
ANALISIS VERIFIKASI *PROOF OF STAKE* (POS) NFT DENGAN TEKNOLOGI *SMART CONTRACT*

Eleazer Gottlieb Julio Sumampouw¹, Irwan Sembiring²

^{1,2}Program Studi Teknik Informatika, Fakultas Teknologi Informasi,
Universitas Kristen Satya Wacana
e-mail: ¹672018137@student.uksw.edu, ²irwan@uksw.edu

ABSTRAK

Penelitian mengenai Analisis Verifikasi Proof of Stake (PoS) NFT dengan Teknologi Smart Contract, yang dilakukan melalui metode eksperimental, menghasilkan pencapaian yang sesuai dengan tujuan penelitian. Peneliti berhasil mengembangkan dan menjalankan sistem sesuai dengan tujuan yang diinginkan. Beberapa pencapaian utama mencakup implementasi berhasil dari proses verifikasi PoS, serta proses Stake, Unstake, dan Claim yang menggunakan integrasi Web3 dan dompet Metamask. Rekam transaksi dengan akurat mencatat waktu pengirim dan penerima bersama dengan prosedur verifikasi pemilik. Lebih lanjut, penelitian ini menyajikan analisis perbandingan antara Proof of Work (PoW) dan Proof of Stake (PoS). Temuan penelitian menunjukkan keunggulan Proof of Stake (PoS) dalam efisiensi waktu transaksi, biaya transaksi yang lebih rendah, peningkatan keamanan melalui pemilihan validator yang cermat, dan ketahanan terhadap berbagai jenis serangan. Secara keseluruhan, penelitian ini mengukuhkan keefektifan dan keunggulan implementasi Proof of Stake (PoS) dalam konteks Non-Fungible Tokens (NFTs) menggunakan Smart Contract.

Kata kunci: Proof of Stake (PoS), Non-Fungible Tokens (NFTs), Smart Contract.

ABSTRACT

The research on the Analysis Verification of Proof of Stake (PoS) NFT Smart Contract Technology, conducted through experimental methods, has yielded successful outcomes aligning with the research objectives. The researcher has successfully developed and executed the system, achieving the intended goals. Key accomplishments include the successful implementation of the PoS verification process, as well as the Stake, Unstake, and Claim processes, utilizing Web3 and Metamask wallet integration. Transaction records accurately capture the timing of sender and receiver actions, alongside owner verification procedures. Furthermore, the research presents a comparative analysis between Proof of Work (PoW) and Proof of Stake (PoS). The findings underscore the superiority of Proof of Stake (PoS) in terms of transaction time efficiency, lower transaction costs, enhanced security through meticulous validator selection, and resilience against various types of attacks. Overall, the research substantiates the efficacy and advantages of implementing Proof of Stake (PoS) in the context of Non-Fungible Tokens (NFTs) using Smart Contracts.

Keywords: Proof of Stake (PoS), Non-Fungible Tokens (NFTs), Smart Contract.

PENDAHULUAN

Dalam era perkembangan teknologi blockchain, konsep *Proof of Stake* (PoS) muncul sebagai mekanisme konsensus yang menarik perhatian berbagai sektor. Blockchain, sebagai teknologi dasar yang mendasari mata uang kripto, telah merevolusi cara kita memandang dan mengelola aset digital menurut Michael dkk (2015). Di tengah perubahan ini, *Non-Fungible Tokens* (NFTs) menjadi fenomena yang signifikan, menyajikan solusi inovatif untuk merepresentasikan kepemilikan aset digital yang unik. NFTs telah diterapkan dalam seni, *gaming*, *real estate*, dan sektor lainnya, memanfaatkan keunggulan tak tertandingi dalam memvalidasi dan melacak kepemilikan aset digital (Sari, 2022).

Namun, di balik kemajuan ini, terdapat tantangan yang perlu diatasi, terutama terkait dengan mekanisme PoS dan implementasi NFTs menggunakan *Smart Contracts* di dalam *blockchain* menurut Firdaus (2020). PoS, meskipun efisien dalam penghematan energi, memiliki keterbatasan dan risiko tertentu yang memerlukan pemahaman mendalam. Selain itu, penggunaan NFTs dengan *Smart Contracts* memunculkan pertanyaan tentang keamanan dan integritas transaksi dalam ekosistem *blockchain* (Yeni & Kumala, 2020).

Analisis verifikasi menjadi aspek kritis dalam menghadapi tantangan ini, terutama dalam konteks PoS NFTs dengan *Smart Contracts* menurut Schmitz (2022). Verifikasi yang tidak memadai dapat membuka peluang risiko keamanan, dan oleh karena itu, diperlukan upaya maksimal untuk meningkatkan sistem verifikasi menurut Fauzi dkk (2023). Inilah latar belakang permasalahan yang mendasari penelitian ini, di mana tujuan utamanya adalah untuk melakukan analisis mendalam terhadap verifikasi *Proof of Stake* NFTs dengan menggunakan *Smart Contracts*.

Berdasarkan penelitian terdahulu yang didapatkan oleh penulis untuk memperkuat penelitian ini antara lain; Penelitian Rizki Pratama (2023) yang menemukan bahwa dalam menganalisis *Proof of Work* (PoW) dan *Proof of Stake* (PoS) untuk implementasi *blockchain* dalam permainan, ditemukan bahwa PoW menawarkan keamanan tinggi, desentralisasi, namun dengan konsumsi energi tinggi dan skalabilitas terbatas. Di sisi lain, PoS menonjolkan efisiensi energi, skalabilitas yang lebih tinggi, dan keamanan yang dianggap lebih tinggi, tetapi memiliki risiko potensial sentralisasi dan distribusi kekayaan yang kurang optimal. Komparasi antara keduanya menunjukkan bahwa PoW lebih efisien secara energi, sedangkan PoS lebih unggul dalam skalabilitas. Keamanan tetap menjadi keunggulan PoW, meskipun dengan keterbatasan efisiensi energi dan skalabilitas. Dalam konteks permainan, PoW dianggap lebih cocok untuk fase pengumpulan koin atau seleksi, menilai kemampuan komputasi pemain untuk membantu pengelompokan seimbang. Penggunaan PoW untuk pengelompokan dianggap dapat meminimalkan kelemahan PoS dalam distribusi dan pemilihan berdasarkan *stake*, yang mendukung distribusi meja yang lebih efektif. Integrasi PoS kemudian dapat menjaga keseimbangan permainan melalui pengelompokan berdasarkan koin dari fase seleksi. Meskipun PoW memperkuat keamanan jaringan permainan, risiko serangan dianggap sangat kecil karena memerlukan biaya dan kapabilitas komputasi tinggi. Kesimpulannya,

kombinasi PoW dan PoS menciptakan permainan yang lebih fair, kompetitif, dan aman dengan memanfaatkan keunggulan masing-masing algoritma konsensus.

Penelitian selanjutnya yang dilakukan Saad dkk (2021) menemukan bahwa Teknologi *blockchain* adalah sebuah buku besar publik yang dapat diakses oleh semua orang tanpa adanya otoritas pusat yang mengendalikan. Teknologi ini umumnya digunakan untuk registrasi dan *smart contract*. Untuk memastikan keamanan dan keaslian informasi transaksi di *blockchain*, banyak penelitian dilakukan terkait algoritma konsensus. Banyak algoritma konsensus digunakan dalam *blockchain*. Menentukan area penelitian utama dan menemukan kunci terbaik dari algoritma konsensus merupakan motivasi dari penelitian ini. Oleh karena itu, penelitian ini akan mengeksplorasi bagaimana area penelitian algoritma konsensus dapat ditentukan dengan mempelajari *Proof of Stake* (PoS) dan *Delegated Proof of Stake* (DPoS). Selain itu, penelitian ini akan meneliti parameter utama yang digunakan dalam kedua algoritma tersebut. Setelah mendapatkan parameter, kita akan membandingkan kinerja keduanya dalam hal transaksi per detik, jumlah *node*, dan ukuran blok. Lebih lanjut, kami akan menyimpulkan efisiensi kedua algoritma ini dari segi skalabilitas. Meskipun diharapkan kinerja DPoS lebih baik daripada PoS, dampak parameter dapat dinilai dan dianalisis untuk melihat dan membuktikan hasilnya.

Penelitian lainnya dari Kin Chan dkk (2020) Hasil penelitian menunjukkan bahwa teknologi *blockchain*, yang mendasarkan diri pada buku besar publik, memberikan akses kepada semua pihak tanpa otoritas pusat yang mengendalikan. Teknologi ini umumnya dimanfaatkan untuk keperluan registrasi dan *smart contract*. Dalam upaya memastikan keamanan dan keaslian informasi transaksi di dalam *blockchain*, banyak penelitian dilakukan terkait algoritma konsensus yang digunakan. Dalam ranah *blockchain*, terdapat banyak algoritma konsensus yang berbeda. Penelitian ini memiliki motivasi untuk menentukan area penelitian utama dan menemukan kunci terbaik dari algoritma konsensus. Fokus utama penelitian adalah pada *Proof of Stake* (PoS) dan *Delegated Proof of Stake* (DPoS). Selanjutnya, penelitian menelaah parameter utama yang digunakan dalam kedua algoritma tersebut. Setelah memperoleh parameter tersebut, dilakukan perbandingan kinerja keduanya, termasuk transaksi per detik, jumlah *node*, dan ukuran blok. Analisis lebih lanjut dilakukan untuk menyimpulkan efisiensi keduanya dari segi skalabilitas. Meskipun diharapkan bahwa kinerja DPoS lebih baik daripada PoS, hasil penelitian menunjukkan bahwa dampak dari parameter-parameter yang digunakan dapat dinilai dan dianalisis secara mendalam untuk membuktikan hasil tersebut. Dengan demikian, penelitian ini diharapkan dapat memberikan solusi terhadap masalah kinerja dan keamanan yang dipengaruhi oleh penerapan algoritma konsensus dalam teknologi *blockchain*.

Berdasarkan latar belakang masalah diatas dan penelitian terdahulu yang telah dirangkum untuk mencapai tujuan ini, penelitian ini memilih metode eksperimental sebagai pendekatan yang memungkinkan pemahaman yang lebih dalam terkait dengan efektivitas verifikasi. Metode eksperimental dianggap relevan karena memberikan keleluasaan untuk menguji dan mengamati performa sistem dalam berbagai skenario. Dengan demikian, penelitian ini bukan hanya mengeksplorasi permasalahan yang ada, tetapi juga berusaha memberikan solusi konkrit melalui pendekatan eksperimental yang

dapat memberikan wawasan yang berharga bagi perkembangan teknologi *blockchain* di masa depan.

KAJIAN TEORI

Penelitian Terdahulu

Penelitian dari Rizki Pratama (2023) yang menemukan bahwa dalam menganalisis *Proof of Work* (PoW) dan *Proof of Stake* (PoS) untuk implementasi *blockchain* dalam permainan, ditemukan bahwa PoW menawarkan keamanan tinggi, desentralisasi, namun dengan konsumsi energi tinggi dan skalabilitas terbatas. Di sisi lain, PoS menonjolkan efisiensi energi, skalabilitas yang lebih tinggi, dan keamanan yang dianggap lebih tinggi, tetapi memiliki risiko potensial sentralisasi dan distribusi kekayaan yang kurang optimal. Komparasi antara keduanya menunjukkan bahwa PoW lebih efisien secara energi, sedangkan PoS lebih unggul dalam skalabilitas. Keamanan tetap menjadi keunggulan PoW, meskipun dengan keterbatasan efisiensi energi dan skalabilitas. Dalam konteks permainan, PoW dianggap lebih cocok untuk fase pengumpulan koin atau seleksi, menilai kemampuan komputasi pemain untuk membantu pengelompokan seimbang. Penggunaan PoW untuk pengelompokan dianggap dapat meminimalkan kelemahan PoS dalam distribusi dan pemilihan berdasarkan stake, yang mendukung distribusi meja yang lebih efektif. Integrasi PoS kemudian dapat menjaga keseimbangan permainan melalui pengelompokan berdasarkan koin dari fase seleksi. Meskipun PoW memperkuat keamanan jaringan permainan, risiko serangan dianggap sangat kecil karena memerlukan biaya dan kapabilitas komputasi tinggi. Kesimpulannya, kombinasi PoW dan PoS menciptakan permainan yang lebih fair, kompetitif, dan aman dengan memanfaatkan keunggulan masing-masing algoritma konsensus.

Penelitian selanjutnya Saad dkk (2021) menemukan bahwa Teknologi *blockchain* adalah sebuah buku besar publik yang dapat diakses oleh semua orang tanpa adanya otoritas pusat yang mengendalikan. Teknologi ini umumnya digunakan untuk registrasi dan *smart contract*. Untuk memastikan keamanan dan keaslian informasi transaksi di *blockchain*, banyak penelitian dilakukan terkait algoritma konsensus. Banyak algoritma konsensus digunakan dalam *blockchain*. Menentukan area penelitian utama dan menemukan kunci terbaik dari algoritma konsensus merupakan motivasi dari penelitian ini. Oleh karena itu, penelitian ini akan mengeksplorasi bagaimana area penelitian algoritma konsensus dapat ditentukan dengan mempelajari *Proof of Stake* (PoS) dan *Delegated Proof of Stake* (DPoS). Selain itu, penelitian ini akan meneliti parameter utama yang digunakan dalam kedua algoritma tersebut. Setelah mendapatkan parameter, kita akan membandingkan kinerja keduanya dalam hal transaksi per detik, jumlah *node*, dan ukuran blok. Lebih lanjut, kami akan menyimpulkan efisiensi kedua algoritma ini dari segi skalabilitas. Meskipun diharapkan kinerja DPoS lebih baik daripada PoS, dampak parameter dapat dinilai dan dianalisis untuk melihat dan membuktikan hasilnya. Kami berharap setelah penelitian ini, dapat diatasi masalah kinerja dan keamanan yang dipengaruhi oleh penerapan algoritma konsensus yang digunakan dalam *blockchain*.

Penelitian lainnya dari Kin Chan dkk (2020) Hasil penelitian menunjukkan bahwa teknologi *blockchain*, yang mendasarkan diri pada buku besar publik, memberikan akses

kepada semua pihak tanpa otoritas pusat yang mengendalikan. Teknologi ini umumnya dimanfaatkan untuk keperluan registrasi dan *smart contract*. Dalam upaya memastikan keamanan dan keaslian informasi transaksi di dalam *blockchain*, banyak penelitian dilakukan terkait algoritma konsensus yang digunakan. Dalam ranah *blockchain*, terdapat banyak algoritma konsensus yang berbeda. Penelitian ini memiliki motivasi untuk menentukan area penelitian utama dan menemukan kunci terbaik dari algoritma konsensus. Fokus utama penelitian adalah pada *Proof of Stake* (PoS) dan *Delegated Proof of Stake* (DPoS). Selanjutnya, penelitian menelaah parameter utama yang digunakan dalam kedua algoritma tersebut. Setelah memperoleh parameter tersebut, dilakukan perbandingan kinerja keduanya, termasuk transaksi per detik, jumlah node, dan ukuran blok. Analisis lebih lanjut dilakukan untuk menyimpulkan efisiensi keduanya dari segi skalabilitas. Meskipun diharapkan bahwa kinerja DPoS lebih baik daripada PoS, hasil penelitian menunjukkan bahwa dampak dari parameter-parameter yang digunakan dapat dinilai dan dianalisis secara mendalam untuk membuktikan hasil tersebut.

Landasan Teori

Konsep *Proof of Stake* (PoS) merupakan paradigma konsensus di dalam jaringan *blockchain*, di mana *validator* blok dipilih berdasarkan jumlah koin atau token yang dimilikinya. Dibandingkan dengan *Proof of Work* (PoW), PoS menawarkan pendekatan yang lebih efisien dan ramah lingkungan. Kelebihannya meliputi efisiensi energi dan skalabilitas, meskipun keamanan dan potensi centralisasi tetap menjadi pertimbangan kritis (Guustaaf dkk, 2021).

Non-Fungible Token (NFT) adalah representasi digital unik dalam *blockchain* yang memberikan sertifikat kepemilikan terhadap suatu aset digital. Standar umum seperti ERC-721 dan ERC-1155 di *Ethereum* menentukan struktur dan operasi NFT. NFT membuka pintu bagi kepemilikan digital yang tidak dapat dipalsukan, mengubah cara nilai dan pertukaran aset digital (Torbeni dkk, 2022).

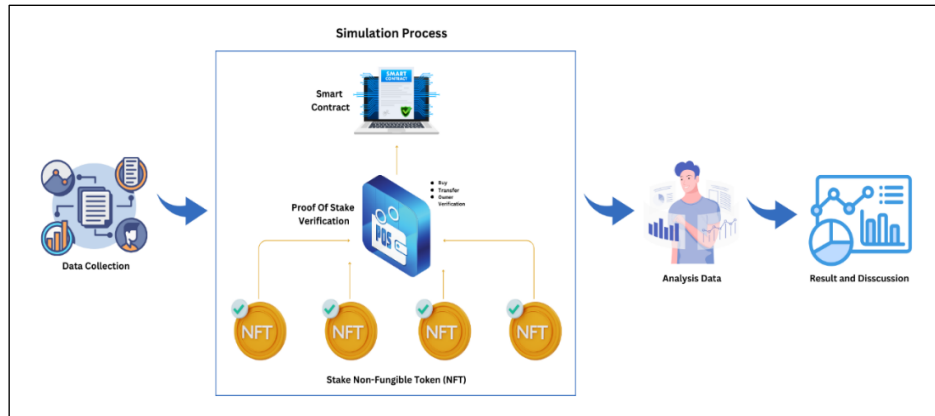
Smart Contracts adalah protokol otomatisasi di dalam *blockchain* yang dapat mengeksekusi, menegosiasikan, atau menegakkan kontrak digital. Dengan menggunakan bahasa pemrograman seperti *Solidity*, *Smart Contracts* memberikan kerangka kerja otomatisasi yang memungkinkan untuk menangani kontrak dan fungsi transaksi tanpa intermediasi pihak ketiga (Crystallography, 2016).

Integrasi PoS, NFT, dan *Smart Contracts* membawa dampak besar terhadap keamanan dan efisiensi operasional dalam ekosistem *blockchain*. Proses verifikasi PoS pada transaksi NFT memerlukan pemahaman mendalam tentang cara PoS diterapkan dan memengaruhi keamanan transaksi. Selain itu, otomatisasi dengan *Smart Contracts* dapat menyederhanakan proses transaksi dan mengurangi risiko kegagalan manusia dalam implementasi ini (Yeni & Kumala, 2020).

METODE PENELITIAN

Penelitian ini akan menggunakan pendekatan eksperimental yang merujuk pada penelitian Muh Ali dkk (2023) untuk menganalisis verifikasi *Proof of Stake* (PoS) pada *Non-Fungible Token* (NFT) dengan Teknologi *Smart Contract*. Eksperimen ini bertujuan

untuk mengumpulkan data empiris yang dapat memberikan wawasan mendalam tentang efektivitas integrasi tersebut dalam ekosistem *blockchain*. Langkah-langkah metode penelitian dapat dilihat pada Gambar 1.



Gambar 1. Langkah Metode Penelitian

Adapun Langkah-langkah pada Gambar 1 dapat dijelaskan sebagai berikut:

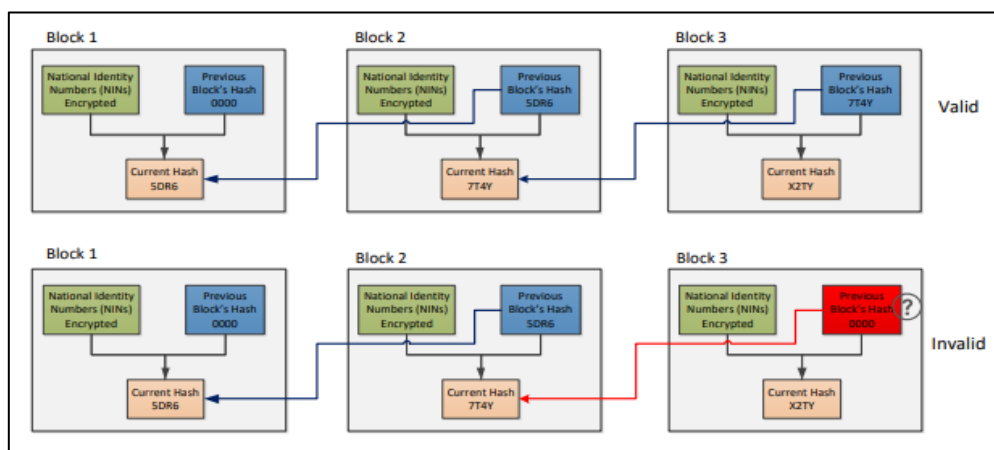
1. Pengumpulan Data (*Data Collection*)
Pada tahapan pertama proses pengumpulan data, pengumpulan data dilakukan oleh peneliti seperti literatur yang membahas mengenai proses verifikasi NFT pada PoS dan *Smart Contract*, pengumpulan data mengenai NFT yang baik digunakan dalam eksperimen ini seperti seni digital, koleksi virtual, atau permainan, selain itu pengumpulan data lainnya seperti memilih pembuatan aplikasi *Smart Contract* menggunakan *Solidity* dan cara untuk memasukan logika *Proof of Stake* (PoS) pada proses validasi dan transaksi.
2. Proses Simulasi (*Simulation Process*)
Pada tahapan selanjutnya, proses simulasi dilakukan terhadap beberapa data yang telah dikumpulkan untuk menjadi dasar pembangunan analisa ini, NFT yang telah didapatkan dan menjadi bahan eksperimen, selanjutnya aplikasi *Smart Contract* yang telah menggunakan logika verifikasi PoS akan memvalidasi proses transaksi NFT seperti proses pembelian, *transfer* dan kepemilikan. Pembuatan *Smart Contract* memanfaatkan *Solidity*.
3. Analisis Data (*Analysis Data*)
Berdasarkan proses simulasi yang telah dilakukan, pencatatan hasil yang dilakukan oleh peneliti dari simulasi tersebut yang kemudian akan dianalisis serta dibandingkan dengan metode tradisional lainnya seperti *Proof to Work* (PoW) atau metode lainnya, data yang dicatatkan seperti waktu transaksi, biaya transaksi, hasil verifikasi PoS, dan data lainnya yang relevan.
4. Hasil dan Diskusi (*Result and Discussion*)
Hasil dari analisis tersebut akan dirangkum dan ditarik kesimpulannya, tahap ini menjadi tahap terakhir dalam penelitian ini, integrasi NFT, PoS dan *Smart Contract* serta perbandingan antara *Proof of Stake* (PoS) dan *Proof of Work* (PoW) dalam NFT menggunakan teknologi *Smart Contract* akan ditampilkan untuk mengetahui

keunggulan serta kekurangan dalam analisis ini, selanjutnya peneliti akan memberikan saran untuk penelitian selanjutnya yang akan berguna dalam ekosistem *blockchain* kedepannya.

HASIL DAN PEMBAHASAN

Data Collection

Pada tahapan awal pengumpulan data yang dilakukan oleh peneliti termasuk mencari literatur yang membahas mengenai proses verifikasi NFT pada PoS dan *smart contract*, Adapun hasil yang didapatkan oleh peneliti yang mengadopsi jurnal dari Irwan Sembiring, dkk adalah Mekanisme Konsensus adalah validasi proses enkripsi melalui mekanisme konsensus yang digunakan dalam jaringan *blockchain*. Algoritma konsensus seperti *Proof of Work* (PoW) atau *Proof of Stake* (PoS) memastikan persetujuan di antara peserta jaringan dan memberikan lapisan keamanan tambahan untuk data terenkripsi. Fungsi hash SHA-256 memastikan integritas data yang kuat dan keamanan tambahan untuk data terenkripsi, seperti yang ditunjukkan dalam Gambar 2 (Sembiring dkk, 2023).



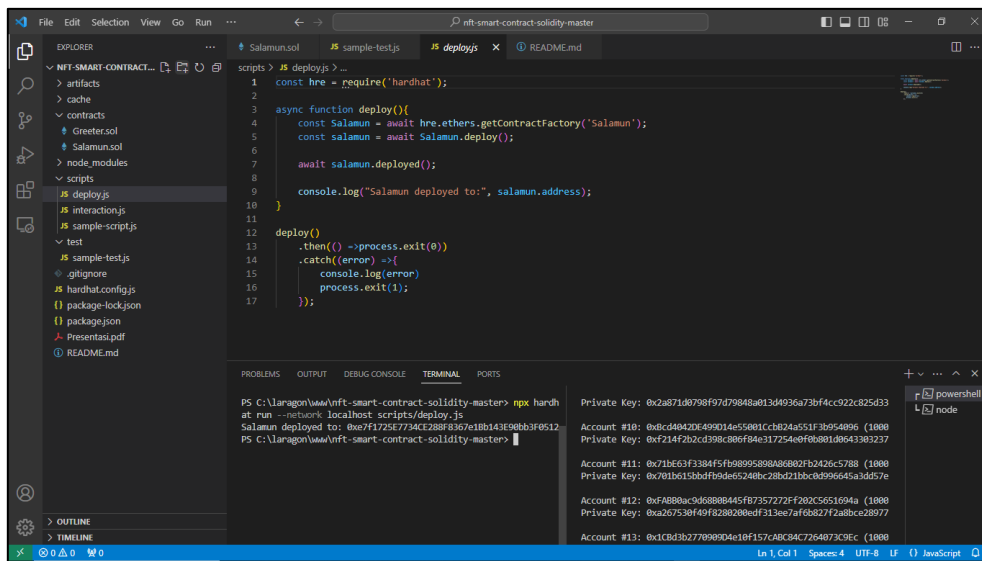
Gambar 2. Proses verifikasi *Proof of Stake* (PoS)

Simulation Process

1. Pembuatan *Smart Contract* dan *Stacking* NFT

Hasil pembuatan *Smart Contract Non-Fungible Token* (NFT) menggunakan bahasa pemrograman *Solidity* menggunakan metode *Proof of Stake* (PoS), merupakan Langkah awal yang dilakukan pada uji eksperimental pada penelitian ini, pembuatan *Smart Contract* menggunakan *clone* dari *Solidity* pada *Github* (<https://github.com/ethereum/solidity>) serta dibantu juga dengan penjelasan mengenai proses pembuatan *smart contract* dari *Github* faerulsalaman-nft-smart-contract-solidity (<https://github.com/faerulsalamun/nft-smart-contract-solidity>), langkah awal yang dilakukan yaitu menggunakan dokumentasi yang disediakan oleh *Hardhat* (<https://hardhat.org/>) yaitu `npm install --save-dev hardhat`, perintah ini sendiri digunakan untuk *install hardhat* pada project yang dibuat agar dapat mempermudah *development local*, selanjutnya penulis juga memanfaatkan *OpenZeppelin*

(<https://www.openzeppelin.com/>) sebagai *blueprint* untuk membuat pembuatan *smart contract* ini, dengan memasukkan perintah `npm install @openzeppelin/contracts` penggunaan *OpenZeppelin* telah tersedia pada proyek yang dikerjakan, selain itu pembuatan *smart contract* ini menggunakan *Visual Code Studio* sebagai *code editor* dikarenakan kemudahan yang diberikan serta mampu menjalankan Bahasa pemrograman ini, pembuatan *smart contract* ini juga bersifat *local* dijalankan menggunakan aplikasi *web service Laragon* (<https://laragon.org/download/index.html>) yang membantu agar dapat melihat serta dijalankan secara *local* pada *device* yang digunakan, pembuatan *smart contract* dapat dilihat pada Gambar 3.



Gambar 3. Pembuatan *Smart Contract* NFT Menggunakan Bahasa Pemrograman *Solidity*

Pada Gambar 3 juga telah digambarkan mengenai proses pembuatan *staking* NFT yang mempunyai beberapa nilai pada *account private*, contohnya pada *Account #1* memiliki *id* (`0x70997970C51812dc3A010C7d01b50e0d17dc79C8`) serta memiliki banyak *staking* yaitu (`10000 ETH`) serta memiliki *private key*: (`0xac0974bec39a17e36ba4a6b4d238ff944bacb478cbed5e`) hal ini menyatakan bahwa *Smart Contract* yang dibuat telah berhasil memberikan nilai *staking* dan juga proses *deploy* yang telah berhasil dilakukan dalam *local*, dalam hal ini pencatatan mengenai waktu pengiriman, kecepatan dan biaya transaksi serta hal-hal lainnya dicatatkan, serta akan menjadi bahan untuk perbandingan dengan metode Tradisional lainnya.

2. Proses verifikasi *Proof of Stake* (PoS) dalam *Smart Contract*

Kode Program 1:

```
function stakeuint256 tokenId_) external {  
    require(salamun.ownerOf(tokenId_) == msg.sender, "Bukan merupakan owner");  
    staked[tokenId_] = Stake  
    tokenId: tokenId_,  
    latestClaim: block.timestamp
```



```
});  
}
```

Kode Program 2:

```
function unstake(uint256 tokenId_) external {  
    require(salamun.ownerOf(tokenId_) == msg.sender, "Bukan merupakan  
owner");  
    require(staked[tokenId_].tokenId == tokenId_, "NFT belum di stake");  
    delete staked[tokenId_];  
}
```

Kode Program 3:

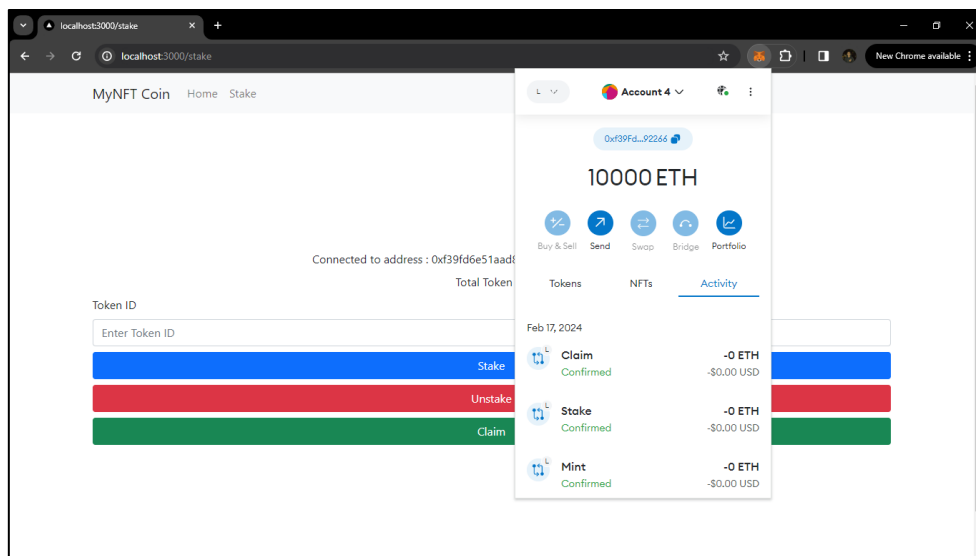
```
function claim(uint256 tokenId_) external {  
    require(salamun.ownerOf(tokenId_) == msg.sender, "Bukan merupakan  
owner");  
    require(staked[tokenId_].tokenId == tokenId_, "NFT belum di stake");  
    uint256 totalClaim = (block.timestamp - staked[tokenId_].latestClaim) / 5;  
    if(totalClaim > 0){  
        staked[tokenId_] = Stake({  
            tokenId: tokenId_,  
            latestClaim: block.timestamp - ((block.timestamp - staked[tokenId_].latestClaim) %  
5)  
        });  
    }
```

Mengadopsi literatur yang didapatkan oleh penelitian sebelumnya, proses verifikasi *Proof of Stake* (PoS) yang dilakukan oleh penulis dengan cara memasukan logika verifikasi PoS kedalam *code* yang telah dibuat, Kode Program 1,2 dan 3 menjelaskan bagaimana proses tersebut terjadi pemanggilan kode `msg.sender` sebagai *alert* atau informasi yang diberikan kepada pengguna dalam proses *stake*, *unstake* dan *claim* apakah pemilik token tersebut adalah *owner*, jika pemilik token tersebut adalah *owner* maka proses *stake*, *unstake* dan *claim* dapat dijalankan pada kontrak ini, Seluruh mekanisme ini bersama-sama menciptakan suatu model *Proof of Stake* sederhana di mana pemegang token yang melakukan *staking* diberikan *reward* berdasarkan waktu staking mereka. Konsep ini cocok dengan prinsip dasar *Proof of Stake* dimana pemilik token yang menahan token mereka dalam jangka waktu tertentu mendapatkan hak untuk mendapatkan *reward* dalam bentuk token tambahan.

3. Implementasi verifikasi *Proof of Stake* (PoS) dan *smart contract* pada *Web3 localhost*

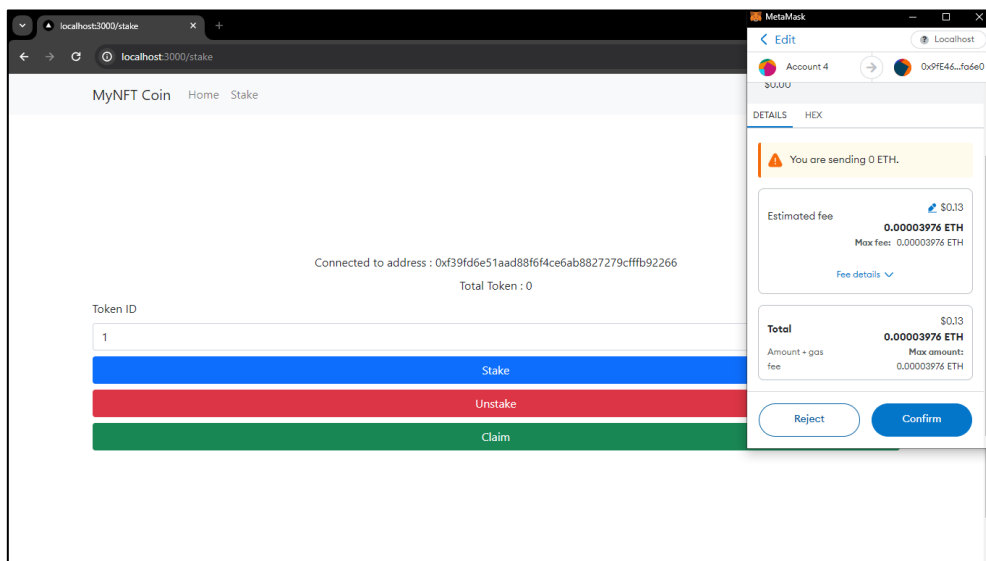
Setelah pembuatan *smart contract* dan logika verifikasi *Proof of Stake* (PoS) yang telah dilakukan oleh peneliti, kemudian proses implementasi untuk membuktikan bahwa kode telah berjalan dengan baik dengan sesuai maka pemanfaatan *Web3* dengan *webservice localhost*, dengan menggunakan perintah `npm run dev` pada *project* yang telah dibuat, *webservice* akan otomatis terbentuk dengan alamat akses (<http://localhost:3000>), tampilan ketika mengakses alamat ini secara otomatis akan menampilkan *wallet* pada *metamask* yang dimiliki oleh peneliti, dengan cara mengkoneksikan *wallet metamask*

dengan jaringan local yang telah dibuat sebelumnya serta memasukkan *private key* yang telah didapatkan pada proses *deploy*, *user* akan mendapatkan 10000 ETH yang nantinya akan digunakan sebagai transaksi pada *stake*, *unstake* dan *claim* dalam pembayaran gas, pada proses ini juga verifikasi PoS telah dijalankan, dilihat pada Gambar 4, alamat dompet atau id transaksi yang berhasil terkoneksi dengan jaringan local dengan status *Connected to address : 0xf39fd6e51aad88f6f4ce6ab8827279cfff92266*, hal ini membuktikan bahwa proses PoS telah memverifikasi bahwa token dan dompet merupakan *owner* dan telah siap dalam melakukan proses transaksi.



Gambar 4. Tampilan Web3 (<http://localhost:3000>)

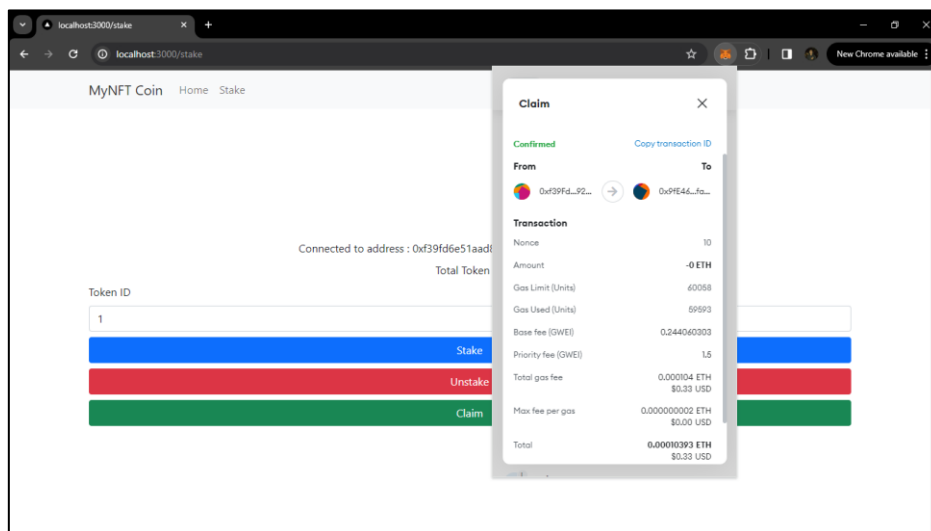
4. Proses *Staking*, *Unstake* dan *Claim* pada Web3



Gambar 5. Proses *Staking* pada Web3

Pada Gambar 5, ditampilkan mengenai proses *staking* yang dilakukan oleh pemilik token, *wallet metamask* akan otomatis juga menampilkan biaya gas serta untuk memverifikasi apakah pemilik token benar merupakan *owner*, setelah melakukan pembayaran sesuai dengan prinsip dasar *Proof of Stake* dimana pemilik token yang menahan token mereka dalam jangka waktu tertentu mendapatkan hak untuk mendapatkan *reward* dalam bentuk token tambahan, proses ini pun terjadi pada penelitian kali ini, proses *stake*, *unstake* dan *claim* memiliki cara kerja yang sama dengan cara memasukan *Token Id* dan membayar gas yang telah ditentukan untuk tercapainya proses transaksi.

5. Pencatatan *Staking*, *Unstake* dan *Claim* pada proses transaksi



Gambar 6. Pencatatan *Staking*, *Unstake* dan *Claim* pada proses transaksi

Pada Gambar 6, seluruh proses transaksi ditampilkan pada *wallet metamask* yang artinya proses transaksi telah berhasil, rincian dari proses transaksi yang merupakan bukti dapat dilihat secara langsung, serta rincian mengenai dari dompet pengirim ke penerima serta biaya gas, waktu hingga total jumlah pengiriman yang ditampilkan.

Analysis Data

Berdasarkan dengan hasil simulasi yang telah dilakukan oleh peneliti, *Proof of Stake* (PoS) dan *Proof of Work* (PoW) Wikarsa dkk (2022) yang akan dibandingkan dengan cara mencari literatur mengenai PoW serta serupa dengan proses yang dijalankan oleh peneliti, maka dari itu didapatkan hasil pada Tabel 1. Berdasarkan hasil analisis, *Proof of Stake* (PoS) menunjukkan keunggulan dalam efisiensi waktu transaksi, biaya yang lebih rendah, keamanan yang ditingkatkan melalui pemilihan validator yang cermat, dan resistensi terhadap beberapa jenis serangan. Dengan demikian, PoS dapat dianggap sebagai metode konsensus yang lebih baik dalam mencapai tujuan keamanan dan efisiensi yang diinginkan dalam konteks ekosistem *blockchain*.

Tabel 1. Analisis Perbandingan *Proof of Work (PoW)* dan *Proof of Stake (PoS)*

No.	Kriteria Analisis	<i>Proof of Work (PoW)</i> <i>Result</i>	<i>Proof of Stake (PoS)</i> <i>Result</i>
1.	Waktu Transaksi	Lebih lama; memerlukan konfirmasi mining	Lebih cepat; berbasis jumlah staking
2.	Biaya Transaksi	Lebih tinggi; dipengaruhi oleh energi dan perangkat keras	Lebih rendah; efisien dan biaya transaksi yang lebih terkontrol
3.	Reward dan Verifikasi	Berbasis <i>mining</i> ; <i>reward</i> untuk penambang	Berbasis <i>staking</i> ; <i>reward</i> untuk pemegang token <i>staking</i> dan hasil verifikasi
4.	Pemilihan Validator	Tergantung pada kekuatan komputasi; potensi risiko 51% attack	Berbasis kepemilikan token; meningkatkan desentralisasi dan keamanan
5.	Ketahanan terhadap Serangan	Rentan terhadap 51% <i>attack</i> ; <i>risiko long-range attack</i>	Tinggi; mitigasi risiko melalui desain PoS
6.	Desentralisasi	Tingkat desentralisasi tergantung pada distribusi kekuatan komputasi	Lebih tinggi; pemilihan validator berdasarkan kepemilikan token
7.	Penggunaan Energi	Memerlukan konsumsi energi tinggi	Lebih efisien; tidak memerlukan kegiatan penambangan fisik
8.	Skalabilitas	Terbatas oleh kecepatan transaksi dan tingginya biaya transaksi	Lebih mudah diimplementasikan dan dapat mencapai skalabilitas yang lebih baik
9.	Partisipasi Pemegang Token	Lebih terbatas; memerlukan investasi besar dalam perangkat keras	Lebih terbuka; lebih mudah untuk partisipasi pemegang token
10.	Kesulitan Penambangan	Tinggi; membutuhkan perangkat keras khusus dan energi tinggi	Lebih rendah; berbasis jumlah staking dan keamanan PoS

KESIMPULAN DAN SARAN

Kesimpulan

Berdasarkan hasil dari penelitian yang telah dilakukan oleh penulis pada Analisis Verifikasi *Proof of Stake (PoS)* NFT dengan Teknologi *Smart Contract* menggunakan metode eksperimental, didapatkan bahwa peneliti telah berhasil membuat dan menjalankan sesuai dengan tujuan permasalahan yang ingin dicapai, beberapa hal yang

berhasil didapatkan yaitu mengenai proses verifikasi PoS yang berjalan sesuai dengan prinsipnya, proses *Stake*, *Unstake*, dan *Claim* yang telah berhasil memanfaatkan Web3 dan *metamask wallet*, pencatatan transaksi sesuai dengan waktu pengirim dan penerima serta verifikasi *owner* yang telah dilakukan, selain itu peneliti menemukan perbandingan antara Analisis Perbandingan *Proof of Work* (PoW) dan *Proof of Stake* (PoS) yang menyatakan bahwa *Proof of Stake* (PoS) menunjukkan keunggulan dalam efisiensi waktu transaksi, biaya yang lebih rendah, keamanan yang ditingkatkan melalui pemilihan validator yang cermat, dan resistensi terhadap beberapa jenis serangan.

Saran

Setelah berhasil menyelesaikan penelitian ini, harapan dari peneliti sebagai saran penelitian kedepannya dengan membuat beberapa eksperimen seperti yang telah dibuat sebelumnya dan membandingkan hasil temuan yang dilakukan dengan penelitian ini, saran selanjutnya lebih kepada token yang digunakan, dikarenakan penelitian ini menggunakan NFT saran kepada penelitian selanjutnya dengan menggunakan token lainnya seperti ETH, DOGE dan lainnya.

DAFTAR PUSTAKA

- Crystallography, X. D. (2016). Tinjauan Yuridis Penerapan SMart Contract DI Indonesia Sebagai Bentuk Perkembangan Kecerdasan Buatan (ARTificial Intelligence). 1–23.
- Fauzi, E., Yuliani, S., Syukriyah, Y., & Zakiah, A. (2023). Model Implementasi Nft Pada Web Sso Melalui Protokol Openid Connect Dan Oauth 2.0 Model of Nft Implementation on Web Sso Over Openid Connect and Oauth 2.0 Protocols. *Journal of Information Technology and Computer Science (INTECOMS)*, 6(2).
- Firdaus, D. H. (2020). Aplikasi Smart Contract dalam E-Commerce Prespektif Hukum Perjanjian Syariah. *Jurnal Qolamuna*, 6(1), 37–54. <https://apjii.or.id/survei>,
- Guustaaf, E., Rahardja, U., Aini, Q., Santoso, N. A., & Santoso, N. P. L. (2021). Desain Kerangka Blockchain terhadap pendidikan: A Survey. *CESS (Journal of Computer Engineering, System and Science)*, 6(2), 236. <https://doi.org/10.24114/cess.v6i2.25099>
- Kin Chan, W., Zhang, R., & Chan, W. K. (2020). Evaluation of Energy Consumption in Block-Chains with Proof of Work and Proof of Stake. *Journal of Physics: Conference Series*, 1584(1). <https://doi.org/10.1088/1742-6596/1584/1/012023>
- Michael, J. W., Cohn, A., & Butcher, J. R. (2015). Journal introduction. *Journal of Cardiovascular Computed Tomography*, 9(4), 249. <https://doi.org/10.1016/j.jcct.2015.05.009>
- Muh Ali, A., Satriawati, S., & Nur, R. (2023). Meningkatkan Hasil Belajar IPA Menggunakan Metode Eksperimen Kelas VI Sekolah Dasar. *PTK: Jurnal Tindakan Kelas*, 3(2), 114–121. <https://doi.org/10.53624/ptk.v3i2.150>
- Rizki Pratama, M. (2023). Konsep Implementasi Metode Konsensus Proof of Work dan Proof of Stake pada Permainan Poker Daring Berbasis Blockchain. 18220110.
- Saad, S. M. S., Radzi, R. Z. R. M., & Othman, S. H. (2021). Comparative Analysis of the Blockchain Consensus Algorithm between Proof of Stake and Delegated Proof of

- Stake. 2021 International Conference on Data Science and Its Applications, ICoDSA 2021, 10(2), 175–180.
<https://doi.org/10.1109/ICoDSA53588.2021.9617549>
- Sari, D. P. (2022). Pemanfaatan Nft Sebagai Peluang Bisnis Pada Era Metaverse. *Akrab Juara : Jurnal Ilmu-Ilmu Sosial*, 7(1), 237.
<https://doi.org/10.58487/akrabjuara.v7i1.1770>
- Schmitz, A. J. (2022). Resolving NFT and Smart Contract Disputes. *SSRN Electronic Journal*, 360(2017). <https://doi.org/10.2139/ssrn.4162969>
- Sembiring, I., Manongga, D., & Saian, S. D. S. (2023). Strengthening the Security and Privacy of National Identity Numbers (NINs) in Smart Contract Mechanisms through AES Encryption. *Journal of Logistics, Informatics and Service Science*, 10(4), 174–188. <https://doi.org/10.33168/JLISS.2023.0412>
- Torbeni, W., Putu, N., Lestari, E. B., Komang, I., & Putra, A. M. (2022). Mengenal Nft Arts Sebagai Peluang Ekonomi Kreatif Di Era Digital. *Online) SENADA*, 5, 342–357. <http://senada.idbbali.ac.id>
- Wikarsa, L., Suwanto, T., & Lengkey, C. (2022). Implementasi Algoritma Konsensus Proof-of-Work dalam Blockchain terhadap Rekam Medis Implementation of Proof-of-Work Consensus Algorithm in Blockchain for Medical Records. *Jurnal Pekommas_Vol. 7_No. 1*, 7(1), 41–52.
<https://doi.org/10.30818/jpkm.2022.2070105>
- Yeni, M., & Kumala, D. (2020). Teknologi Blockchain untuk Transparansi dan Keamanan pada Era Digital. 6. <http://repository.unmuha.ac.id/xmlui/handle/123456789/579>