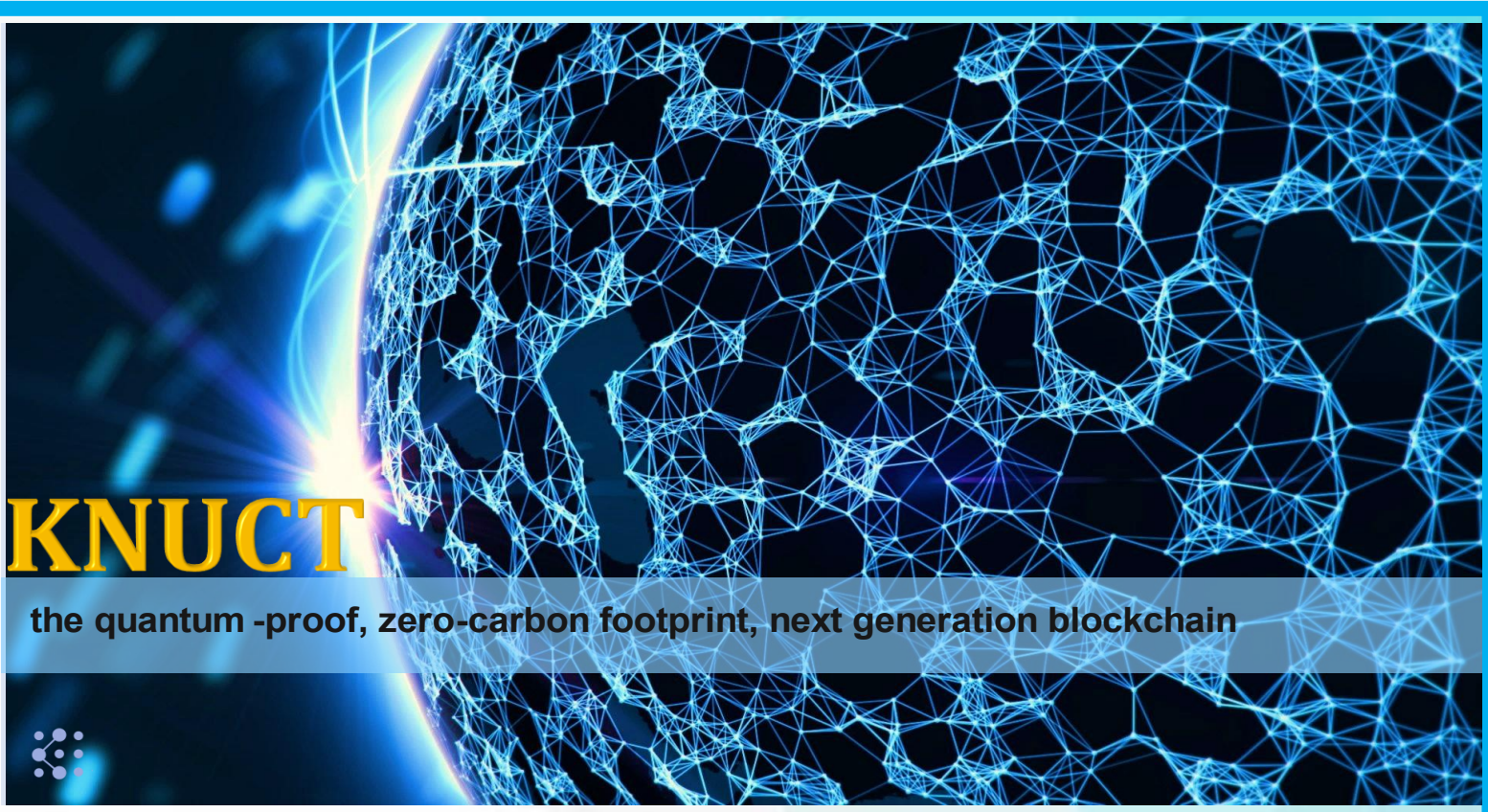
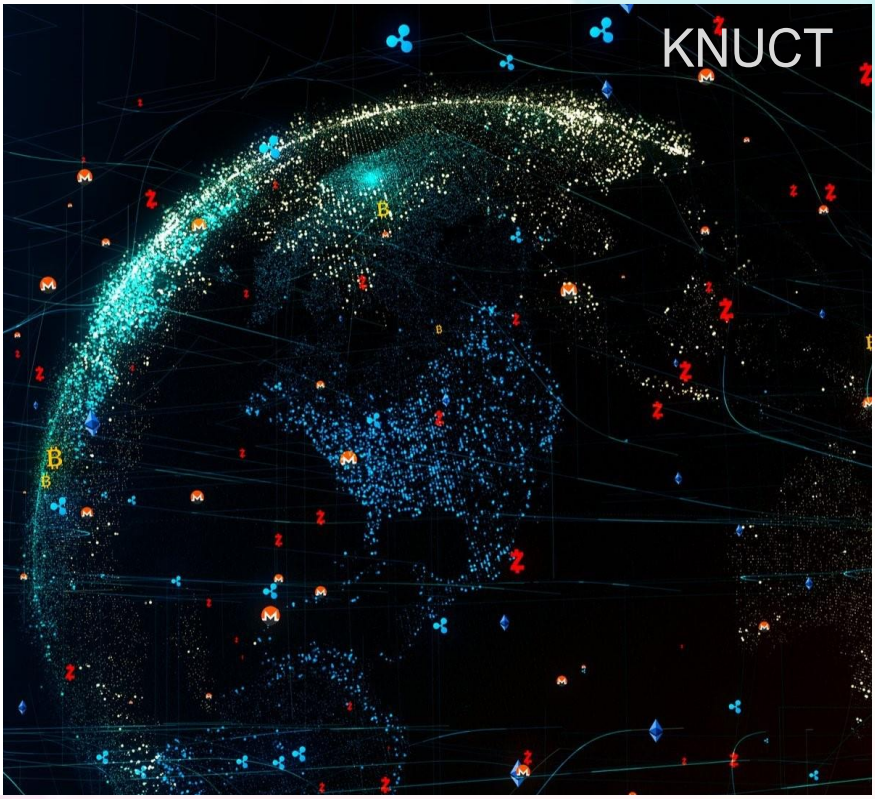


KNUCT BLOCKCHAIN

Quantum Immune



Our Mission

Build scalable, secure, and efficient global solutions by unleashing the power of blockchain to minimize transactional costs for everyone.

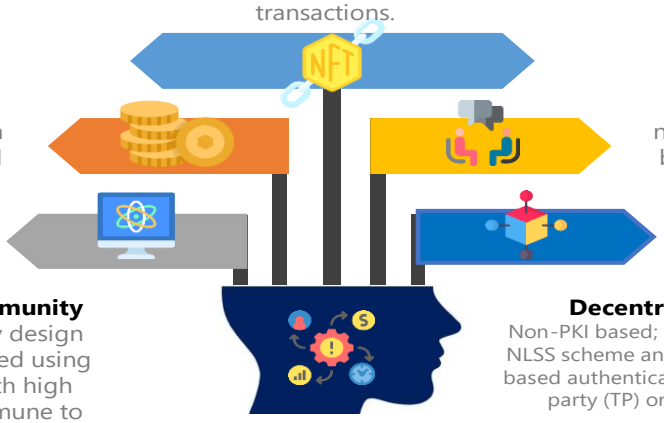
Note: According to the Global Blockchain Market Report 2021, the Market Size is Projected to Grow from $4.9 Billion in 2021 to $67.4 Billion by 2026, at a CAGR of 68.4%

Dr S Venkataraman, Director
svraman@crraoaimscs.res.in
director@crraoaimscs.res.in
C.R.Rao Advanced Institute of Mathematics, Statistics and Computer Science (AIMSCS), University of Hyderabad Campus, Hyderabad

Our Features

Tokenchain
Tokenchains collectively constitute and preserve the global state of the network. Nodes need to maintain tokenchains (including data & proofs) only for related transactions.

Tokenization
Unique patented (DIEHARD Test verified) pre-mined bootstrap tokens using Latin squares - limited supply and pseudo-token induction prevention.



Proof-of-Publish Consensus
All nodes consent to be validators/miners. Quality of network, system requirements & balance-of-proof credits decide eligibility. Consensus data is distributed (to sender, buyer, validators) using NLSS.

Post Quantum Immunity
Privacy is rooted by design and all data is secured using patented NLSS with high crack resistance immune to even Quantum attacks.

Decentralized Identity (DID)
Non-PKI based; Secure identity using patented NLSS scheme and challenge response scheme - based authentication. Requires no Trusted Third party (TP) or Certificate Authority (CA).

KNUCT

Our Unique Selling Points

Ultra-light weight nodes 01
Needs very low computing power and storage

02 **Quick Realization of Tokenchains**
High throughput (tps) and no delays due to unrelated transactions

04 **Complete ownership**
Wallet-to-wallet transfer of crypto and NFT tokens

Near-zero carbon footprint 03
Eco-friendly proof-of-publish consensus

KNUCT

Our Product Accomplishments So Far

Proof-of-Publish Consensus Security Testing

Alpha Testing of KNUCT Token Transfer

Blockchain Explorer

Alpha Testing of NFT Transfer

Web Wallet 2.0 and Desktop Wallet for Mac, Windows & Linux

Our Current Work in Progress

Knuct for Android/ IOS

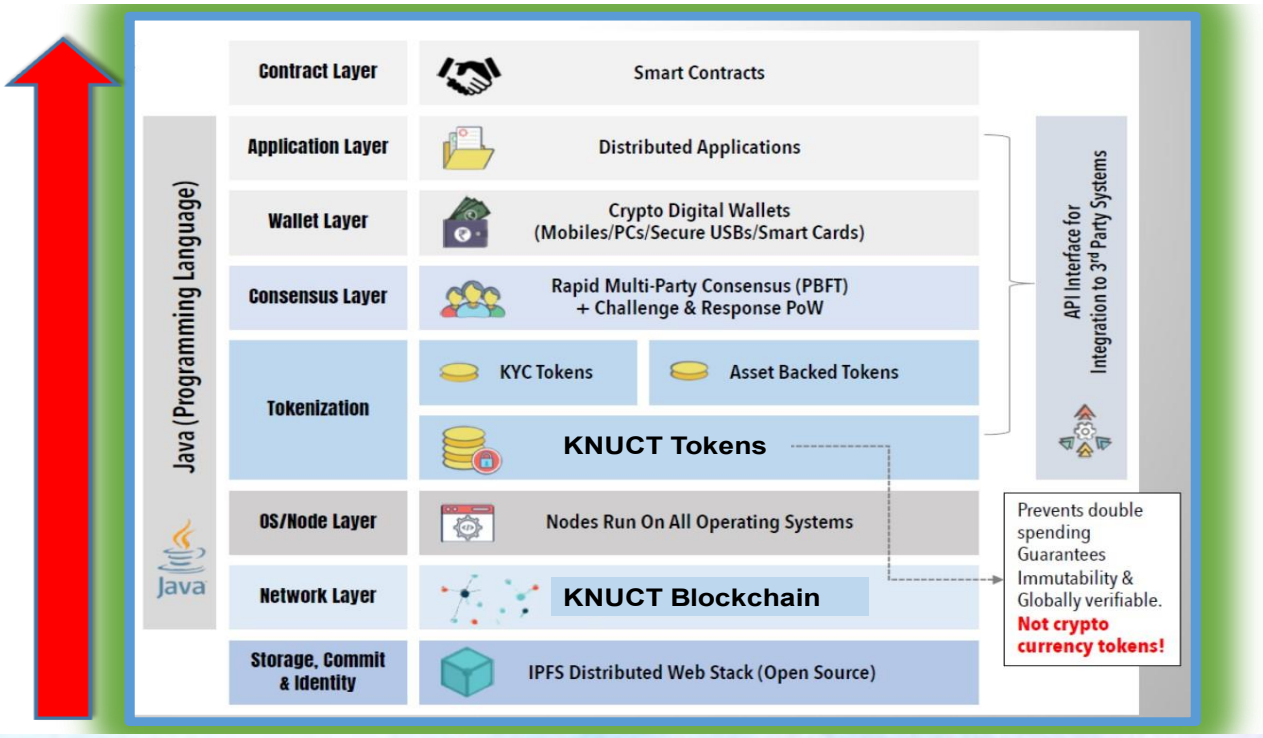
Knuct for IoT devices
(Testing)

ICO

Deploy on TCP/IP stack of Ethernet Cards

Live Dapp development

Smart Contract Development



Our Technology Stack

Application Layer
Decentralised Applications Smart Contracts

Wallet Layer
Crypto Digital Wallets (Mobiles, PCs, secure USB, Smart Card)

Consensus Layer
Rapid Multi-Party Computation based PBFT Consensus

Tokens Layer
Utility, Asset Tokens

Network Layer
Knuct Tokenchain

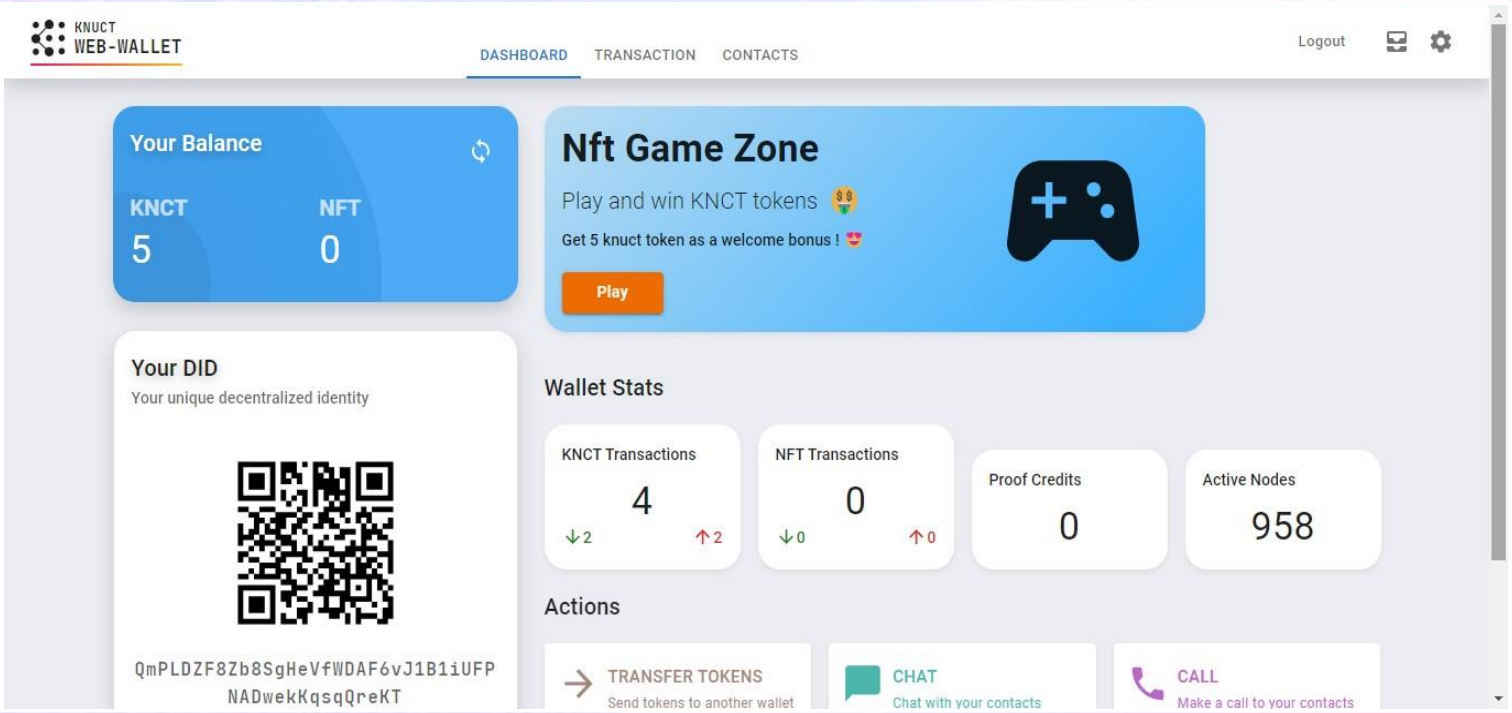
Storage Layer
IPFS Distributed Web Stack

Knuct blockchain is built in Java

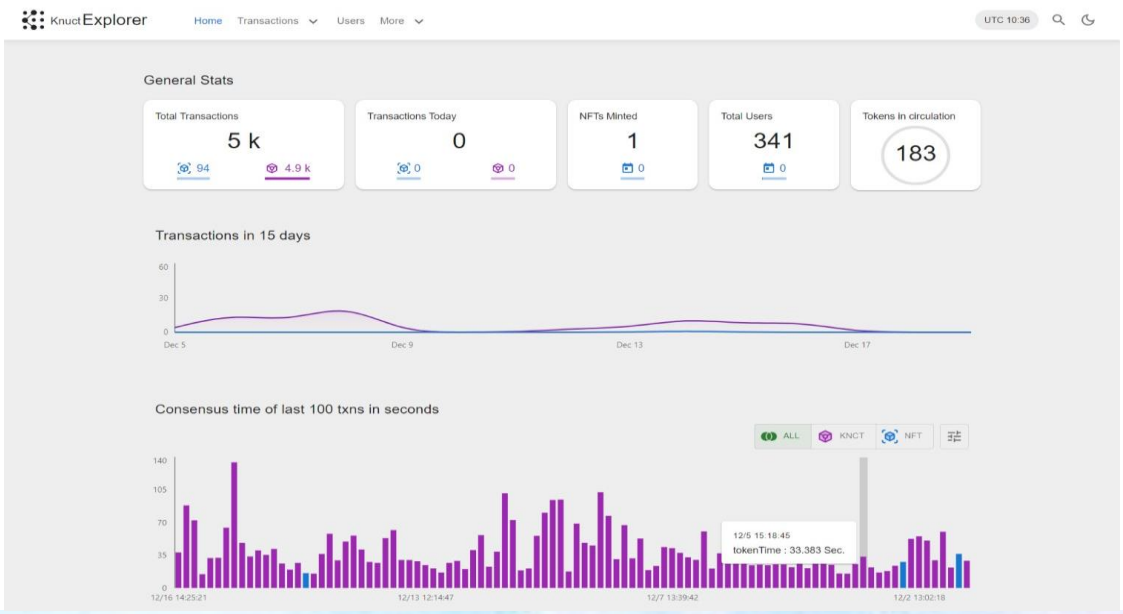
All storage functions integrated with IPFS storage

Tokenchains are introduced to offer immutability and global verification

Tokenchains are not the same as crypto tokens on a public blockchain.



Explorer Interface



Product Roadmap

- Knuct 3.0
- Additional Patent Processing
- Global Token Exchange & Payment Platform
- Global Live Main net
- Global Live Test net
- Post-quantum cryptographic research

PROJECTS

Multi-Party Threshold Cryptography MPTC

Overview

The multi-party paradigm of threshold cryptography enables a secure distribution of trust in the operation of cryptographic primitives. This can apply, for example, to the operations of key generation, signing, encryption and decryption.

This project focuses on **threshold schemes for cryptographic primitives**: using a "secret sharing" mechanism, the secret key is split across multiple "parties"; if some (up to a threshold *f* out of *n*) of these parties are corrupted, the key secrecy remains uncompromised; the secret-sharing remains even during the cryptographic operation that depends on the key. This approach can be used to distribute trust across various operators, and is also useful to avoid various single-points of failure in the implementation.

The multi-party threshold cryptography project will consider devising guidelines and recommendations pertinent to threshold schemes that are interchangeable (in the sense of NISTIR 8214A, Section 2.4) with ECDSA

PROJECT LINKS
Overview
News & Updates
Events
Publications
Presentations
ADDITIONAL PAGES
Email List (MPTC Forum)

Secret Sharing Schema…as one of the NIST based PQC ..methods

10.1109/ACCESS.2020.2968985, IEEE Access
IEEE Access
T. M. Fernández-Caramés, P. Fraga-Lamas: Towards Post-quantum Blockchain

that they are currently some of the most promising candidates for implementing schemes for post-quantum blockchains. In fact, the comparisons performed in this article have shown that lattice-based algorithms Three Bears and SABER are really fast, even when executed on low-power microprocessors for laptops. In addition, a scheme like Round5 KEM IoT seems appropriate for being executed in most current blockchain node hardware and in many applications that do not require very high security. Furthermore, lattice-based digital signature cryptosystems have already been suggested and tested in different practical blockchain implementations [170], [173], [177] and, according to the comparisons shown in this article, certain optimized versions of DILITHIUM and q A are among the fastest ones.

– Multivariate-based public-k need to be improved to inc and to decrease key size. noted that some multivari gorithms optimized for the (i.e., LUOV, MQDSS and faster than most of the com cryptosystems.
– Hybrid schemes like the ones tested by gle (CECPQ1 and CECPQ2) seem to be the n step prior to the actual implementation of pure post-quantum blockchains, but they require to make use developments [234].
– Identity-Base Encryption (IBE). It enables a sender and a receiver to communicate without exchanging public or private keys. For such a purpose, a trusted third-party is used as a middle-man between the sender and the receiver to generate private keys, which are sent to the receiver upon request. The scheme has been also generalized as Identity-based Broadcast Encryption (IBBE), which is able to manage multiple receivers instead of only one. IBE and IBBE are interesting for closed groups of users like private blockchains [235] and there are already implementations [236] (even for embedded systems [237]), but their need for a trusted third-party seems to be in conflict with the concept of public blockchain, whose existence is precisely justified by the lack of trust.
– Secret sharing. It consists in dividing a piece of sensitive information into multiple parts that are distributed among diverse participants and which can be reconstructed by using a minimum number of parts [238]. For instance, in [8] it is introduced a private-key distribution method to help recover lost private keys that is based in secret sharing and in network protocols that guarantee the security of secret share transmission. Another example can be found in [239], where the authors use secret sharing to distribute transaction data securely among peers in a blockchain.