From NFTs to Tokens: The Evolution of Blockchain Services in Internet Computing

Dr.Jitendra Saturwar
HoD, Computer Department
Universal College of Engineering
Thane, India

Khushi Nairy
Computer Department
Universal College of Engineering
Thane, India

Vismay Malviya
Computer Department
Universal College of Engineering
Thane, India

Shahima Khan
Computer Department
Universal College of Engineering
Thane, India

***Abstract*—This study has been undertaken to determine a model which works on Internet Computer, which is the world's highest usage public blockchain. This study shows the next generation blockchain features of Internet Computing in combination with Canister Development Kit (CDK) and Chain Key Technology (CKT). An important feature - ICP token is applied on an actual NFT exchange platform. The system being developed uses WebAssembly (WASM) to compile smart contracts which are written in motoko in such a format that they can be executed on Internet Computer. The Network Nervous System (NNS) is used to manage the allocation of resources on the Internet Computer, ensuring that the network remains stable and efficient. Hence presenting a decentralized finance (DeFi) application built on Internet Computer blockchain: Crypton.**

Keywords—Internet Computing, Cryptocurrency, Non Fungible Tokens, Blockchain.

I. Introduction

This article's primary objective is testing and implementing the next generation features of the Internet Computing with the combination of blockchain, as internet computing and blockchain are complementary technologies that can be leveraged together to build innovative solutions for various industries, including finance, supply chain management, healthcare and more and hence we bring a new application of the Internet Computing with this study.

Smart contract specific blockchains do face a significant challenge with partial decentralization due to the deployment of their front-end on third-party servers such as AWS, Mailchimp, and Heroku as well. This arrangement leaves the power to shut down these Decentralized Apps with mainstream companies, thus calling into question the completeness of their decentralization. To address such issue, we aim to explore and leverage the Internet Computer blockchain, which allows for the complete deployment of code on the platform without the interference of third-party servers. This approach enables us to achieve true decentralization of our DApps, thereby ensuring maximum security, reliability and trust for our users.

Internet Computer is a platform to run any computation using blockchain for decentralization and security. The original whitepaper defines it as: "The Internet Computer (IC) is a new platform for executing smart contracts. Here, we use the term 'smart contract' in a very broad sense- a general-purpose, tamperproof. computer program whose execution is performed autonomously on a decentralized public network."

For end-users, accessing IC-based services is always largely transparent. The Internet Computer is a Web3 platform that provides a complete alternative to the traditional IT stack. The Internet Computer introduces a new form of smart contracts: canisters smart contracts, which has powerful capabilities that enable the cryptocurrency cloud.

The Internet Computer is created by the ICP (Internet Computer Protocol), the most advanced network protocol ever devised, in ICP the independent node providers own and operate node machines in data centers worldwide and hence the ICP combines such nodes to form efficient subnet blockchains. Subnet blockchains add the capacity for running canister smart contracts, and at the end such subnets combine into one such serverless autonomous cloud with unbounded capacity which is known as the Internet Computer, which is ultimately a new derived blockchain network.

To actually implement these features we have built a DeFi application which is a NFT exchange system. The application is built using Motoko, a programming language designed for developing smart contracts on the Internet Computer (IC). The front-end of the application is built using React, while the back-end is built using the Canister Development Kit (CDK), which provides a set of tools and libraries for developing and deploying canisters on the Internet Computer. The Crypton application uses Chain Key Technology (CKT) to securely and efficiently manage the keys used to sign transactions on the blockchain. Internet Identity (II) is used for user authentication, providing a secure and decentralized identity system that users can use to log in to the application.

II. Literature Survey

A literature analysis was conducted to find multiple articles linked to the pertinent study that has/had been published in international magazines, journals, books, etc in order to understand the concept and protocol more precisely and to look out for their applications as well that will suit our study.

R. Gupta, V. Sekhri, A. K. Somani. CompuP2P: An Architecture for Internet Computing Using Peer-to-Peer Networks [1]. Here the CompuP2P is a lightweight architecture for enabling Internet Computing. It simply uses peer-to-peer networks for sharing of computing resources. This following paper discusses the system architecture, functionality, and applications of the proposed CompuP2P architecture.

Satoshi Nakamoto. A peer-to-peer electronic cash system [2]. The paper proposes a decentralized digital currency system called Bitcoin, aiming to enable peer-to-peer transactions without the need for central authority. It introduces the concept of blockchain technology as a means of maintaining a secure, transparent ledger of transactions.

Nikita K., Antorweep C., Chunming R., [3]. Blockchain Based Transaction System with Fungible and Non-Fungible Tokens for Community-Based Energy Infrastructure. This study presents a unified blockchain-based system for energy asset transactions among prosumers, electric vehicles, power companies, storage providers, etc.

Akash A., Kanishk, Shailendra K., [4]. Smart Contracts and NFTs: Non-Fungible Tokens as a core component of Blockchain to be used as Collectibles. While outlining the theoretical implications and use cases of NFTs, it mainly aims to analyze blockchain and cryptocurrencies' technical underpinnings, specifically non-fungible tokens or "crypto-collectibles".

Jens Groth, [5]. Dfinity Foundation. Non-interactive distributed key generation and key resharing. The paper discusses its new contribution that is constructing non-interactive distributed key generation and key resharing protocols for threshold BLS signatures in the context of the Internet Computer. The protocols are built on a new pairing-based CCA-secure public-key encryption scheme with forward secrecy.

DFINITY Foundation, [6]. The internet computer for geeks. The following whitepaper explains in detail the major scientific and engineering breakthroughs behind the Internet Computer. The Internet Computer, which is based on a set of cryptographic protocols that combine hardware node machines running within independent data centers into a collection of subnet blockchains.

Koushik B.M., Khushboo S., Karthik E.M., [7]. A Blockchain Based Decentralized Computing And NFT Infrastructure For Game Networks. The paper aims to create and study a decentralized computation and token management infrastructure for game networks. It also focuses on using Ethereum Blockchain, IPFS and ERC - Ethereum Request for Comment 1155 architecture to build a gaming-oriented public decentralized network.

III. Proposed System

Our team has designed a secure and scalable NFT marketplace on the Internet Computer Protocol (ICP) blockchain. Our team's secure and scalable NFT marketplace on the ICP blockchain leverages Internet Identity for user authentication on the frontend. Here's an update to our previous explanation Here's a breakdown of the system architecture:

Frontend Authentication with Internet Identity:
We utilize Internet Identity on the Frontend Wallet Canister and the Frontend NFT Marketplace Canister. This allows users to authenticate securely without managing usernames and passwords.During login, the frontend canister interacts with the Internet Identity Service Canister on the ICP blockchain.Upon successful authentication, the Internet Identity Service Canister provides a cryptographic token or signature to the frontend canister.This token or signature is then used by the frontend canister to identify the user and potentially access user-specific data from the backend canisters.

Microservices with Canisters:
Frontend Wallet Canister: This React canister provides a user-friendly interface for managing wallets. It interacts with the Backend Wallet Canister to retrieve and display data using props.
Backend Wallet Canister: This Motoko canister serves as the brain of the wallet system. It handles functionalities like viewing balances and interacting with the Chronos token system. It communicates with the Chronos backend and potentially the NFT Marketplace backend.
Frontend NFT Marketplace Canister: This React canister drives the user experience for buying, selling, and exploring NFTs. It utilizes props to exchange data with the Backend NFT Marketplace Canister.
Backend NFT Marketplace Canister: This Motoko canister is the engine of the marketplace. It manages NFT listings, purchases, ownership transfers, and interacts with the Chronos backend for currency transactions. It might also communicate with the Frontend Wallet Canister for user information.

Seamless Chronos Integration:
Frontend Chronos Canister: This React canister allows users to interact with Chronos functionalities like claiming faucet tokens, transferring, receiving, buying, and selling NFTs. It retrieves data from the Backend Chronos Canister using props.
Backend Chronos Canister: This Motoko canister handles the core logic behind Chronos integration. Since Motoko doesn't natively support arrays, we've implemented temporary arrays to efficiently process data retrieved from hash tables (chosen for stability and persistence) before sending it to the frontend.

Secure and Efficient Communication:
Canisters communicate with each other through well-defined calls within their interfaces. These calls can involve data transfer or invoking functions on the receiving canister.
Communication likely happens through the Internet Computer Service Nervous System (SNS), the backbone for inter-canister calls on the ICP blockchain.

Focus on Security and Scalability:
Security is paramount. We've implemented robust authentication and authorization mechanisms to safeguard user funds and NFTs using internet identity
Scalability is a key consideration. The architecture is designed to handle increased user traffic and data volume as our marketplace thrives.
User Experience Matters: We've optimized data fetching and rendering processes to minimize lag and ensure a smooth user experience.

Uploading the crypton_backend Canister: The Wasm binary file would then be uploaded to the ICP blockchain as the backend canister "crypton_backend". This can be done using the DFX CLI as well.

Interacting with the ICP Blockchain: Once both canisters are deployed to the ICP blockchain, the frontend canister would be able to interact with the backend canister using the provided canister interface. This interface allows the frontend to send messages to the backend canister and receive responses, enabling the two canisters to communicate with each other and perform the necessary actions for the application.

Overall, the process involves compiling and uploading both the frontend and backend canisters to the ICP blockchain, and using the provided canister interface to enable communication between them.

IV. Methodology

The methodology section describes the experimental work done to claim the ICP tokens which can be later used to buy and sell the NFT (art) and even claim on a daily basis.

Create a decentralized NFT marketplace: The system's goal is to establish a platform where users can trade NFTs without relying on a central authority. This approach ensures transparent, secure, and tamper-proof transactions, eliminating the potential for censorship or external interference.

Utilize the capabilities of the Internet Computer blockchain: The system harnesses the power of the Internet Computer blockchain, capitalizing on its benefits such as rapid, cost-effective transactions, scalability, and robust security. These advantages are pivotal in offering users a smooth and efficient marketplace experience.

Guarantee utmost security and dependability: Through the innovative architecture of the Internet Computer blockchain, the system removes the reliance on third-party servers, ensuring heightened control over data and privacy.

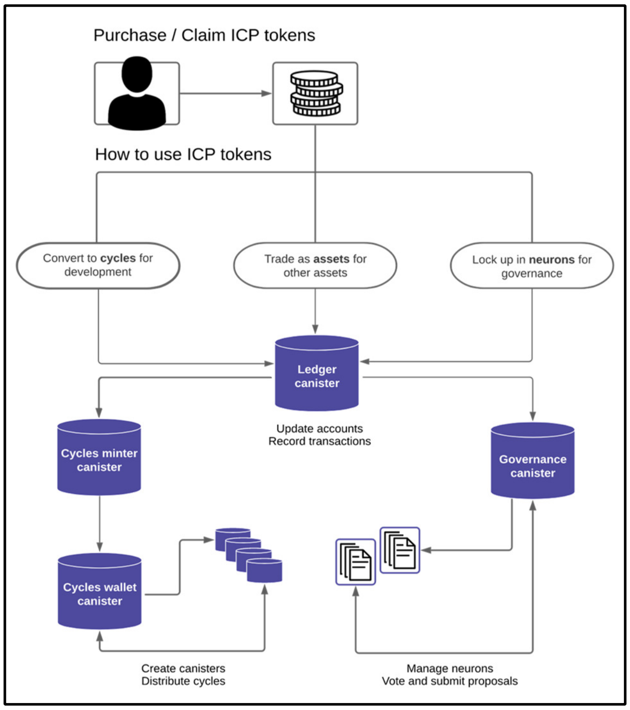

Figure 1 : Claiming the ICP Tokens

Offer an intuitive interface and user-friendly features: The system prioritizes user experience by providing an intuitive interface, simplifying navigation for both buyers and sellers. Features like search and filtering options, bidding and purchasing mechanisms, and user-friendly digital wallet management enhance the overall user experience.

Nurture a dynamic community of creators, collectors, and enthusiasts: The system aims to cultivate a vibrant community of NFT creators, collectors, and enthusiasts. By facilitating social sharing, encouraging user-generated content, and organizing community-driven events, the platform fosters engagement and innovation within the broader digital asset ecosystem.

V. System Architecture

The architecture of the Crypton is designed to provide a highly scalable, secure, and efficient platform for building and deploying decentralized applications (DApps) and services. The following are the key components of the ICP architecture:

Network: The ICP network consists of a global network of independent data centers, or nodes, that are interconnected via the internet. These nodes work together to provide a decentralized platform for hosting dApps and services.

Chain Key Technology (CKT): ICP uses a novel consensus mechanism called Chain Key Technology (CKT) to achieve fast and efficient validation of transactions on the network. CKT provides a secure way to validate transactions and reach consensus without relying on traditional mining methods used by other blockchain platforms.

Canister: A canister is a secure and isolated environment within the ICP network that hosts dApps and services. Each canister has its own memory and processing resources, and can interact with other canisters on the network.

Internet Identity (II): Internet Identity is a decentralized identity system that allows users to create and manage their identities on the ICP network. II provides a secure and user-friendly way to authenticate users and manage access to dApps and services on the network.

WebAssembly (WASM): ICP uses WebAssembly as its primary programming language for building dApps and services. WASM is a low-level virtual machine that enables efficient execution of code in a secure and sandboxed environment.

Network Nervous System (NNS): The Network Nervous System is a governance mechanism that allows the ICP community to propose and vote on changes to the network. NNS ensures that the network is secure, stable, and adaptable to changing requirements.

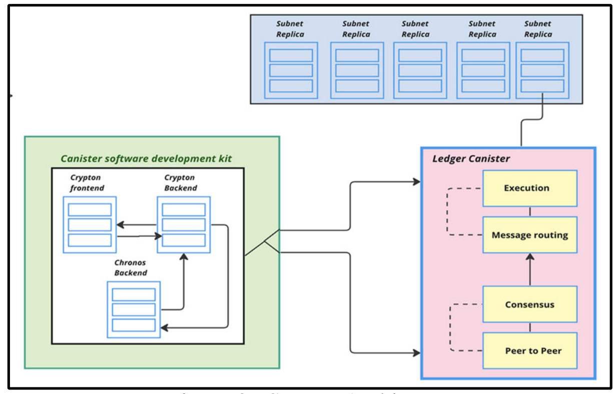

Figure 2 : System Architecture

Internal Canister Communication

Communication between frontend and backend canisters within the same microservice (wallet or marketplace) primarily leverages props in React. This mechanism allows the frontend canister to:

Send requests to the backend canister by invoking functions defined in its interface.

Receive responses from the backend canister containing the requested data or results.

Backend canisters might also need to communicate with each other to fulfill user actions. This communication likely utilizes similar function calls defined in the respective canister interfaces. For example, the NFT marketplace backend might call the wallet backend to verify a user's balance before completing an NFT purchase.

External Canister Communication (Chronos)

The Chronos integration involves two canisters:

Frontend Chronos Canister: This React canister allows users to interact with Chronos functionalities (claiming faucet tokens, transferring tokens).

*Backend Chronos Canister***:** This Motoko canister handles core Chronos logic.

Communication between these canisters and the external Chronos system likely involves the Internet Computer Service Nervous System (SNS). Here's the breakdown:

1. The Frontend Chronos Canister sends user requests (as props) to the Backend Chronos Canister.
2. The Backend Chronos Canister interacts with the Chronos canister on the ICP blockchain (potentially through the SNS) to execute the requested functions.
3. The Chronos canister processes the request and sends a response back to the Backend Chronos Canister.
4. The Backend Chronos Canister receives the response and sends it back to the Frontend Chronos Canister through props.

VI. Model

Figure 3 shows the Entity Relationship Diagram of the proposed system. Entity Relationship diagram is a data modeling technique that graphically illustrates an information system's entities and the relationships between those entities. Here, the entities are: - User, Ethereum Wallet ,Crypton Wallet, Chronos, and Internet Identity owner. The diagram shows the different attributes of these entities and also shows the relationship among these different entities.

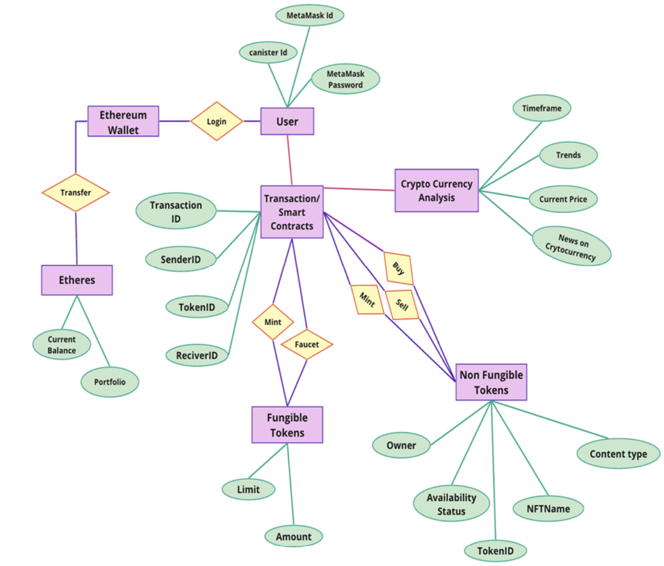

Figure 3: Entity-Relationship Diagram

Following are the DFD Level 0 (Figure 4), Level 1 (Figure 5) and Level 2 (Figure 6) diagrams of the working model and Use Case Diagram (Figure 7):

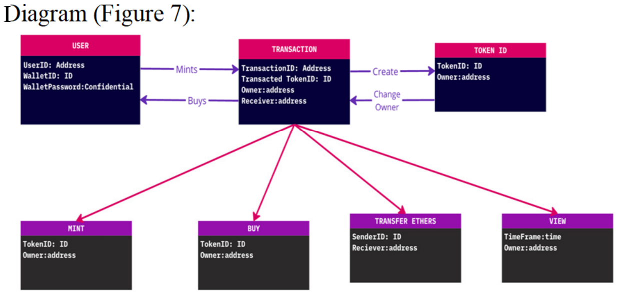

Figure 4 : DFD Level 0

The FT and NFT encoded in the Crypton backend can interact with different users on the Internet Computer (ICP) blockchain through the frontend and backend canisters. When a user interacts with the frontend canister, they can initiate a request to buy or sell a token. The frontend canister can then send this request to the backend canister which will handle the processing of the transaction.

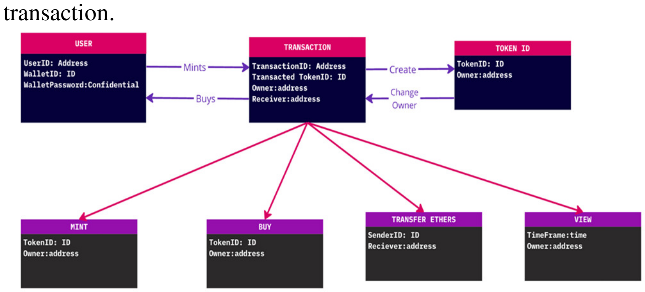

Figure 5 : DFD Level 1

The backend canister will have code to interact with the ICP blockchain, including smart contracts for handling the buying and selling of tokens. When a user initiates a request to buy or sell a token, the backend canister will perform the necessary checks, such as verifying that the user has sufficient funds or that the token being sold is valid.

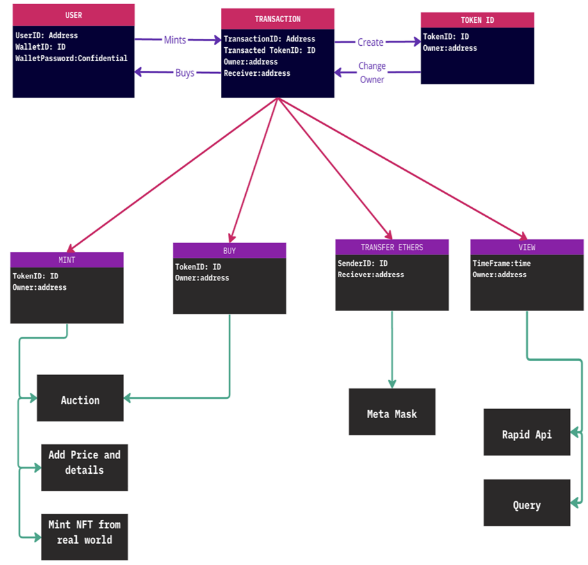

Figure 6 : DFD Level 2

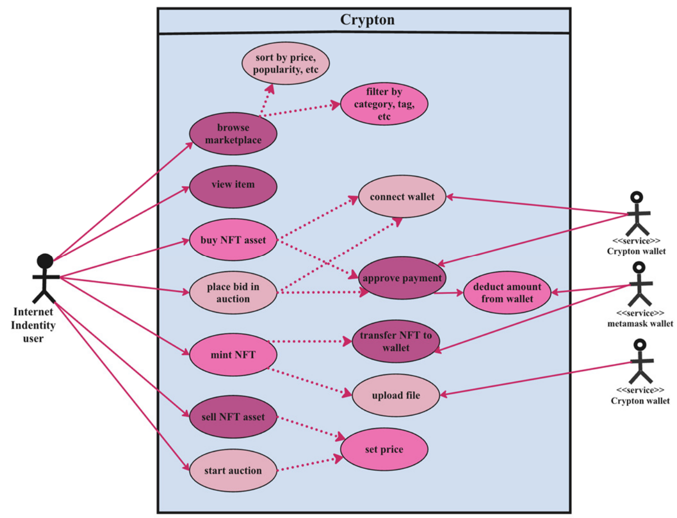

Figure 7 : Use Case Diagram

The backend canister will have code to interact with the ICP blockchain, including smart contracts for handling the buying and selling of tokens. When a user initiates a request to buy or sell a token, the backend canister will perform the necessary checks, such as verifying that the user has sufficient funds or that the token being sold is valid.

Once the backend canister has processed the transaction, it will update the state of the FT or NFT on the ICP blockchain, reflecting the new ownership or changes to the token's metadata. The backend canister can also update the user's account balance to reflect the purchase or sale of the token.

The frontend canister can then receive the updated information from the backend canister and display it to the user, showing the updated token ownership, account balance, and any other relevant information.

VIII. RESULTS

The existing system that is implemented will provide a decentralized platform for digital assets, enabling direct person-to-person transactions while removing the intermediaries from the process and creating a secure, transparent blockchain infrastructure to host the decentralized applications. It addresses the problems related to the size and ease of use commonly seen in current blockchain technologies while utilizing advanced cryptographic methods to ensure the safe and provable storage and transfer of data and facilitates community engagement and decision-making through the Network Nervous System. Figure 8 shows the GUI of Crypton.

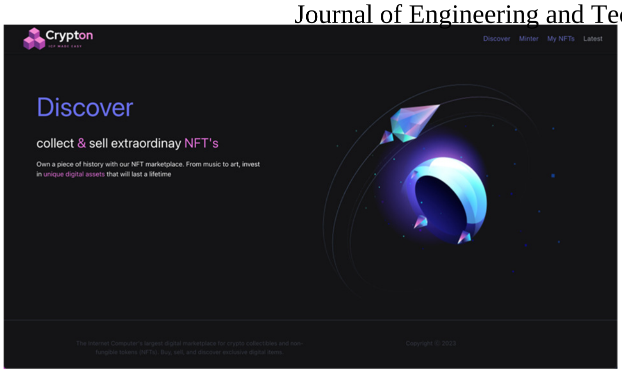

Figure 8 : GUI of Crypton

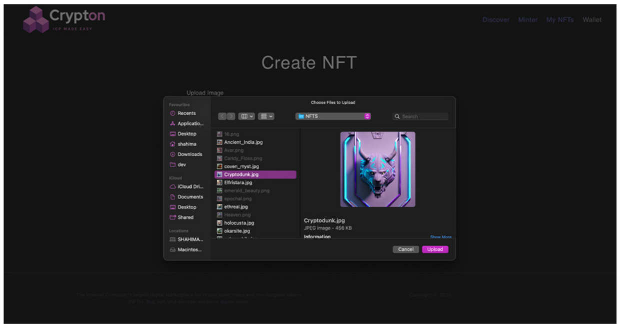

Figure 9 : Create NFT from your system

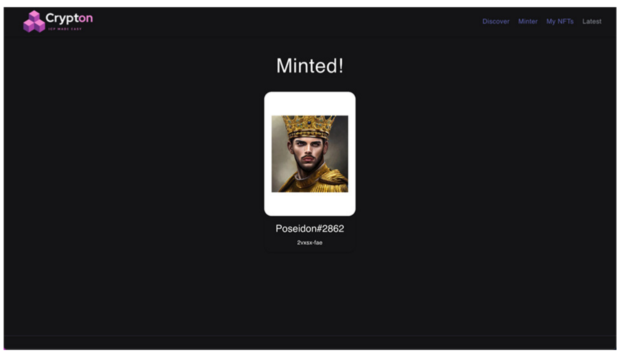

Figure 10 : GUI of Successfully Minted the NFT

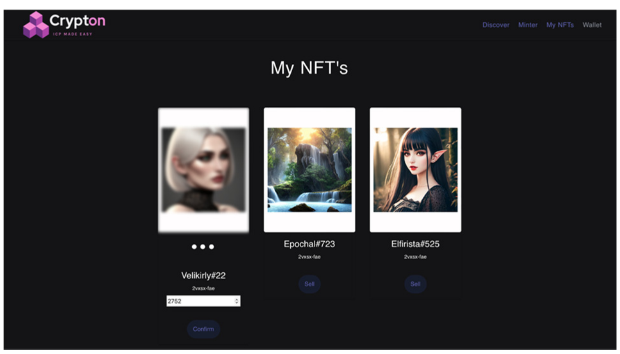

Figure 11 : GUI of desktop Application

Figure 12 : GUI of claiming tokens from the faucet

VIII. Conclusion

Hence, in conclusion we say that Crypton represents a pioneering step towards achieving true decentralization in the realm of decentralized finance (DeFi) applications, and so by leveraging the Internet Computer (IC) blockchain, Crypton overcomes the challenges posed by partial decentralization encountered by smart contract-specific blockchains. Through the complete deployment of code on the platform without reliance on third-party servers, Crypton ensures and aims for maximum security, reliability, and trust for its users.

Furthermore, the adoption of Internet Identity (II) for user authentication enhances the security and decentralization of the platform, providing the users with a secure and decentralized identity system for accessing the application securely.

The introduction of Crypton's native tokens, chronos, does facilitate seamless transactions within the platform, offering users a convenient and efficient means of engaging with the ecosystem. The inclusion of the chronos claiming interface, known as the faucet, further enhances the accessibility and user engagement.

In essence, Crypton embodies the ethos of decentralization, security, and user empowerment, paving the way for the future of Decentralized Finance (DeFi) applications on the Internet Computer blockchain. As the cryptocurrency landscape continues to evolve, Crypton stands as a testament to the transformative potential of blockchain technology in revolutionizing financial systems and empowering individuals worldwide.

References

[1] R. Gupta, V. Sekhri, A. K. Somani. CompuP2P: An Architecture for Internet Computing Using Peer-to-Peer Networks.

[2] Satoshi Nakamoto. A peer-to-peer electronic cash system.

[3] Nikita K., Antorweep C., Chunming R. Blockchain Based Transaction System with Fungible and Non-Fungible Tokens for Community-Based Energy Infrastructure.

[4] Akash A., Kanishk, Shailendra K. Smart Contracts and NFTs: Non-Fungible Tokens as a core component of Blockchain to be used as Collectibles.

[5] Jens Groth. Dfinity Foundation. Non-interactive distributed key generation and key resharing.

[6] DFINITY Foundation. The internet computer for geeks.

[7] Koushik B.M., Khushboo S., Karthik E.M. A Blockchain Based Decentralized Computing And NFT Infrastructure For Game Networks.

[8] How to trade cryptocurrencies: A beginner's guide to buy and sell digital currencies. https://cointelegraph.com/trading-for-beginners

[9] [BGLS03] D. Boneh, C. Gentry, B. Lynn, and H. Shacham. Aggregate and Verifiably Encrypted Signatures from Bilinear Maps. In E. Biham, editor, Advances in Cryptology - EUROCRYPT 2003, International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4-8, 2003, Proceedings, volume 2656 of Lecture Notes in Computer Science, pages 416– 432. Springer, 2003.

[10] [BKM18] E. Buchman, J. Kwon, and Z. Milosevic. The latest gossip on BFT consensus, 2018. arXiv:1807.04938, http://arxiv.org/abs/1807.04938. [BLS01] D. Boneh, B. Lynn, and H. Shacham. Short Signatures from the Weil Pairing. In C. Boyd, editor, Advances in Cryptology - ASIACRYPT 2001, 7th International Conference on the Theory and Application of

Cryptology and Information Security, Gold Coast, Australia, December 9-13, 2001, Proceedings, volume 2248 of Lecture Notes in Computer Science, pages 514–532. Springer, 2001.

[11] [But13] V. Buterin. Ethereum whitepaper, 2013. https://ethereum.org/en/ whitepaper/. [CDH+21] J. Camenisch, M. Drijvers, T. Hanke, Y.-A. Pignolet, V. Shoup, and D. Williams. Internet Computer Consensus. Cryptology ePrint Archive, Report 2021/632, 2021. https://ia.cr/2021/632.

[12] [CDS94] R. Cramer, I. Damg˚ard, and B. Schoenmakers. Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols. In Advances in Cryptology - CRYPTO ’94, 14th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21-25, 1994, Proceedings, volume 839 of Lecture Notes in Computer Science, pages 174–187. Springer, 1994.

[13] Adeyanju, C.: What crypto exchanges do to comply with KYC, AML and CFT regulations. https://cointelegraph.com/news/what-crypto-exchanges-do-to-comply-with-kyc-aml-and-cft-regulations.

[14] Alexander C, Dakos M (2020) A critical investigation of cryptocurrency data and analysis. Quantitative Finance 20(2):173–188.

[15] Ardia D, Bluteau K, Rüede M (2019) Regime changes in bitcoin garch volatility dynamics. Finance Res Lett 29:266–271

[16] Barnwal A, Bharti H, Ali A, Singh V (2019) Stacking with neural network for cryptocurrency investment. arXiv preprint arXiv:1902.07855

[17] WIKIPEDIA: Cryptanalysis, Cryptography, Crypto Wars, Cryptocurrency.

[18] An Analysis of Cryptocurrency, Bitcoin, and the Future - Peter D. DeVries Professor of MIS University of Houston.

[19] Allen, D.W.E., Berh, C., and Novak, M. (2018). Blockchain: An entangled political economy approach. J. L. (1975) How to do things with words, 2nd edn. Oxford University Press.

[20] Non-interactive distributed key generation and key resharing. Dfinity Foundation.

[21]https://internetcomputer.org/docs/current/developer-docs/getting-started/cycles/cycles-faucet.