Volume 01 | Issue 03| December 2025

CyberPeace

CYBERPEACE MAGAZINE

CRYPTOCURRENCY & BLOCKCHAIN

SECURITY, LEGAL & POLICY DIMENSIONS

CYBERPEACE MAGAZINE

OUR SUPPORTERS

SHAH & ANCHOR SM

CyberPeace
CENTER OF EXCELLENCE

Army Institute of Technology, Pune
Onward to Glory

PARTNERS

Autobot Infosec

SysTools®
Simplifying Technology

Cyber 4N6 Consultants

OUR TEAM

OUR FOUNDERS

Maj. Vineet Kumar

Founder and Global
President CyberPeace

OUR MENTORS

Shri SN Pradhan

IPS (Retd), Global CEO,
CyberPeace
Former DG, Narcotics Control
Bureau

Lt Gen (Dr.) Rajesh Pant (retd)

Global Advisor CyberPeace,
PVSM, AVSM, VSM
Former National CyberSecurity
Coordinator

TECHNICAL COMMITTEE

Mr. MAKP Singh,

Chief Technical &
Training Officer
CyberPeace

Dr. Nilakshi Jain,

HoD, Shah &Anchor
Kutchhi Engineering
College, Mumbai

EDITOR IN CHIEF

Maj. Vineet Kumar

Founder and
Global President
CyberPeace

COORDINATOR

Ms. Ayndri

Research Analyst,
Policy & Advocacy,
CyberPeace

DESIGN AND DEVELOPMENT

Mr. Ajeet Kumar
Concept & Design

Senior graphic designer- Media &
Design, CyberPeace Foundation

HEAD OUTREACH

Lt Cdr Seema Gupta
(Retd.)

Head, Outreach Program &
Admin , CyberPeace

Editor's Note

Maj Vineet Kumar

Founder & Editor-in-Chief

Cryptocurrency and blockchain technologies have moved far beyond their early perception as niche innovations. Today, they sit at the crossroads of finance, technology, governance, and global policy debates.As adoption accelerates, from retail investors to institutional players and even sovereign experiments, the conversation is no longer about whether these technologies matter, but how they should be governed, secured, and integrated into existing systems.

At the heart of blockchain's appeal lies its promise: decentralization, transparency, and immutability. Yet, these same features introduce complex security challenges. While blockchain networks themselves are often resilient by design, the broader ecosystem of wallets, exchanges, smart contracts, and user interfaces remains vulnerable. High-profile hacks, phishing schemes, and smart contract exploits have exposed a critical truth: trust in the system depends not only on cryptography, but on human behavior, code quality, and institutional safeguards. Security, therefore, must evolve from being purely technical to becoming systemic, encompassing education, standards, and accountability.

Parallel to security concerns is the rapidly evolving legal landscape. Cryptocurrencies disrupt traditional definitions of money, assets, and ownership, leaving regulators grappling with classification dilemmas. Are they currencies, commodities, securities, or something entirely new? Different jurisdictions have responded with varying degrees of openness and caution, resulting in a fragmented regulatory environment. This inconsistency creates uncertainty for innovators and investors alike, while also opening avenues for regulatory arbitrage. A coherent legal framework is no longer optional; it is essential for stability and long-term growth.

Policy considerations add yet another layer of complexity. Governments must balance innovation with risk mitigation, encouraging technological advancement without compromising financial stability, consumer protection, or national security. Issues such as anti-money laundering (AML), combating the financing of terrorism (CFT), data privacy, and taxation are central to this balancing act. Meanwhile, the rise of central bank digital currencies (CBDCs) signals that states are not merely observers but active participants shaping the future of digital finance.

What emerges is a landscape defined by tension and opportunity. Cryptocurrency and blockchain technologies challenge existing power structures while offering tools for greater financial inclusion and efficiency. However, without robust security practices, clear legal definitions, and forward-looking policy frameworks, their transformative potential risks being undermined.

This moment calls for collaboration—between technologists, regulators, policymakers, and civil society. The path forward is not about constraining innovation, but about guiding it responsibly. As the lines between code and law continue to blur, the question is no longer just how blockchain works, but how it should work within the societies it aims to serve.

Maj Vineet Kumar

Founder & Editor-in-Chief

TABLE OF CONTENTS

TABLE OF CONTENTS

CYBERPEACE
MAGAZINE

INTRODUCTION TO BLOCKCHAIN:

Applications, Risks and the Hype around Crypto

• SIMRAN DHAKAR, MPDNLU

What is Blockchain?

Blockchain is a specialised technology that records and verifies transactions securely across a series of networks or computers for multiple independent parties. It functions in a manner similar to a shared digital notebook or an online ledger which cannot be tampered with, is[1] transparent and immutable. Blockchain operates on a decentralised distributed database that includes information which is spread across various different regions or locations. This database is jointly maintained and shared over a user-to-user log without a single authority or an intermediary having any control over it.

Origin, Background and Growing Popularity

The origin of blockchain technology can be traced back to 1991, when American researchers Stuart Haber and W. Scott Stornetta developed a cryptographically secure chain of blocks to prevent the tampering of digital documents. In 2008, an individual with the pseudonym, Satoshi Nakamoto, introduced this novice idea in his research paper 'Bitcoin: A Peer-to-Peer Electronic Cash System'. After about a year, Bitcoin was launched on the blockchain system. Soon developers and programmers realised that blockchain has a lot of potential.

Consequently, this resulted in the launch of blockchain applications such as Ethereum, which was launched in 2015 by Vitalik Buterin, a Canadian computer programmer. Ethereum broadened the domain of blockchain by introducing smart contracts and self-executing applications.

How does Blockchain work – Understanding the process

- **Transaction facilitation-** A new encrypted tran saction is initiated by a user in the blockchain network. After the initiation, the transaction is broadcasted to all nodes participating in the network.

- **Verifying the transaction-** All the nodes then verify and validate the transaction with the help of consensus algorithms or mechanisms. Thes e algorithms run on an agreed protocol which have been previously utilised by older chains. They check if the user has proof of permission and if the data shared is credible.

- **Creation of Blocks-** Once verified, the nodes compile the transactions into blocks. Each block in this chain holds a set of transactions and has a timestamp.

- **Adding the Blocks to the Chain-** Once a block is full, it is connected to the previous block using special codes called cryptographic hashes. This process links the blocks together to form a continuous chain.

- **Uniform Accessibility and Trustworthy Record -s-** The updated blockchain, that is accessible to all nodes, ensures that they all hold the same version of the ledger at all times. This decentralisation process ensures keeping the transaction records permanent, secure and unchangeable.

How is Blockchain applied and utilised?

Blockchain has gained considerable momentum in recent years owing its popularity to an ever growin -g demand for secure and transparent transactions in the digital landscape. Various industries and sect -ors have implemented this nuanced technology that has helped reduce administrative burdens, fra -udulent transactions, operational costs and proce -ssing time. The most eminent contribution of block chain has been in the financial sector. Bitcoin and Ethereum are cryptocurrencies that use blockchain to carry out transactions without the need to rely on intermediaries such as banks. Even banks and businesses are able to swiftly and securely transfer funds through the use of blockchain, eliminating the need for middlemen and lowering the instances of fraud.

In the healthcare sector, blockchain processes safeguard patient records and make it easy for physicians to exchange information and patient data while maintaining patient privacy. Blockchain is also applied in the supply chain sector to trace items or goods from a particular manufacturer to a retailer. This ensures authenticity and lowers the possibility of counterfeit goods. For real estate companies, automation of contracts and protection of property data is facilitated through blockchain, which simplifies the mechanism of property related transactions among buyers and sellers. Even Gove rnments are now considering the prospects of Blockchain to help improve the transparency and reliability of public data and voting systems. The education sector is also witnessing blockchain as a resourceful and beneficial tool for verifying acade mic credentials and maintaining student records securely. Online authentication through blockchain is also being simplified by reducing identity thefts and impersonations. Through digital IDs, individual s can confirm and verify their identity independent of centralised authorities. Blockchain is rapidly tran sforming several industries by enhancing daily ope -rations with increased security, speed, and tran sparency.

Risks posed by Blockchain

Although Blockchain is mostly acknowledged for its advantages and for the transparency it offers, yet there are still risks involved in this process.

- The biggest concern is the susceptibility to cyb -er-attacks. Cyber-attacks can render entire sys tems inoperable when a sole entity takes contr ol over a network, leading to misrepresentation or manipulation of data.

- Privacy concerns may also arise, especially in large public blockchains. Participants on a netw -ork have access to all transactions, which may include sensitive information. Access to this sensitive information can be misused since it is not regulated or controlled by any central authority.

- Smart contracts, although automated, can also pose a serious threat as they may fail to opera -te efficiently due to poor or faulty coding. Sinc -e they are immutable, any illegal or incorrect information can affect the transaction process which may even lead to financial losses.

- Uncertainty in the regulatory and legal frame work for blockchain processes is also a cause for concern since laws based on cryptocurren cies are still developing and evolving in many countries.

- Operational and environmental risks can also arise when the consensus mechanisms of the Blockchain systems consume very high energy to carry out their massive and large scale verification processes.

Why the hype around Crypto?

Crypto, also known as cryptocurrency, is a digitali sed form of currency that functions on a decent ralised network wherein transactions are secured through data encryption. The world is witnessing a frenzy surrounding cryptocurrency, which seems to be the result of a combination of factors such as rapid technological advancement and the exciting prospect of decentralised global finance. For those looking for financial independence, or those who have privacy concerns, cryptocurrency assets like Bitcoin and Ethereum make it possible to transmit money quickly and safely across borders without depending on conventional banks and governmen -ts. The transparent and tamper proof nature of the blockchain technology promotes ideas for more open and equitable market places, making crypto an exciting concept. To an extent, social media is also responsible for amplifying this excitement by disseminating information and trends to users. Influencers frequently endorse cryptocurrencies or investment techniques which attract novice investors. Cryptocurrency is turning out to be a result of a confluence of technology, speculative investments and social trends. However, the risks of crypto, which stem from its unregulated and highly volatile nature, also need to be made clear to the public.

References

- Cambridge Bitcoin Electricity Consumption Ind -ex (CBECI), University of Cambridge.

- Catalini, C., & Gans, J. (2016). Some Simple Eco nomics of the Blockchain. MIT Sloan Research Paper.

- Crosby, M., Nachiappan, Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016).

- Blockchain Technology: Beyond Bitcoin. UCS Berkeley Sutardja Center.

- Luu, L., et al. (2016). “Making Smart Contracts Smarter.” ACM Conference on Computer and Communications Security. Nakamoto, S. (2008). Bitcoin: A Peer-to- Peer Electronic Cash Sys tems

- Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018) . Blockchain Technology Overview (NISTIR 820 2). National Institute of Standards and Techno logy.

Hithika Kohli,

Law and Education Expert

INDIA'S NATIONAL BLOCKCHAIN INFRASTRUCTURE:

Architecture, Use-Cases and Deployment

- ANUPMA PRAKASH SRIVASTAVA,

Visiting Faculty, Institute of Cost and Works Accountants of India

Introduction

Satoshi Nakamoto, presumed pseudonymous for a person or group of people, has been cred -ited to conceptualise the first decentralised blockc hain way back in 2008. Soon, the technology was refined by Bitcoin cryptocurrency and Walmart for logistics requirements. Blockchain is a distributed ledger which uses the structure of blocks to record transactions and information. Each block is made up of three components. First, data or information. Secondly, every block has a fingerprint which is cal -led a hash which is unique to that block. Thirdly, each block stores the hash or fingerprint of the pre -vious block as well which is nothing but a chain of interlinked transactions. These are the unique feat -ures which make any document, transaction recor ded on blockchain tamper proof and immutable. Not far to be left behind, the technology was soon adopted by the Government of India to bring about transparency, remove red tapism and corruption and make the system efficient for swift delivery of its flagship programs and relieve the citizens and its Government functionaries with unnecessary checks and errors. The tamper resistant nature of blockchain made it imperative for the Government of India to adopt this technology.

Blockchain Policy Framework in India

Ministry of Electronics and Information Technology (MeitY) initiated

the development of National blockchain fr -amework (NBF) to provide application of blockcha -in technology that can be applied to various sect ors in India. Vishvasva Blockchain Stack is the most significant development under the NBF. Blockchain technology particularly becomes very important for India owing to India's vast demography, number of public disbursal schemes, huge transactions due to vast population and various stake holders involved in every transaction. The National Informatics Centr e has established CoE for rapid adoption of block chain technology. It is designed to promote, co-ordinate, establish interoperable blockchain syste ms all over India.

Vishvasya Blockchain Stack

Vishvasya Blockchain Stack was developed indige nously as a permissioned blockchain application to provide transparent, immutable and decentralised financial services and enhance government efficie ncy. It was launched on 4 th September 2024. Its key features are:

- Permissioned Blockchain layer- Vishvasya bloc -kchain only allows verified or authorised parti cipants to validate the transactions.
- NIC Data centers- The blockchain is deployed at NIC data centers namely, Pune, Bhubaneshw -ar and Hyderabad.
- Application Programming Interfaces- the stack provides open API's for authentication.
- BaaS- Blockchain as a service allows governm ent to use blockchain services to build their ap plications, smart contracts while CoE manages to keep the infrastructure operational

Praamaanik

Praamaanik makes use of blockchain technology to verify the source of mobile applications. Mobile phones are the most targeted device for cyber-attacks. When a user scans the downloaded application, praamanik validates the details with data available on blockchain records. It enhances mobile security and transparency which is part of the cyber hygiene initiative.

Types of Blockchain

- Public blockchain- A nonrestrictive permissionl -ess decentralized ledger system.
- Private Blockchain- Private blockchain is a per missioned and restrictive system which is desig ned to operate only in closed networks.
- Consortium Blockchain -It's a semi decentralize -d system where more than one organization acts as nodes.
- Hybrid Blockchain - Hybrid, as the name sugge -sts, is a combination of Public and Private bloc kchain. Selected sections of data are allowed for the public to access whereas a large part of the data is kept confidential.

Use of Blockchain by Government of India

Certificate Chain-

The unabated use of fake documents to avail gove -rnment benefits, incessant paperwork for docume nt verification resulting in delayed service, prompte d NIC to adopt Blockchain technology. Academic (Blockchain) Documents (ABCD) provides a platfor - m to store and access tamperproof marksheets by students, educational institutions, Government and employers.

Document chain-

A blockchain based system, certificate chain system, has been developed to record, store,

access and retrieve documents digitally. Various stakeholders like Revenue, registrar of Birth and death, sub registrar offices etc. have been benefitted by adopting certificate chain system. The Certificate chain is an instrument to verify the documents issued by the government.

Judiciary Chain

Judicial proceedings require a lot of documents and case proceeding details to form their judgement. Additionally, deposits maintained on the blockchain system helps in deposit transactions without tampering and automatic refund of the same. FIR, traffic challans, chargesheets and fine amounts can be maintained on blockchain. Bail orders issued by the court are maintained on blockchain which ensures swift retrieval of bail order documents by police. Judiciary can trail the transaction details and ownership details in case of land disputes by maintaining data on tamperproof blockchain systems. Important certificates such as marksheets, birth and death certificate, caste certificate , disability certificate that are maintained on blockchains can be accessed and utilised by the judiciary while drafting their judgement. Forensic reports are also stored on blockchain to secure evidence to avoid loss or tampering.

Drug logistics chain

The Karnataka state drugs logistics and warehousing society chain uses Blockchain technology which benefits patients, hospitals and government. The Aushada system of Karnataka (medicines of Karnataka) uses blockchain to record transactions right from the purchase, distribution and collection of drugs by the government. The system is transparent and immutable which prevents spurious medicines from reaching the end users. Karnataka state medical supplies corporation limited together with 2924 hospitals and 32 hospitals along with quality testing laboratories have benefitted immensely by implementing blockchain technology.

Property Chain

Property chain uses blockchain system and is developed by Centre of excellence (CoE) by National Informatics center (NIC). Land record system maintains Record of rights (RoR) documents which is used by farmers to avail subsidy for seeds and fertilisers as well as to secure loans from the government.

Similarly, purchase and sale of land, mortgage on land, inheritance transactions, court orders passed related to property and other property transactions of various stakeholders are recorded on property chain blockchain which is tamper proof. Decentralized recording of transactions makes them secure. Over 48,000 documents are of the document chain as on 21st October 2025. Public Distribution system, Land registration, Blood bank remote Voting and GST chain are other pilot projects that have been taken by CoE of National Informatic Centre.

Conclusion

Blockchain is a breakthrough technology which is most suitable for the Indian landscape where documents are required by multiple departments and public welfare schemes have to be implemented over a large area and population. The system will not only benefit the real users but also provide them services in an efficient and swift way. Blockchain automatically weeds out chances of corruption and fake documents. The way forward is development and application of this technology in many other areas which will pave the way for a sustainable growth and development model in India.

References

- https://blockchain.gov.in/Documents/Concept_Note_Generic_CertChain_Ver1.1.pdf
- https://blockchain.gov.in/Documents/JudiciaryChain.pdf
- https://dlc.kar.nic.in/AboutDLC.aspx
- https://blockchain.gov.in/Documents/Concept_Note_on_Property_Chain_Ver%201.1.pdf
- https://blockchain.gov.in/Home/BlockChain?blockchain=type
- https://blockchain.gov.in/Documents/Concept_Note_GST_Chain.pdf
- https://blockchain.gov.in/Home/CaseStudy?CaseStudy=BloodBank
- https://blockchain.gov.in/Home/CaseStudy?CaseStudy=PDS
- https://blockchain.gov.in/Home/CaseStudy?CaseStudy=remotevotingchain
- https://blockchain.gov.in/Home/CaseStudy?CaseStudy=LandRegistration

BLOCKCHAIN APPLICATIONS IN EDUCATION

Healthcare and Supply Chain Security in India

Rahul Kumar, Advocate , Punjab and Haryana High Court

Introduction

Initiatives such as Digital India and Make in India have put India on the global front and reshaped India's digital transformation. As India moves towards a knowledge and data driven economy, it has become pertinent to ensure transparency, trust and efficiency across all sectors. Blockchain technology is a decentralised, tamper-proof and transparent system. Beyond cryptocurrencies, blockchain is now slowly finding real world applicability in various sectors of India such as education, healthcare and supply chain security. This may lead to strengthened data integrity and accountability across sectors.

Blockchain in Education: Building Trust in Academic Records

India is witnessing a significant change towards digital credentialing in education. However, the problem of fake degrees, unverifiable mark sheets and slow verification processes continue to undermine and damage the system. Blockchain offers a promising and revolutionary remedy to address these issues.

Digital Credential Verification

Blockchain systems allow institutions to issue digital certificates that cannot be changed and are automatically verifiable. This eliminates risk of fraud and manual delay. Universities in India are now exploring blockchain systems for their academic record keeping, ensuring that their student credentials can be authenticated, stored and verified indefinitely.

Universities around the world have adopted similar systems. For example, the Massachusetts Institute of Technology (MIT) issues digital diplomas on blockchain through its Blockcerts system, which is an internationally recognized standard and secures important digital records. This system offers a dependable way to verify credentials, confirming blockchain's ability in establishing trust and transparency in the process of academic credentialing.

Academic Bank of Credits (ABC)

The Academic Bank of Credits (ABC) is an online repository where students deposit their academic credits, awarded to them by the institutions that are officially recognized under the National Education Policy (NEP) 2020. The Academic Bank of Credits is a digitally verified repository that uses blockchain technology which ensures that a ledger of credits is tamper-proof, transparent, easily transferable between universities and not subject to being altered or manipulated. The SWAYAM program (Study Webs of Active Learning for Young Aspiring Minds) was introduced by the Government of India in 2017 to make high quality education available to all. Credits earned through the SWAYAM platform are automatically recognized and endorsed by the ABC for academic purposes. This advancement has not only facilitated fluid academic mobility and lifelong education, but has also ensured reliability of credit transfers within India's education framework.

Transparent Scholarships and Grants

Smart contracts are digital agreements that run on blockchain platforms and can be automatically enforced.

Smart contracts automate scholarship payments by releasing funds when the specific conditions such as attendance, performance or completion of a course are met. This enables payments to be made quickly and transparently. Additionally, blockchain based academic records enable institutions and funding organizations to identify deserving candidates accurately, which further reduces institutional bias and ensures a fair selection process.

Blockchain in Healthcare: Ensuring Data Security and Transparency

India's healthcare sector also faces challenges such as duplicative records, patient data privacy concerns, counterfeit medications and a lack of coordination among stakeholders. Blockchain technology can contribute to a secure patient centered healthcare system.

Safe Medical Data Management and Health Record

Blockchain allows for safe storage of health records in blockchain encrypted and tamper-proof blocks. All medical records such as lab reports, prescriptions, hospital visits, etc., are allotted a unique timestamp when they are registered within the blockchain. This technology creates a reliable and auditable timeline of a patient's health history. It maintains data integrity, reduces the risk of unauthorized changes and ensures that patients and healthcare providers can access medical records at any time without risk.

Interoperability with ABDM

The Ayushman Bharat Digital Mission (ABDM) is designed to build a smooth and a unified digital health ecosystem where patients and healthcare providers can securely exchange data. Integrating blockchain into this framework can strengthen the system by providing an audit based, transparent, tamper proof trail of consent, data sharing and access among all healthcare stakeholders.

Fraud Reduction on Health Insurance

Blockchain also simplifies, facilitates and creates transparency for insurance claims by using shared ledgers and unique Ids linked to verified medical outcomes. This allows insurers to quickly review medical records across different healthcare providers and health departments. This helps in confirming treatments, preventing fraud or duplicate claims and also speeds up the claim process.

Blockchain in Supply Chain Security: Strengthening Trust and Traceability

Supply chains form the backbone of India's economy, especially in sectors like agriculture, pharmaceuticals, and manufacturing. However, persistent issues such as counterfeiting, lack of transparency, and logistical delays undermine efficiency and trust.

Food and Agricultural Traceability

The states of Telangana and Karnataka have significant agricultural bases. They are now exploring how blockchain technology can modernize agricultural marketing and supply chain management. To increase the trust between producers and consumers in the marketplace, the two states are considering how blockchain can be used to improve transparency related to the origin, movement and prices of the products.

By establishing a digital connection between farmers and buyers, blockchain can circumvent intermediaries yielding farmers a greater share of profits. The traceability characteristics of blockchain support can lead to improved quality control and better food safety standards.

As the second largest state in India, Maharashtra has taken up a multi-sectoral strategy to the integration of blockchain technology. The state government is employing blockchain technology solutions in agriculture and supply chains and in other sectors as well, such as vehicle registration, land records and document management. In agriculture, blockchain is being implemented to provide more effective tracking of movement of produce, improved marketing techniques and transparency in farmer-buyer transactions. In the long run, this approach will lead to improved efficiency, accountability and trust in the economy and administrative systems in Maharashtra.

Pharmaceutical and Medical Devices

Serialization systems play a critical role in the pharmaceutical industry by protecting the integrity of the supply chain. By attaching unique digital identifiers to medicines and medical devices, each level of activity in the pharmaceutical supply chain can be tracked and verified, including manufacturing, distribution, and retail. While regulators such as the United States Food and Drug Administration and the European Medicines Agency have not made blockchain mandatory, its potential as a tamper-proof decentralized digital ledger to enable traceability and data integrity, is beginning to garner consideration as a potential strategy in improving drug tracing. Many experts believe that when blockchain is combined with serialization, it can help authenticate drugs, prevent counterfeit or expired drugs from reaching hospitals and pharmacies and ultimately increase patient safety. For a country like India, one of the largest producers of pharmaceutical products in the world, implementing a blockchain based traceability system can boost global confidence in the quality of its healthcare.

Conclusion

Blockchain is still a developing technology, however its capabilities for revolutionizing various key sectors of India have been demonstrated by incorporating trust, transparency and traceability into various digital systems. Blockchain technology has improved academic integrity in the educational sector, increased care coordination in the health sector and upgraded product viability and operational efficiency within supply chains.

References

- Pradipta Mukherjee. (2024). India curbs academic fraud, reshapes the education sector with blockchain. https://coingeek.com/india-curbs-academic-fraud-reshapes-education-sector-with-blockchain/#
- Elizabeth Durant. (2017). Digital Diploma debuts at MIT. https://news.mit.edu/2017/mit-debuts-secure-digital-diploma-using-bitcoin-blockchain-technology-1017
- Anurag Garg, Shyamli Varshney, Avinash K, Pooja Kansra. (2024). Role of blockchain technology in boosting Ayushman Bharat scheme implementation in India. https://pmc.ncbi.nlm.nih.gov/articles/PMC11463249/
- (2024). Blockchain Blossoms: Top Indian states taking root in agritech. https://agritimes.co.in/agri-technology/blockchain-blossoms-top-indian-states-taking-root-in-agritech/
- (2025). Pharmaceutical Serialization Software and Regulatory Compliance. https://intuitionlabs.ai/articles/pharmaceutical-serialization-software-regulations

NEURAL NETWORK-ENHANCED BLOCKCHAIN AUTHENTICATION

Behavioural Biometrics Integration for DeFi Security

Kritika, Independent Researcher(Cybersecurity), India

Introduction

The industry of decentralised finance (DeFi) facing security vulnerabilities has a history of its own, with authentication failures being the most severe threat in the context of modern blockchain . According to recent security analysis, in 2025, the security threat of DeFi has not only changed fundamentally (technical exploits to human-oriented threats), but also 56.5% of all security breaches will fall under phishing and social engineering threats. Authentication vulnerabilities have taken catastrophic proportions on the financial implications. The lucrative analysis of DeFi security incidents highlights that the smart contract vulnerabilities and authentication failures resulted in billions of losses across major protocols. The conventional multi-factor authentication (MFA) systems are not effective within a decentralised setting where,in the absence of central recovery systems, users have a direct control over their private keys. This authentication crisis requires new solutions that would integrate the inflexibility of blockchain technology with the complexity of neural network-based behavioural biometrics to develop strong and user-friendly security frameworks.

Neural Network Authentication Methods

Neural network-based behavioural biometrics is a paradigm shift with respect to the traditional methods of static authentication to dynamic, pattern-based systems of user verification that take advantage of distinct human behavioural patterns. The keystroke dynamics is the logical base of

The current implementation of the keystroke dynamics uses advanced neural network models to examine temporal dynamics such as dwell, flight, typing pressure change and consistency of rhythm. The latest surveys on biometric cryptosystems show that the choice of the neural network architecture has a considerable effect on the accuracy of the keystroke-based biometric identification, with Convolutional Neural Networks (CNNs) performing exceptionally good with regard to the recognition of patterns within the sequence of typed words, whereas Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks are the best at recognising pattern changes across the typing pattern sequence. K-DSA methodologies have yielded authentication accuracy scores higher than 95 percent in controlled settings. It uses data fusion techniques which use keystroke dynamics and deep learning. Neural networks are also used to develop secure and resistant to tampering authentication schemes in advanced biometric cryptosystems that can distinguish between genuine users and attackers with low computational load that can be incorporated in blockchain. Multi-modal behavioural fusion methods increase security strength through a combination of the dynamics of keystroke, mouse movements, scrolling, as well as error correction habits.

Blockchain Integration Architecture

Combining neural network-based behavioural bio metrics with a blockchain-based system requires advanced building structures balancing the concepts of security, privacy, and decentralisati on. Decentralised biometric verification is based on smart contract-based authentication systems and performs authentication logic on-chain independen tly without relying on trusted third parties or centralised servers. Present-day applications take into account issues of privacy, scalability, and interoperability, adding biometric authentication and decentralised identity to build secure online definitions of personal identities.

More modern blockchain designs employ convolutional neural network (CNN) biometric cryptosystems in order to provide stronger security of blockchain private key encryption. Cloud-based storage systems that are decentralised adopt distributed file systems to distribute encrypted biometric templates and apply consensus-based validation of cloud-based data to eliminate single points of failure and ensure data integrity.
Homomorphic encryption, secure multi-party computation, and differential privacy are privacy preserving mechanisms that guarantee the safety of sensitive biometric data through distributed network nodes to meet General Data Protection Regulation and other regulatory compliance demands. Interoperability is achieved through cross-chain authentication protocols, which can be used between blockchain platforms, and they share standardised APIs and protocol bridges to ensure consistent authentication across blockchain platforms.

Current Industry Implementations

Biometric authentication using blockchain is on the move, with platforms implementing neural network-based systems to be used in the real world in DeFi. These systems have been able to attain a higher authentication accuracy rate of over 97 percent with the false positive and false negative rate of less than 0.1 percent and less than 2 percent respectively. It has been demonstrated that these systems are viable when executing the DeFi transactions with high frequency and sub-second authentication time is appropriate when handling high frequency transactions. They also exhibit extreme breach resistance, and in controlled test environments they have had zero successful authentication bypass. The growing influx of investment is triggered by the integration of AI and blockchain technologies into the realm of improved security of financial services. These advanced platforms are also able to implement complex attack containment features such as real time behavioural anomaly detection giving early warning mechanisms that effectively supplement the traditional security monitoring strategies.

Future Directions & Policy Implications

The integration of neural network authentication and blockchain technology requires global standardisation to ensure interoperability, security, and regulatory compliance. Regulatory evolution emphasises robust authentication for digital currency implementations and compliance requirements for biometric data processing in financial services. By 2030, single-token digital identities will be established that will transform digital identity management across sectors. Technological advancements include AI and machine learning for behavioural pattern recognition, quantum-resistant biometric authentication, and next-generation biometric modalities.

Security & Privacy Considerations

The implementation of neural network-based authentication mechanisms based on blockchain demands a critical analysis of the data protection systems, regulatory compliance standards, and novel threat vectors. The best security practices in recent times involve hardware security modules, multi-factor authentication, and access control. The concept of data protection compliance is a complicated issue, and the aspects of GDPR indicate the necessity to implement privacy-by-design principles in the biometric data processing.

Threat modelling is used to deal with complex attacks. Organisations that have a comprehensive biometric security framework have lower rates of attack success than their conventional counterparts. Privacy-by- design systems are based on local processing models, federated learning models, and data collection minimalism. Response protocols to incidents include biometric template revocation procedures, system recovery procedures and security patching procedures.

References

- https://secureframe.com/blog/data-breach-statistics
- https://techblog.cymetrics.io/en/posts/alice/2024_defi_hack/
- Sharma, S., Saini, A., & Chaudhury, S. (2023). A survey on biometric cryptosystems and their applications. Computers & Security, 134, 103458.
- Albakri, A., & Mokbel, C. (2019). Convolutional neural network biometric cryptosystem for the protection of the blockchain's private key. Procedia Computer Science, 160, 235-240.
- Sharma, S., & Dwivedi, R. (2024). A survey on blockchain deployment for biometric systems. IET blockchain, 4(2), 124-151.
- https://www.halborn.com/reports/top-100-defi-hacks-2025 Sarier, N. D. (2025). Best of two worlds: Efficient, usable and auditable biometric ABC on the blockchain. Computer Standards & Interfaces, 92, 103916.
- https://www.biometricupdate.com/202111/integration-of-blockchain-and-biometrics-to-redefine-digital-identity-by-2030-report
- Shukla, H., & Bhushan, B. (2023, November). Empowering Biometrics Authentication System Using Decentralized Blockchain Based Applications. In 2023 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS) (pp. 1177-1182). IEEE.

BLOCKCHAIN IN THE DIGITAL WELFARE STATE

PROMISE, PRACTICE, AND PITFALLS

• SIMRAN DHAKAR, MPDNLU

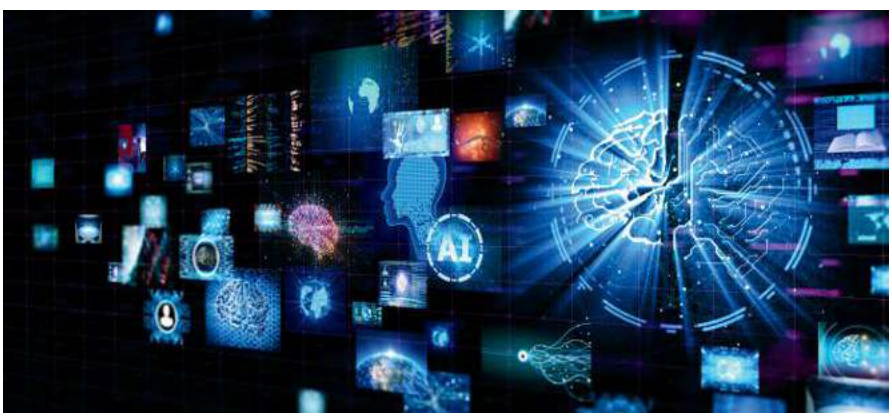
INTRODUCTION

In the twenty-first century, technology has become an integral component of governance given the challenges faced in the implementation of various welfare schemes in the Indian context particularly in the administration of welfare programs and social security schemes. Governments around the globe are increasingly adopting a "digital welfare state," where benefits such as pensions, healthcare subsidies, and cash transfers are sent electronically.

While there is such digitisation, age-old issues like fraud, data tampering, delayed payment of funds, and lack of transparency have been constantly plaguing welfare dispensation. In this regard, Blockchain technology is a probable game-changer .

Blockchain, a decentralised digital record where transactions are imputed in an immutable and open way, holds the potential to infuse efficiency, accountability, and confidence into the administration of welfare. It can potentially overcome structural inefficiencies by rendering transactions which are transparent, by upgrading verification procedures and eliminating redundant middlemen.

This article explores the potential of blockchain to reimagine the digital welfare state by examining its value mechanisms, empirical findings from pilot schemes, salient issues and controversies, and policy recommendations for ethical adoption.



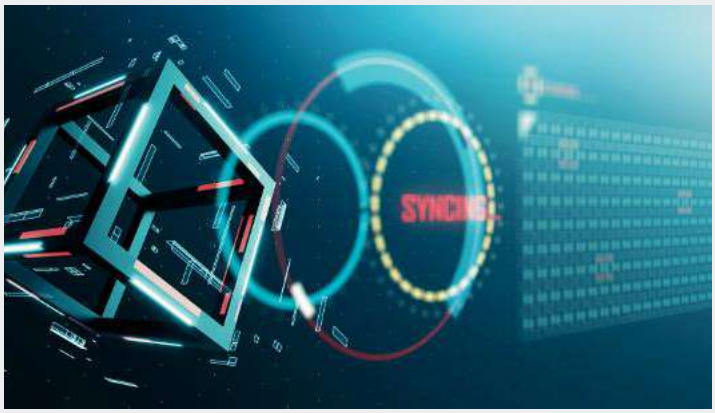
VALUE MECHANISMS FOR WELFARE

Blockchain contributes to the digital welfare system several key value mechanisms. For one, it creates an unalterable common ledger where beneficiary information and transactions are held securely. Every transaction in the ledger is stamped with a timestamp and cannot be reversed, meaning it is nearly impossible to alter beneficiary records or payment history. This significantly reduces corruption and duplication of welfare schemes.

Secondly, blockchain enables programmable transactions in the form of smart contracts that automatically release funds under certain conditions, say, a child going to school or getting vaccinated. This minimises the bureaucratic delay and maximises efficiency in conditional cash transfer programs.

BLOCKCHAIN SIMPLIFIES COORDINATION AMONG MULTIPLE STAKEHOLDERS

Thirdly, decentralised identity systems using blockchain allow users to own their own personal information and securely share it with agencies simultaneously without getting exposed to exploitation. This is privacy-reserved and interoperable between government departments.



Lastly, blockchain simplifies coordination among multiple stakeholders, ministries, banks, and service providers, by having a single source of validated facts, thus minimising reconciliation errors and administrative slowdowns. Combined with the above mechanisms, welfare distribution can also be made cost-effective, more inclusive and transparent.

EVIDENCE FROM PILOTS AND EVALUATIONS

Potential for blockchain for welfare has been tested through numerous pilots globally. Humanitarian organisations such as the UN World Food Programme and UNHCR have used blockchain technology to deliver cash assistance to refugees, notably through projects such as Building Blocks and Stellar. These projects demonstrated quicker-than-conventional transactions, reduced administrative charges, and greater transparency in the delivery of assistance. Similarly, UNICEF's blockchain-based cash transfer pilot project in Nepal, Project Rahat, improved traceability and accountability but also brought out implementation challenges such as low digital literacy and availability of networks.

Within the government setting, certain countries such as Estonia, India and the United Arab Emirates have tested blockchain in the areas of improved record-keeping, identity management, and disbursal of welfare.

BLOCKCHAIN

For Welfare

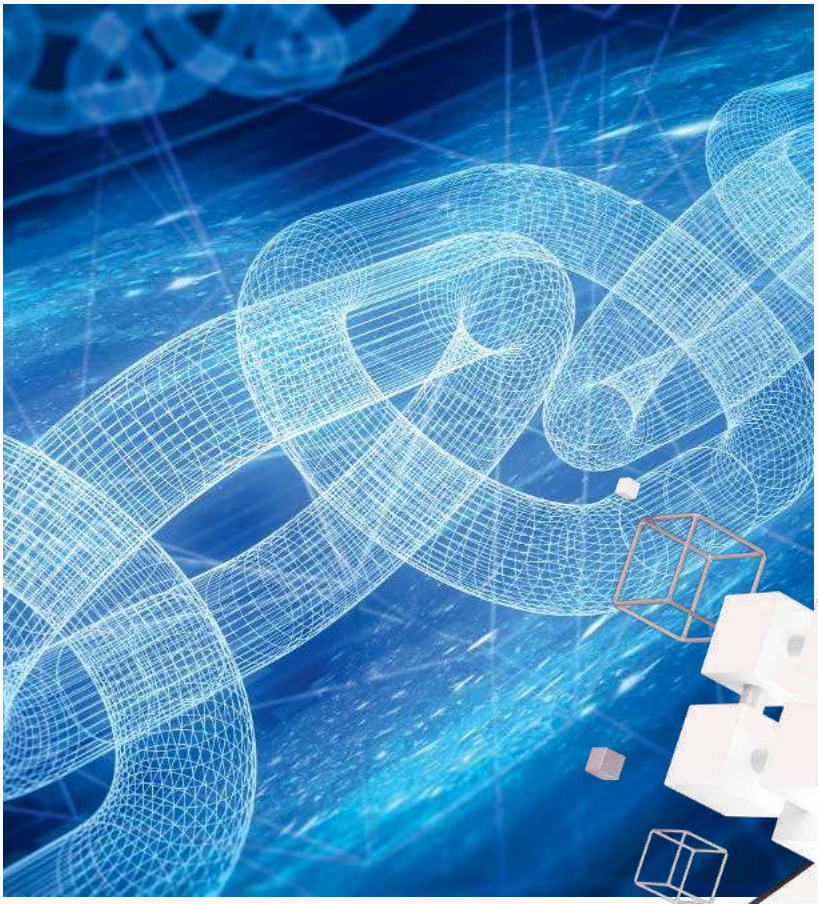
India's attempts to promote blockchain use through central bank digital currency experiments and asset tokenisation are a sign of growing trust in its role to simplify welfare payments and expand financial inclusion. However, examination of such pilots has shown that though blockchain increases transparency and reduces delays, its utility tends to depend on complementary systems like efficient digital payment channels, beneficiary education, and efficient grievance redressal systems.

Major Concerns and Criticisms

Notwithstanding its potential, blockchain technology in welfare programs is not without its critics. The biggest concern is data privacy. Since blockchain records are immutable, placing sensitive beneficiary data directly on the ledger creates serious privacy concerns. Any mishap or mismanagement may result in an irreversible breach of personal information. For this reason, experts suggest storing blockchain merely to keep encrypted references or hashed identifiers instead of unencrypted personal data.

Digital exclusion is another major challenge. A majority of beneficiaries, especially in the global south, lack access to the internet or the digital skills required to leverage blockchain technologies, a prospect that promises to amplify the digitally empowered and the excluded.

Scalability and affordability are equally significant challenges, public blockchains would naturally suffer from slow rates of transactions and high energy needs, while private or permissioned blockchains stand the risk of repeating centralisation and undermining the values of decentralisation. In addition, legal uncertainty around the use of smart contracts, their enforceability, and their compatibility with existing administrative legislations complicates their adoption.



Finally, as witnessed in some humanitarian pilots, overemphasising technology has the potential to deflect responsibility away from human decision-making and diminish local participation, thereby making provision of welfare more rigid and less humane.

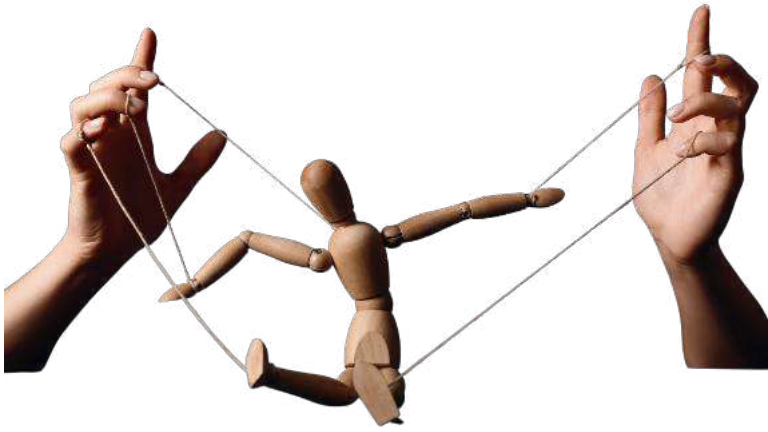
DESIGN PRINCIPLES FOR POLICYMAKERS

To effectively unlock blockchain's potential, policymakers must adopt its use carefully and explicitly. First, they should have a problem-first, then-technology strategy; blockchain would be utilised only if it clearly supersedes existing solutions to problems such as leakages, latency, or transparency holes.

Second, data protection will need to take center stage. Personal data should remain off-chain, with only encrypted or minimal amounts of data held on the blockchain to comply with privacy legislation.

Third, adopting hybrid approaches that combine blockchain for verification with traditional databases for storage can be efficient and flexible.

Fourth, blockchain initiatives need to be integrated with the dominant digital payment platforms and grievance redressal mechanisms to prevent exclusion or confusion.



Fifth, pilot initiatives must be backed by open evaluation frameworks that track not only technical success but social effects like user experience, accessibility, and gender equity.

Finally, the legal and institutional frameworks must be updated to recognise blockchain records and smart contracts as formal evidence, wherein technology supplements, and not replaces, due process and accountability in welfare governance.

6. CONCLUSION

Blockchains are double-edged swords which at one hand provide opportunity and on the other hand these opportunities come with intrinsic challenges for the digital welfare state. It has potential to ramp up transparency, accountability, and automation which can revolutionise the way welfare benefits are delivered and monitored.When it is used responsibly, the government can get an upper hand by this, to build trust with citizen, circumvent corruption, and public funds can be managed efficiently. However, the technology is no silver bullet. Blockchain technology is not sufficient to ensure equity in welfare systems, but it requires robust governance structures, privacy protection, and participatory policy design; blockchain-based welfare programs can perpetuate or exacerbate existing inequalities. The success of these initiatives relies less on the development of the technology itself and more on the guiding principles of the institutions that are implementing it. The government should ensure that ethics, equality and empowerment of citizens are the principles around which blockchain application is applied for public good only then it will ensure fair , transparent and quick distribution of public welfare schemes.

REFERENCES

- World Bank, Blockchain and Emerging Digital Technologies for Enhancing Post-COVID Government Operations (2021), https://documents.worldbank.org/.
- Primavera De Filippi & Aaron Wright, Blockchain and the Law: The Rule of Code (Harvard Univ. Press 2018).
- Michael Pisa & Matt Juden, Blockchain and Economic Development: Hype vs. Reality, Ctr. for Global Dev. Working Paper No. 455 (2017).
- UN World Food Programme, Building Blocks: Blockchain for Zero Hunger (2020), https://innovation.wfp.org/project/building-blocks.
- UNICEF Innovation Fund, Project Rahat: Blockchain-Based Cash Transfers in Nepal (2021), https://www.unicef.org/innovation/project-rahat.
- Estonian Information System Authority, e-Estonia: Blockchain and e-Governance Framework (2020), https://e-estonia.com/.
- UNHCR, Blockchain for Refugees: Enhancing Cash-Based Interventions (2019), https://www.unhcr.org/innovation/blockchain/.

The Weaponisation of Blockchain:

Crypto, Sanctions

EVASION AND THE GEOPOLITICS OF BLOCKCHAIN

BARSHAN KARMAKAR , PHD SCHOLAR, AMITY INSTITUTE OF DEFENCE AND STRATEGIC STUDIES

Introduction

The 21st century has witnessed a shift in the tools of power from conventional and traditional traditional methods to those that are intangible and that cannot be seen, such as the economic domains. Today, tanks or missiles are not the only means that alone determine global military or security dominance, as money-flows and payment systems now serve as equally powerful weapons.

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) is a network which links more than 11,000 banks across 200 countries. This network has become one of the sharpest instruments in western coercive diplomacy. The United States and its allies have often exercised financial exclusion by removing banks or even entire countries from SWIFT - as a non-military action to punish geopolitical adversaries. When Iran was cut-off in 2012 and Russia in 2022, they lost access to major global financial arteries, causing serious economic damage without the use of any military weapons.

The story does not end here completely, as the West perfects financial weaponry, whereby its adversaries are now discovering new forms of defence mechanisms through blockchain, cryptocurrency and sovereign digital currencies. These innovations which were originally celebrated as tools of decentralisation and inclusion are now being repurposed as instruments of resistance against the Western financial hegemony. The weaponisation of blockchain has become the new reality that marks the dawn of a digital arms race in the realm of finance.

FROM CRYPTO-HYPE TO CRYPTO-WARFARE:

A TRANSFORMATION

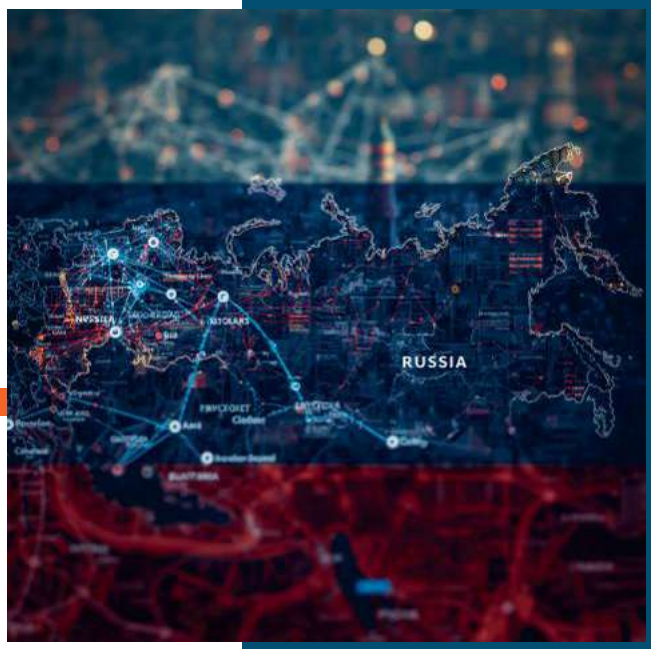
In the 2010s, Bitcoin and other cryptocurrencies were dismissed by central bankers as volatile fads and speculative bubbles. But the shift in geopolitical realities have transformed their true significance and this has led to SWIFT becoming a political weapon and blockchain emerging as a political refuge.

The key features of blockchain such as decentralisation, pseudonymity, and borderless transactions, are one of the most important points that are precisely making it attractive to sanctioned or isolated states. Cryptocurrencies are also enabling financial flows beyond the jurisdiction of the US, offering access to liquidity without the need for Western banks or intermediaries

Russia, Iran, and North Korea are some of the countries where this technology provides not only an economic advantage, but also a geopolitical lifeline. Their use of cryptocurrencies varies from mining to trading, and in some cases, outright theft. But the goal of all the states is the same, which is to ensure their survival outside a global system dominated by the US dollar.

RUSSIA: A CASE FROM SWIFT EXILE TO DIGITAL RESILIENCE

Russia's invasion of Ukraine in the year 2022 triggered one of the harshest financial sanctions regimes in modern history. Major Russian banks were cut off from accessing the SWIFT system and over $300 billion of their reserves were frozen which caused the Ruble to plunge. However, Moscow adapted to this change at a faster rate than expected. Within months, Russia developed a parallel financial infrastructure to help withstand the challenges posed by the West.



SPFS AND CIPS INTEGRATION

Russia also expanded its domestic payment messaging network, the System for Transfer of Financial Messages (SPFS), and linked it with China's Cross-Border Interbank Payment Systems (CIPS), which is a Yuan-based equivalent of the SWIFT payment systems.

DE-DOLLARISATION ATTEMPTS

While doing trade with China, India and the Middle Eastern countries, Russia shifted towards the Ruble, Yuan, Rupee and Dirham, thereby reducing its dependence on dollar settlements.

ADOPTION OF CRYPTO

Stablecoins like United States Dollar Tether (USDT) and United States Dollar Coin (USDC) began appearing in Russia's oil and commodities trade, which allowed for high-value transfers to take place beyond the scrutiny of the West.

3.4 CARVING OUT STRATEGIC INNOVATIONS

Russia and Iran have even discussed creating a gold-backed Stablecoin to facilitate their energy trade, signalling a move towards blockchain-based monetary diplomacy.

In this case, Russia's focus has mainly been on a key geopolitical reality, that when economic coercion reaches its peak, innovation becomes the real quest for survival. By blending blockchain, commodities and an alternative system of payment, Russia has laid the groundwork for a multipolar financial ecosystem that boldly opposes Western dominance over the global financial ecosystem.

IRAN: A CASE FOR MINING CRYPTO FOR SURVIVAL FROM SANCTIONS

Very few countries have illustrated financial resilience through the use of technology as vividly as has been done by Iran. After the expulsions from SWIFT in 2012 and 2018, Iran was effectively locked out of the international banking systems. However, instead of collapsing, Tehran re-engineered and reshaped its economy around cryptocurrency mining and blockchain-based trade.

By leveraging its abundant and cheap electricity, Iran also legalised large-scale Bitcoin mining operations. Miners were required to sell their output directly to the Central Bank of the Islamic Republic of Iran by creating a state-controlled crypto liquidity pool. This allowed the regime to utilise Bitcoin for import payments and cross-border transactions without requiring the traditional banking systems. In 2022, Iran also conducted its first $10 million import order by using cryptocurrency. This event marked a milestone in its adaptation to digital finance. With the help of crypto, Iran effectively replaced SWIFT's global messaging architecture with a decentralised network of miners, wallets and exchanges.

NORTH KOREA: A CASE ON THE NEGATIVE SIDES OF DECENTRALISATION

Russia and Iran have used trade against sanctions, however North Korea has utilised it as an outright weapon.

It is a source of income for them and not an edge against sanctions. This also includes a record-breaking Axie Infinity hack of 2022 of over $600 million and numerous other attacks on decentralised finance (DeFi) platforms.

Thus, unlike Iran's regulated mining or Russia's stablecoin settlements, North Korea has represented an example of the weaponisation of crypto as a means of cyber-warfare, in the form of an asymmetric power projection wherein codes have been replaced by missiles.

China: The case of digital Yuan and the geopolitics of CBDCs

CHINA:

THE WESTERN

attention has been focused on the role of evasion of sanctions over cryptocurrencies, China has quietly been leading a different revolution, one that could reshape the architecture of the international finance system.

The Digital Yuan (e-CNY) has been developed by the People's Bank of China. It is the world's most advanced Central Bank Digital Currency (CBDC). As compared to other decentralised cryptocurrencies, the e-CNY program is traceable and is state-controlled. This program has been designed in such a manner that China can utilise it to monitor, regulate and program real-time monetary flows.

China's aim is strategic in nature, whereby it wants to create a sovereign digital payment infrastructure that would be independent from the Western networks. Beijing is laying the foundation for a post-SWIFT and post-dollar ecosystem by promoting the e-CNY across the Belt and Road Initiative (BRI) partner nations and integrating it with the CIPS systems.

If the digital Yuan is widely adopted, it could allow for cross-border trade settlements that bypass the oversight of the US and may even challenge the dominance of the US Dollar in the Asian energy markets. This move may strengthen China's geopolitical leverage over the developing world. In short, it seems that China is not just in the process of evading sanctions, but it might be writing the global rules of finance.

THE AMERICAN COUNTERMEASURES: REGULATIONS, FATF AND THE DIGITAL DOLLAR DEBATE

The United States seems to be at a crossroads with those who are faced with digital insurgency. The very system that once guaranteed its global financial supremacy, the dollar-based order, now stands under threat from both decentralised crypto networks and state-led CBDCs. The Financial Crimes Enforcement Network (FinCEN) and the Office of Foreign Assets Control (OFAC) have broadened their sanctions to cover cryptocurrency wallets, exchanges, and mixing services like Tornado Cash. In order to prevent money laundering, the Financial Action Task Force (FATF) had implemented a travel regulation that required an exchange of sender and recipient information.

DIGITAL DOLLAR

Washington's long-term response is the Digital Dollar, which is a US CBDC aimed at preserving the influence of dollars in an increasingly digital economy. However, there are concerns over surveillance and civil liberties that have been delayed as part of their progress. So, without any such currencies, the US also risks ceding the technological initiative to China, just as it had done in the case of 5G and AI infrastructures.

An attempt towards balancing innovation and security: India's Strategic Ambiguity

India plays a complex role in this developing scenario. As a member of the BRICS bloc (a group of emerging economies that include Brazil, Russia, India, China, South Africa, Egypt, Ethiopia, Iran and Indonesia) and as a country emerging in the digital revolution, India is aware of the potential and the risks associated with blockchain technology. In an effort to modernise digital payments while retaining state authority, the Reserve Bank of India (RBI) started the e-Rupee pilot in 2022. In addition to challenging the dollar, the e-Rupee is intended to improve financial inclusion, efficiency, and transparency inside India's borders.

The Reserve Bank of India (RBI) started the e-Rupee pilot in 2022

However, India remains cautious and aware about the unregulated crypto markets that may include national security risks, money laundering and terror financing concerns. Unlike the top-down approach of China or the digital authoritarianism of the market-led innovation of the US, India's approach shows strategic ambiguity. India seems to be keeping a strong leverage over the benefits of blockchain but at the same time it is keeping tight reins on its risks

As the global digital currencies continue to evolve, India has the potential to emerge as a balancing power and can aim to attain digital financial sovereignty by bridging regulatory frameworks with the help of the BRICS-led push.

The rise of parallel

SYSTEMS LIKE SPFS, CIPS, AND THE BRICS DIGITAL BLOC

One of the most profound and unintended outcomes of Western sanctions has been the fragmentation of the global financial system. In this case, measures have been designed to isolate nations like Russia and Iran. Therefore, an alternative and parallel financial architecture is now coming up that can challenge the long-standing dominance of Western-led mechanisms like the SWIFT network.

Taking the example of the three major banking systems across the world, let us see some of the key examples, such as:

- The Russian-developed System for Transfer of Financial Messages (SPFS) continues to serve as a domestic variant of SWIFT, which allows the Russian banks to conduct transactions with the help of a secure and independent framework. This system also ensures that even when they are excluded from the SWIFT network, the Russian financial institutions can maintain critical communication links for domestic and limited international transfers.
- In the meantime, China has also extended its Cross-Border Interbank Payment System (CIPS), which is known for enabling international transactions based on the Yuan. Beijing's strategic goals aim at internationalising the Yuan and offer a substitute settlement method that will lessen reliance on dollar-based trade.
- In addition to this change, the BRICS countries are moving forward with plans for a BRICS Pay platform and a possible BRICS digital currency. To facilitate cross-border settlements without the use of intermediaries like the US dollar, this initiative also aims to establish a common digital payment infrastructure that links member economies. By reducing exposure to Western sanctions and currency fluctuations, such platforms, when operationalised in the future, have the potential to transform trade between BRICS members and their partners.

The emergence of blockchain-based settlement systems, such as the Russia-Iran gold-backed Stablecoin for energy trade, alongside platforms like SPFS, CIPS, and BRICS, reflect a broader shift towards decentralisation, with a sanction-resistant financial network in the Global South.

Conclusion

A PICTURE OF THE FUTURE ECONOMIC WARFARE

The weaponisation of blockchain is not an anomaly, rather it is the logical evolution of a world where the economic domain, which deals with our regular financial transactions, has become a probable area of threat. The consequences relate to the scenario whenever the US or the EU attempt to weaponise or securitise their dollar system. This has provoked its adversaries to innovate and develop a different domain to counter it. Starting from Russia's Stablecoin Experiments to China's Digital Yuan Diplomacy, or Iran's mining to North Korea's cyber raids, the contours of global finance have been shifting towards decentralisation, diversification, and exerting their own digital sovereignty

This leaves a question for all policy makers, which is to no longer enforce sanctions, but rather govern a fragmented financial order where power gets measured not in reserves or interest rates, instead it is executed in control over digital ledgers and payment rails. However, the next geopolitical contest would not be fought over natural resources, territories or ideology, but over data, codes, and currencies, where blockchain is shaping up as the probable battlefield.

REFERENCES

- Advocate Anwar M Quereshi. (2025). The Weaponisation of Financial Systems: Swift Ban, Cryptocurrency Workarounds, and International Legal Perspectives. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5319012

- Oladipupo Abdul Malik Olalekan. (2025). Sanctions Evasion 2.0: Unpacking the Role of Cryptocurrency in North Korea and Iran's External Trade Relations. https://www.researchgate.net/publication/392312032_Sanctions_Evasion_20_Unpacking_the_Role_of_Cryptocurrency_in_North_Korea_and_Iran's_External_Trade_Relations

- Summer Wright. The Evolution Of Sanctions Evasion: How Cryptocurrency is the new game in evading sanction and how to stop it. https://jilet.org/wp-content/uploads/2025/01/3.1.1.pdf

- Godspower Oke Omokaro, Zipporah Simiyu Nafula, Nwankwo Evalistus Iloabuchi, Ogheneochuko Shadrack Efeni, Opelopejesu Israel Adeyanju, Oyedele Opeoluwa Janet, Omodot Udim Idiong. (2025). Energy sanctions in the global economy: Geopolitical disruptions, market fragmentation, innovation and green transition. https://www.sciencedirect.com/science/article/pii/S2096248725000268

- William Alan Reinsch, Andrea Leonard Palazzi. (2022). Cryptocurrencies and U.S. Sanctions Evasion: Implications for Russia. https://www.csis.org/analysis/cryptocurrencies-and-us-sanctions-evasion-implications-russia

- Chainalysis team. (2025). Iranians Flock to Crypto Amidst Geopolitical Tension; International Sanctions Actions Disrupt Russia's War Machine. https://www.chainalysis.com/blog/crypto-crime-sanctions-2025/

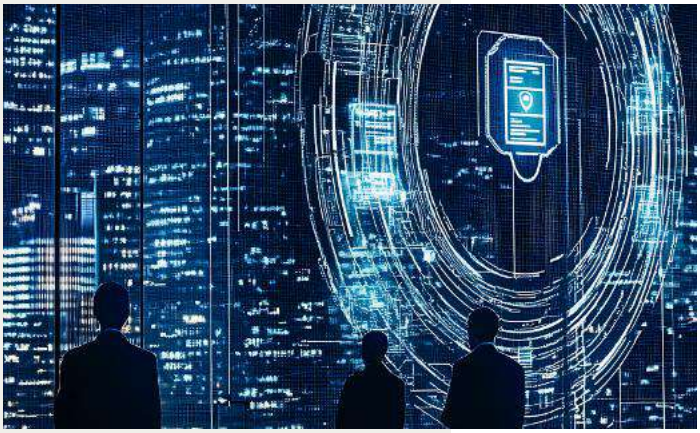
Digital Laundering on the Rise

Crypto Crime Investigations Challenges for India

PRIYA DUTT, STUDENT, CHANAKYA NATIONAL LAW UNIVERSITY

INTRODUCTION

Cryptocurrency in India has been undergoing a critical investigation crisis. Since 2015, the Enforcement Directorate (ED) has achieved only a 0.25% conviction rate. Although these cases differ in the types of fraud, from narcotics to corruption, the most rapidly advancing segment is cryptocurrency-related laundering and fraud. The regulatory framework of India, i.e., the current amendments in the Prevention of Money Laundering Act, 2002 (PMLA), is not sufficient to curb the rise in crypto crimes since it presents a systemic failure of investigations due to its lack of forensic infrastructure for new kinds of laundering, such as DeFi (Decentralised Finance) protocols, privacy coins, and chain bridges. This analysis demonstrates that India is a haven for cryptocurrency laundering, precisely because of the lack of effective enforcement capabilities.



CRISIS OVERVIEW

The Enforcement Directorate has filed 5,892 cases under PMLA between 2015 and 2025 and has convicted 15 individuals, with a 0.25% conviction rate, which suggests that deterrence may be ineffective. Comparatively, the U.S. and the European Union's (EU) financial crime conviction rates are relatively higher. In India, with a conviction probability of nearly zero, criminal deterrence falls, demonstrating a situation where laws exist only on paper, with troubled enforcement.

THE NEW THREAT LANDSCAPE

Privacy Coins

The privacy coins that the world transacted between 2023 and 2024 rose significantly. The Monero and zero-knowledge proofs of Zcash have a ring signature that renders the operations opaque; however, India has not imposed any ban or due diligence. Criminals use the regulated exchange deposits and convert them to privacy coins, which cannot be traced. India is not as outspoken as the EU (MiCA – Markets in Crypto-Assets) and Japan. This gives a gateway to the criminals in India, and the privacy coin outflow is not controlled effectively.

DEFI LAUNDERING BY UNREGULATED PROTOCOLS

DeFi platforms have no KYC (Know Your Customer) or ownership verification or reporting (supporting peer-to-peer transactions). The flash loans that have less forensic evidence are also supported by smart contracts. According to some sources, this laundering is projected to hit 2.3 billion by 2024-2025, an increase of 340 per cent, and 15-20 per cent of criminal crypto flows are currently through DeFi. India has no particular regulation or monitoring systems of DeFi, though the latter is not the subject of traditional regulation.

MULTI-BLOCKCHAIN LAUNDERING PATHWAYS CROSSCHAIN BRIDGES

It is possible to initiate cross-chain bridges between blockchains, i.e., laundering chains can be transferred between audited networks to privacy-oriented ones. The number of cross-chain bridges is predicted to reach almost 4.8 billion monthly by the year 2025 (subject to different market metrics and varying forecasts), with 15-20 per cent of such volumes linked to laundering. The ED and CBI (Central Bureau of Investigationn) can only follow cross-chain forensics; state police cannot trace multi-chain flows, creating a dead end in the investigation. India has lost its cross-chain protocols, and this absence of protocols in India becomes an increasingly dangerous blind spot as bridge technology becomes increasingly decentralised.

Institutional Reality-Investigative Inequality

Two-Tier Forensic System (Modern State in 2025)

There is a two-tier forensic gap in the 2025 investigational environment of India. At the central level, ED and CBI both have advanced solutions like Chainalysis and Elliptic. Transaction clustering, darknet markets mapping, and detailed monitoring fall under the jurisdiction of ED, and cross-chain analysis, ransomware tracing and the dissemination of intelligence across borders fall under the jurisdiction of CBI. However, such infrastructure is lacking at the state level.

The Training Disaster: No Skill Conveyor

There is no official training pipeline in 2025 in the Indian cryptocurrency investigation. NFSU (National Forensic Sciences University) teaches drone forensics and does not offer a substantial number of courses in cryptocurrency. In the Indian Police Academy, where officials are trained, there is no specialised cryptocurrency course. Very few universities in India offer a degree in cryptocurrency forensics, and no standard procedures are in place, which need to be developed to identify crypto laundering. The problem with the structure is the lack of training, and the increase in the number of crypto crimes. Yet the number of trained investigators remains low.

Emerging Responses of Regulatory Incompetence

A regulation that has not been realised

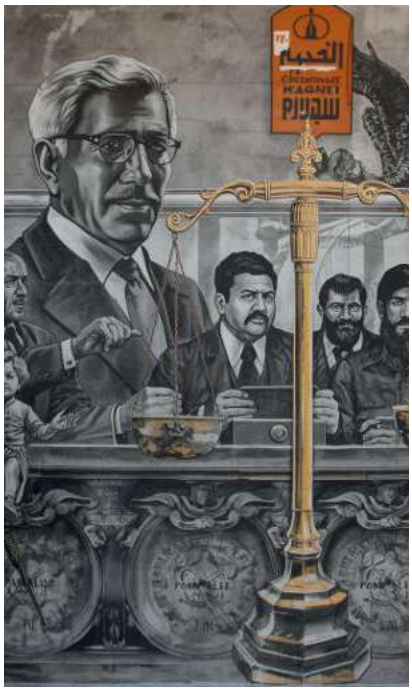
In March 2023, a new amendment to the PMLA added a specific regulation of VDA (Virtual Digital Asset), although the capacity to enforce laws has been lacking and has left an empty framework with laws in place but not operative. The amendment gives express authority to ED on money laundering and exchange-level KYC involving VDA, suspicious transaction reporting, and beneficial ownership verification. However, it does not provide funding to state police in the context of forensic infrastructures, standardised investigation procedures, cryptocurrency-related training, privacy coin auditing procedures, DeFi, or cross-chain activity. It also lacks lean arrangements of global collaboration. The additional indication of the enforcement being aspirational is - the notices dated September 2025 to 25 non-compliant offshore platforms operating in India and offering services to Indian users, not because the regulation does not apply, but because the capacity to enforce cannot keep up.

Global Comparison

The reactions of the global regulations are in contrast with the reactions of India, which are negligible. MiCA Regulation of the EU (2024) restricts privacy coins trading, implements traceability, stablecoin reserve, and DeFi custody issues. The US FinCEN (United States - Financial Crimes Enforcement Network) guidance (2023-2024) offers the procedures of tracking ransomware, enforces the Travel Rule and outlaws privacy coin mixing services. The AML (Anti-Money Laundering) framework 2024 (Singapore) provides no exchange of privacy coins except, beneficial ownership must be verified, DeFi custody is required, and regional investigation systems are coordinated. Relative to privacy coins, DeFi, and cross-chain bridges, the regulatory structure of India is still silent on older and newer threats, which may move forward unchallenged. It is a reactive control stance where India continues to grapple with the 2022-2023 risks because the vulnerabilities of 2024-2025 keep getting out of hand.

The India of Contemporary Criminals

The Cost-Benefit Analysis of Criminal Activities



Modern money laundering systems enter a jurisdiction that depends on the strength of their regulation, their capacity in forensics, the likelihood of conviction, the anticipated losses and the overall riskiness. The US and the EU have mature systems, developed forensic systems, and higher conviction rates. Although the 2023 revision of PMLA has been introduced, yet India has a fragmented forensic capacity and a conviction rate of 0.25 per cent, which incurs much less financial impact. This forms what is termed an ideal criminal operation target in which regulation provides the illusion of being in control, and investigative restrictions ensure that criminal operations have minimum legal exposure.

Current Witnesses to this Exploitation

Almost half of the cryptocurrency losses in India can be attributed to Southeast Asian scam rings, which target India because regulatory enforcement opportunities are minimal. The fact that 25 unregistered offshore platforms were still operating in September 2025 is an indication that such services operate with impunity since enforcing the same is difficult. Criminals realise that the anticipated punishment is nearly nothing. By formulating regulations and failing to provide effective enforcement procedures, the regulatory design in India has created the risk-adjusted success of organised cryptocurrency crime.

POLICY IMPERATIVES OF FUNCTIONAL ENFORCEMENT

Immediate Actions (0–6 Months)

Short-term actions include acquiring emergency access to forensic systems, such as Chainalysis and Elliptic, via bulk licensing to minimise the cost per seat and centralise forensic services.

The policy should also be clear on the position of India towards the use of privacy coins, either preventing a trade in regulated exchanges or requiring higher levels of due diligence, including the tracking of ownership and regulation of the transactions.

MEDIUM-TERM REFORMS (6–18 MONTHS)

The medium-term reforms should include developing standardised cryptocurrency investigation curricula that include blockchain mechanics, transaction clustering, subpoena processes, privacy coin constraints, cross-chain examination, and DeFi inquiries.

India should also institutionalise structures of cooperation with exchanges and have particular schedules of information exchange and freezing of assets. Moreover, there should be a regulatory framework for DeFi and cross-chain management, such as transaction reporting and investigational procedures.

LONG-TERM INFRASTRUCTURE

In the long term, it will be possible to develop indigenous open-source cryptocurrency forensic tools, in line with the Indian legal requirements, to minimise reliance on commercial platforms and establish local capacity.

There should also be an enhancement in regional coordination with formal investigative cooperation procedures with the FIA (Federal Investigation Agency) in Pakistan and the CID (Criminal Investigation Department) in Bangladesh (especially where cryptocurrency laundering borders on narco-terrorism and organised crime).

Conclusion

The cryptocurrency issue in India is not technological, but institutional. Investigative capacity is still lacking, even though tools are available, as well as the PMLA 2023 framework. Conviction rate of 0.25% of 5,892 cases, where 25 unregistered offshore platforms are operating openly, indicates that there is regulation but no enforcement. In the meantime, privacy coins, DeFi, and cross-chain bridges are not discussed

The key issue is whether India can transform ceremonial regulation into functional regulation. India needs immediate forensics, training and an upsurge in detecting new threats, or it would be a routine haven of organised digital crime.

References

Financial Action Task Force (FATF). (2023). Illicit Financial Flows Involving Virtual Assets.
https://www.fatf-gafi.org/en/publications/Methodsandtrends/illicit-financial-flows-cyber-enabled-fraud.html

Chainalysis. (2024). Crypto Crime Report.
https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/

European Union. (2024). Markets in Crypto-Assets (MiCA) Regulation.
https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica

Volume 01 | Issue 03| December 2025

CyberPeace

CYBERPEACE MAGAZINE

CRYPTOCURRENCY & BLOCKCHAIN