada salah satu server, dengan struktur server (view) yang terdiri dari satu server primary dan beberapa server backup. Setiap server memiliki initial state:

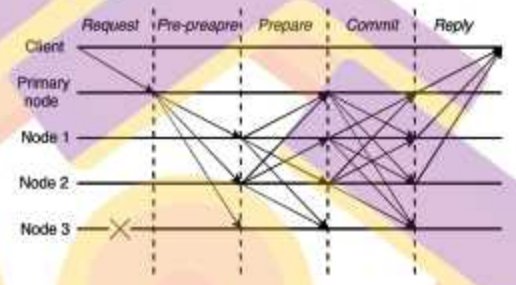
a. service yang sama. Artinya perilaku dalam memproses data transaksi pada setiap server adalah sama;

b. log pesan yang sama. Log pesan terdiri dari: (1) request operation, yaitu operasi yang diminta oleh client; (2) sequence number, yaitu nomor urut yang diberikan pada setiap request operation untuk menjamin eksekusi request operation dilakukan sesuai dengan nomor urut dan tidak ada request operation yang hilang; dan (3) status, yang terdiri dari pre-prepared, prepared, commit;

c. ID view yang sama.

PBFT memiliki model konsensus yang terbagi menjadi lima tahap pada no-fault operation dan fault operation, yaitu Request, Pre-prepare, Prepare, Commit, dan Reply. Sementara pada view-change operation, yaitu operasi untuk mengganti server primary, tahapan pada protokol ini berbeda. Protokol PBFT dapat mentoleransi sejumlah server malicious (m) $\leq$ f pada

kondisi jumlah server (n) = 3f + 1. Contohnya, pada kondisi jumlah server sebanyak empat (f = 1) ketika terdapat 1 server malicious (m = f), protokol ini tetap dapat mentoleransi fault yang terjadi dengan menjamin interactive consistency 1, yaitu semua server non-malicious memproses data transaksi yang sama (agreement), dan interactive consistency 2, yaitu data transaksi yang diproses adalah valid (validity). Ilustrasi tahapan fault dan no-fault pada protokol PBFT dapat dilihat pada Gambar 2.4.



Gambar 2.4 *PBFT Network*

4. Perbandingan Consensus

Secara umum, perbandingan fault-tollerance diantara 3 konsensus tersebut adalah sebagai berikut:

Tabel 2.2 Perbandingan Consensus Blockchain

Name	PoW	BA (PoS)	PBFT
Usage	Ethereum, Bitcoin	Algorand	ByzCoin
Fault Tolerance	50%	50%	33%
Power Consumption	Large	Less	Negligible
Type	Probabilistic-finality	Probabilistic-finality	Absolute-finality

2.4.2 HTTP3 (Quic Protocol)

HTTP3 merupakan versi ketiga dari HTTP, yang sebelumnya dikenal sebagai HTTP-over-QUIC. Awalnya, QUIC (Quick UDP Internet Connections) dikembangkan oleh Google dan merupakan penerus HTTP2. QUIC pernah digunakan oleh Google dan Facebook untuk meningkatkan kecepatan website.Versi baru dari protokol HTTP ini memiliki lebih banyak keunggulan ketimbang protokol UDP tingkat rendah, dan logam terbuka HTTP3 pun memiliki banyak fitur baru yang belum ada di versi HTTP sebelumnya pada lapisan TCP. Saat diluncurkan, versi ini langsung disukai karena mampu membuat website yang dikelola bergerak dengan lebih cepat dan dengan jeda waktu yang singkat.

Yang membedakan antara versi kedua dan versi ketiga dari HTTP adalah protokol yang digunakan. HTTP2 menggunakan protokol TCP sedangkan HTTP3 menggunakan protokol UDP. Pada dasarnya kedua protokol tersebut memiliki konsep yang sama, namun berbeda dalam hal efisiensinya[3][4][5][6].

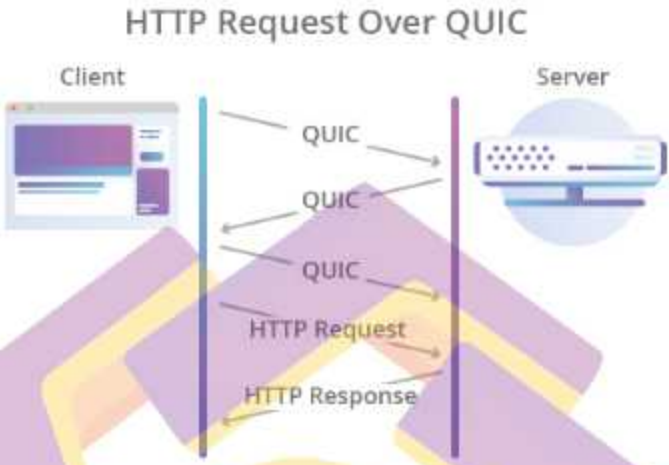
Meskipun IP adalah lapisan yang menjadi dasar dari semua komunikasi online, TCP (Transmission Control Protocol) adalah bagian tingkat yang lebih tinggi dari rangkaian protokol internet. TCP memberikan kehandalan yang diperlukan oleh website, email, transfer file (FTP), untuk lapisan aplikasi atau protokol internet. Termasuk pembuatan koneksi multi-langkah, dengan jabat tangan, pesanan packet yang terjamin, dan transmisi ulang packet yang hilang. Di sisi lain, UDP (User Datagram Protocol), sama seperti namanya, merupakan protokol tanpa koneksi berbasis diagram. Artinya, tidak ada jabat tangan dan tidak ada jaminan pemesanan atau pengiriman. Konsekuensinya, semua langkah yang mungkin dilakukan untuk memastikan pengiriman, integritas dara, dan hal-hal lainnya, diserahkan kepada aplikasi[7][8]. Aplikasi yang dibangun di atas UDP, dapat memilih strategi yang akan digunakannya tergantung pada kasus konkretnya. Atau, sebagai alternatif, mereka dapat memanfaatkan elemen lapisan tautan, seperti checksum, untuk menghindari overhead.

Karena UDP yang juga tersebar luas seperti halnya TCP, maka memungkinkan untuk mencapai peningkatan tanpa perubahan firmware pada semua perangkat yang terhubung ke internet, atau perubahan signifikan pada sistem

operasi. HTTP3 memberikan pembaharuan yang sangat signifikan jika dibandingkan dengan versi sebelumnya.

Pertama, HTTP3 berguna untuk membuat website lebih cepat diakses. Dengan menggunakan protokol UDP, proses transfer file atau data tidak mengalami kendala sehingga website bisa lebih cepat untuk diakses. Kedua, HTTP3 dapat mengunduh file tanpa mengalami proses penundaan. Jadi, saat Anda mengunduh sesuatu dari internet melalui smartphone, Anda tidak perlu mengulang proses download ketika koneksi WiFi yang digunakan terputus. Karena koneksi akan dialihkan secara otomatis ke koneksi mobile data yang Anda gunakan di smartphone. Hal ini, kendati bermanfaat, tidak bisa ditemui di versi HTTP2[9][10].

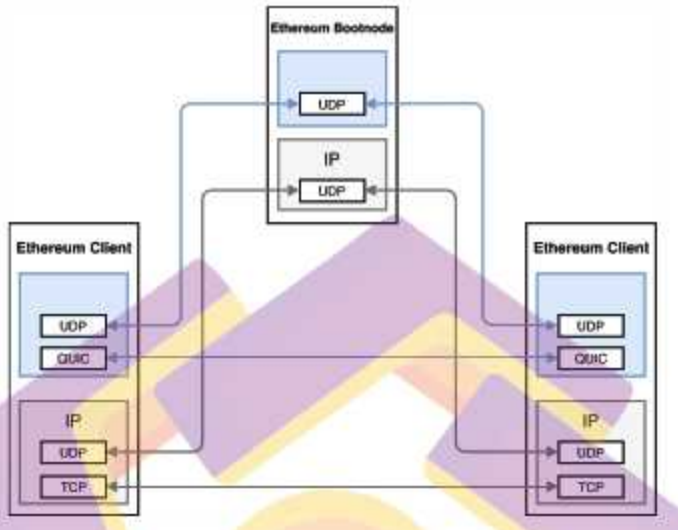
Kegunaan ketiga dari HTTP3, adalah memungkinkan transfer data terjadi hanya dengan sekali proses saja, dan membuat keamanan data dapat berlangsung lebih cepat. Hal ini berbeda dengan HTTP2 yang melakukan proses transfer melalui dua proses, yaitu proses meminta dan menerima packet yang terjadi secara berulang-ulang. Di sepanjang perjalanannya sebagai protokol transfer data, HTTP ini banyak mengalami pembaharuan ke hal yang lebih baik mulai dari HTTP2 hingga HTTP3. Di versi terbarunya ini, HTTP3 banyak sekali mengalami perubahan dengan penambahan fitur-fitur terbaru. Banyak sekali kegunaan dari HTTP3 setelah mengalami pembaharuan, mulai dari membuat situs website dapat cepat diakses, akses streaming menjadi lebih cepat, hingga dapat mengunduh file tanpa mengalami proses penundaan.



Gambar 2.6 *HTTP Over Quic Protocol*

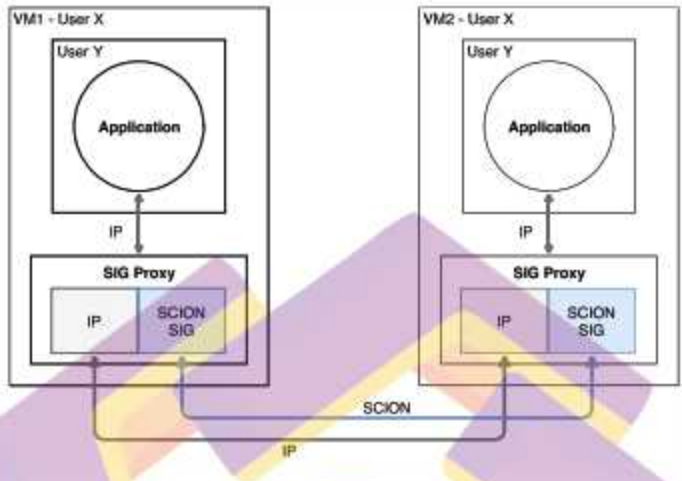
2.5 Desain Program & Hasil

Pada bagian ini, penulis mengacu kepada hasil penelitian sebelumnya, dimana salah seorang peneliti dari Swedia bernama Aleksandar Vorkapic menerapkan protocol HTTP over UDP dan TCP untuk mengamankan blockchain yang berjalan diatas consensus Proof of Work (Ethereum) dengan project bernama SCION yang berisi pseudocode dan diterapkan pada cloud computing. Adapun rancangannya adalah sebagaimana berikut :

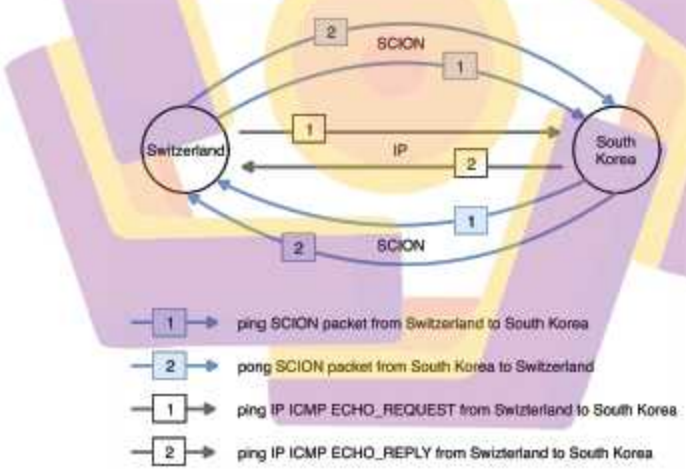


Gambar 2.7 *Ethereum Over Hybrid Protocol*

Adapun konfigurasi pada level VM menggunakan proxy agar dapat terhubung di internal network di cloud computing dengan protocol berbeda (direct vs hybrid protocol) seperti yang ditunjukan pada Gambar 2.8. Untuk metode pengetesan berupa round time trip dengan flow yang digambarkan pada Gambar 2.9, serta hasil ditunjukan pada table 2.3 serta 2.4



Gambar 2.8 *IP vs Programmed Proxy Connection*



Gambar 2.9 *Path Testing for IP vs Scion Connection*

Tabel 2.3 Hasil Pengetesan Direct IP

IP	Germany	USA	South Korea
Avg RTT (ms)	28.781	126.005	287.131
Std dev RTT (ms)	1.395	8.947	15.597
Avg hops	15.2	18	18.6
Std dev hops	1.4	0.0	0,9
Packet loss (%)	1.4	0.0	0.0

Tabel 2.4 Hasil Pengetesan Scion (Hybrid protocol)

SCION	Germany	USA	South Korea
Avg RTT (ms)	62.568	150.734	301.898
Std dev RTT (ms)	3.246	6.213	6.247
Avg hops	7.7	7.7	8.8
Std dev hops	0.5	0.9	0.7
Packet loss (%)	0.0	0.0	0.0

2.6 Kesimpulan

Berdasarkan penelitian diatas, dan literature review secara komprehensif, didapatkan bahwasanya hasil pseudocode pada bagian 2.5 didapatkan latency yang lebih tinggi pada Ethereum Node, walau secara teori seharusnya HTTP/3 dapat bekerja lebih cepat, namun pada Consensus Nakamoto / Proof of Work terlihat lebih lambat, bisa jadi dikarenakan adanya tambahan proses yang menambah delay pada miner atau node yang dijalankan. Hal ini tidak menutup kemungkinan untuk membuat hasil yang lebih cepat pada consensus lain seperti Byzantine Agreement/Proof of Stack dikarenakan secara modelnya tidak memerlukan proses mining, namun pseudocode tersebut harus disesuaikan dengan protocol yang bersangkutan dikarenakan mekanisme yang berbeda dari sistem Proof of Stack.

2.7 Daftar Pustaka

1] Blockchain Charts. (n.d.). Retrieved April 14, 2021, from https://www.blockchain.com/en/charts/mempool-count?timespan=24h

[2] Bentov, I., Gabizon, A., & Mizrahi, A. (2014). Cryptocurrencies without Proof of Work. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 9604 LNCS, 142–157. Retrieved from http://arxiv.org/abs/1406.5694

[3] Carlucci, G., De Cicco, L., & Mascolo, S. (2015). HTTP over UDP: An experimental investigation of QUIC. In Proceedings of the ACM Symposium on Applied Computing (Vol. 13-17-April-2015, pp. 609–614). New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/2695664.2695706

[4] Castro, M., & Liskov, B. (n.d.). Practical Byzantine Fault Tolerance.

[5] Cook, S., Mathieu, B., Truong, P., & Hamchaoui, I. (2017). QUIC: Better for what and for whom? In IEEE International Conference on [6] Communications. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICC.2017.7997281

[7] Daliot, A., & Dolev, D. (2005). Self-stabilization of Byzantine protocols. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) (Vol. 3764 LNCS, pp. 48–67). Springer, Berlin, Heidelberg. https://doi.org/10.1007/11577327_4

[8] Daliot, A., & Dolev, D. (2009). Self-stabilizing Byzantine Agreement. Retrieved from http://arxiv.org/abs/0908.0160

[9] De Coninck, Q., & Bonaventure, O. (n.d.). Multipath QUIC: Design and Evaluation.

[10] de Vries, A. (2018, May 16). Bitcoin's Growing Energy Problem. Joule. Cell Press. https://doi.org/10.1016/j.joule.2018.04.016

[11] Decker, C., Seidel, J., & Wattenhofer, R. (2014). Bitcoin Meets Strong Consistency. ACM International Conference Proceeding Series, 04-07-January-2016. Retrieved from http://arxiv.org/abs/1412.7935

[12] Dolev, D. (1982). The Byzantine generals strike again. Journal of Algorithms, 3(1), 14–30. https://doi.org/10.1016/0196-6774(82)90004-9

[13] Self-Stabilization: Dolev, Shlomi: 9780262529211: Amazon.com: Books. (n.d.). Retrieved April 14, 2021, from https://www.amazon.com/Self-Stabilization-Shlomi-Dolev/dp/0262529211

[14] Dolev, S., Georgiou, C., Marcoullis, I., & Schiller, E. M. (2018). Self-stabilizing Byzantine Tolerant Replicated State Machine Based on Failure Detectors. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) (Vol. 10879 LNCS, pp. 84–100). Springer Verlag. https://doi.org/10.1007/978-3-319-94147-9_7

[15] Gencer, A. E., Basu, S., Eyal, I., Van Renesse, R., & Sirer, E. G. (n.d.). Decentralization in Bitcoin and Ethereum Networks.

[16] Gilad, Y., Hemo, R., Micali, S., Vlachos, G., & Zeldovich, N. (n.d.). Algorand: Scaling Byzantine Agreements for Cryptocurrencies.

[17] Kokoris Kogias, E., Jovanovic, P., Gailly, N., Khoffi, I., Gasser, L., Ford, B., … Ford EPFL, B. (2016). Enhancing Bitcoin Security and Performance with Strong Consistency via Collective Signing. Retrieved from https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/kogias

[18] Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine Generals Problem. ACM Transactions on Programming Languages and Systems (TOPLAS), 4(3), 382–401. https://doi.org/10.1145/357172.357176

[19] Langley, A., Riddoch, A., Wilk, A., Vicente, A., Krasic, C., Zhang, D., … Shi, Z. (2017). The QUIC Transport Protocol: Design and Internet-Scale Deployment, 14. https://doi.org/10.1145/3098822.3098842

[20] Nakamoto, S. (n.d.). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from www.bitcoin.org

[21] Natoli, C., Yu, J., Gramoli, V., & Esteves-Verissimo, P. (2019). Deconstructing Blockchains: A Comprehensive Survey on Consensus, Membership and Structure. ArXiv. Retrieved from http://arxiv.org/abs/1908.08316

[22] Dolev, S., Georgiou, C., Marcoullis, I., & Schiller, E. M. (2018). Self-stabilizing Byzantine Tolerant Replicated State Machine Based on Failure Detectors. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) (Vol. 10879 LNCS, pp. 84–100). Springer Verlag. https://doi.org/10.1007/978-3-319-94147-9_7

[23] Pease, M., & Lamport, L. (1980). Reaching Agreement in the Presence of Faults.

[24] Viernickel, T., Froemmgen, A., Rizk, A., Koldehofe, B., & Steinmetz, R. (2018). Multipath QUIC: A Deployable Multipath Transport Protocol. In IEEE International Conference on Communications (Vol. 2018-May). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICC.2018.8422951

[25] Wood, D. (2014). ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER. Undefined.

[26] Vorkapic, A. (2018). Secure Blockchain Network Communication using SCION. DEGREE PROJECT COMPUTER SCIENCE AND ENGINEERING.

[27] Zhang, S., & Lee, J. H. (2020). Analysis of the main consensus protocols of blockchain. ICT Express, 6(2), 93–97. https://doi.org/10.1016/j.icte.2019.08.001

[28] Gilbert, S., & Lynch, N. (2002). Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web services. ACM SIGACT News, 33(2), 51–59. https://doi.org/10.1145/564585.564601

[29] You, C. S., Yeom, J. S., & Jung, B. C. (2020). Cooperative maximum-ratio transmission with multi-antenna relay nodes for tactical mobile ad-hoc networks. ICT Express, 6(2), 87–92. https://doi.org/10.1016/j.icte.2020.04.002

[30] Wang, L., Shen, X., Li, J., Shao, J., & Yang, Y. (2019). Cryptographic primitives in blockchains. Journal of Network and Computer Applications, 127, 43–58. https://doi.org/10.1016/j.jnca.2018.11.003

[31] Kiayias, A., Russell, A., David, B., & Oliynykov, R. (2017). Ouroboros: A provably secure proof-of-stake blockchain protocol. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) (Vol. 10401 LNCS, pp. 357–388). Springer Verlag. https://doi.org/10.1007/978-3-319-63688-7_12

[32] Helliar, C. V., Crawford, L., Rocca, L., Teodori, C., & Veneziani, M. (2020). Permissionless and permissioned blockchain diffusion. International Journal of Information Management, 54. https://doi.org/10.1016/j.ijinfomgt.2020.102136

[33] Lee, S., Youn, J., & Jung, B. C. (2020). A cooperative phase-steering technique in spectrum sharing-based military mobile ad hoc networks. ICT Express, 6(2), 83–86. https://doi.org/10.1016/j.icte.2020.04.001

[34] Das, M., Luo, H., & Cheng, J. C. P. (2020). Securing interim payments in construction projects through a blockchain-based framework. Automation in Construction, 118. https://doi.org/10.1016/j.autcon.2020.103284

[35] Wasim Ahmad, R., Hasan, H., Yaqoob, I., Salah, K., Jayaraman, R., & Omar, M. (2021). Blockchain for aerospace and defense: Opportunities and open research challenges. Computers and Industrial Engineering, 151. https://doi.org/10.1016/j.cie.2020.106982

[36] Berdik, D., Otoum, S., Schmidt, N., Porter, D., & Jararweh, Y. (2021). A Survey on Blockchain for Information Systems Management and Security. Information Processing and Management, 58(1). https://doi.org/10.1016/j.ipm.2020.102397

LAMPIRAN

Lampiran 1 : Plasmanation Reward

Lampiran 2 : Jurnal Acceptance

Lampiran 3 : Link Source Code Program.

https://gitlab.com/hackshields/http3-blockchain