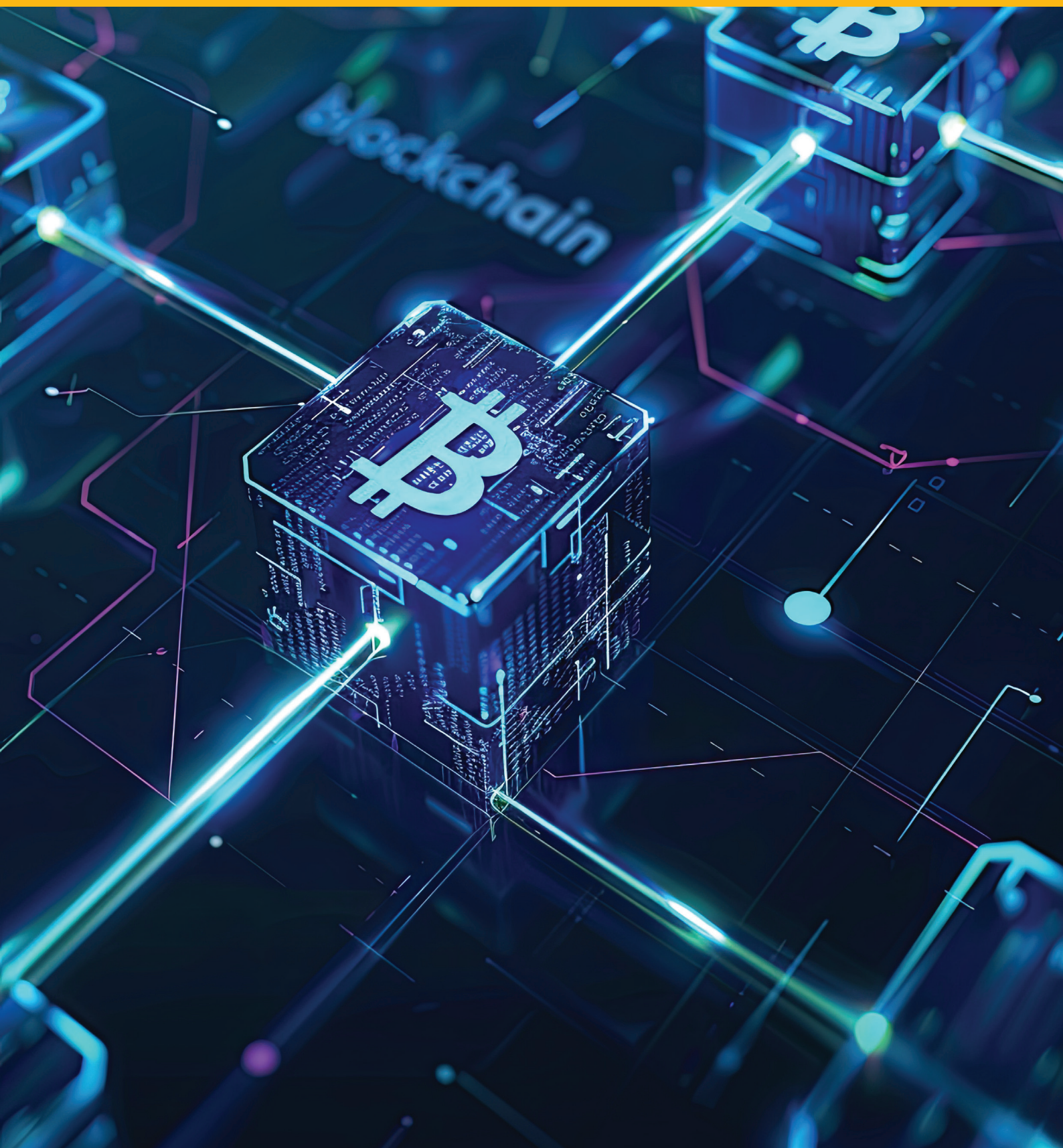




'creating a level playing field'

The Information Society Watch: Blockchain Technology



FOREWORD



The telecommunications industry is a cornerstone of modern connectivity, driving economic growth, fostering innovation, and shaping the future of global communication. As the sector continues to expand, it faces a rapidly evolving regulatory landscape, with increasing demands for transparency, data integrity, and compliance. Traditional methods of regulatory oversight are being challenged by the complexities of digital transformation, calling for new approaches that ensure security and accountability in an interconnected world.

With its promise of immutable data records, transparent processes, and enhanced security, blockchain technology has emerged as a key enabler in addressing these challenges. This white paper examines how blockchain can streamline regulatory compliance in telecommunications by enhancing data integrity, creating robust audit trails, and fostering transparency. Through case studies and practical insights, we highlight the real-world applications of blockchain, while also addressing the regulatory considerations and challenges that must be navigated for successful adoption.

POTRAZ is committed to fostering innovation and exploring forward-looking solutions that strengthen the regulatory framework of the telecommunications industry. We invite you to engage with this comprehensive analysis and join us in envisioning an Information and Communication Technology (ICT) landscape where technology and regulation coexist to deliver greater efficiency, transparency, and security. Together, let us harness the power of blockchain to build a future-ready digital landscape.

A handwritten signature in black ink, reading "G. K. Machengete", written over a horizontal line.

G. K. Machengete (Dr)

Director General

ABOUT THIS REPORT

The Information Society Watch is a quarterly publication by the Postal and Telecommunications Regulatory Authority of Zimbabwe's (POTRAZ). It is a collection of research whitepapers presenting information, expert analysis and insights into emerging trends and key issues as they relate to Information and Communication Technologies. It is based on quantitative and qualitative data gathered by the Authority from service providers, government, end-users, as well as reputable physical and online resources. It also provides valuable insights from industry and policy experts.

This quarterly publication of research whitepaper is in pursuit of building intellectual capital, delivering research evidence and building knowledge societies. In today's world, the creation, dissemination and utilization of information and knowledge are important as knowledge is widely regarded as a very important factor of production. Further-more, the whitepapers in this publication are intended to inform policy on various Information and Communication Technology matters of interest, nationally and globally.

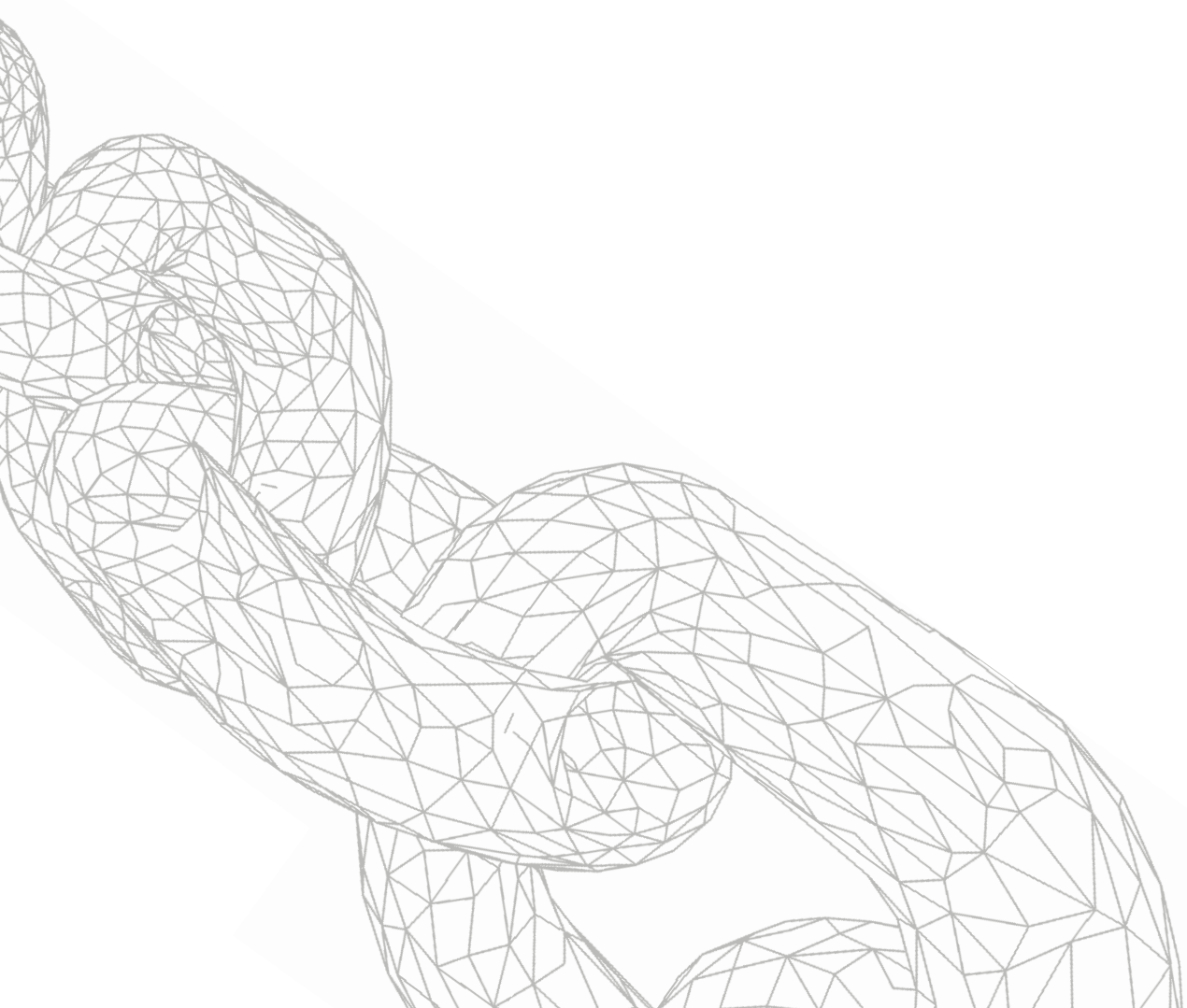


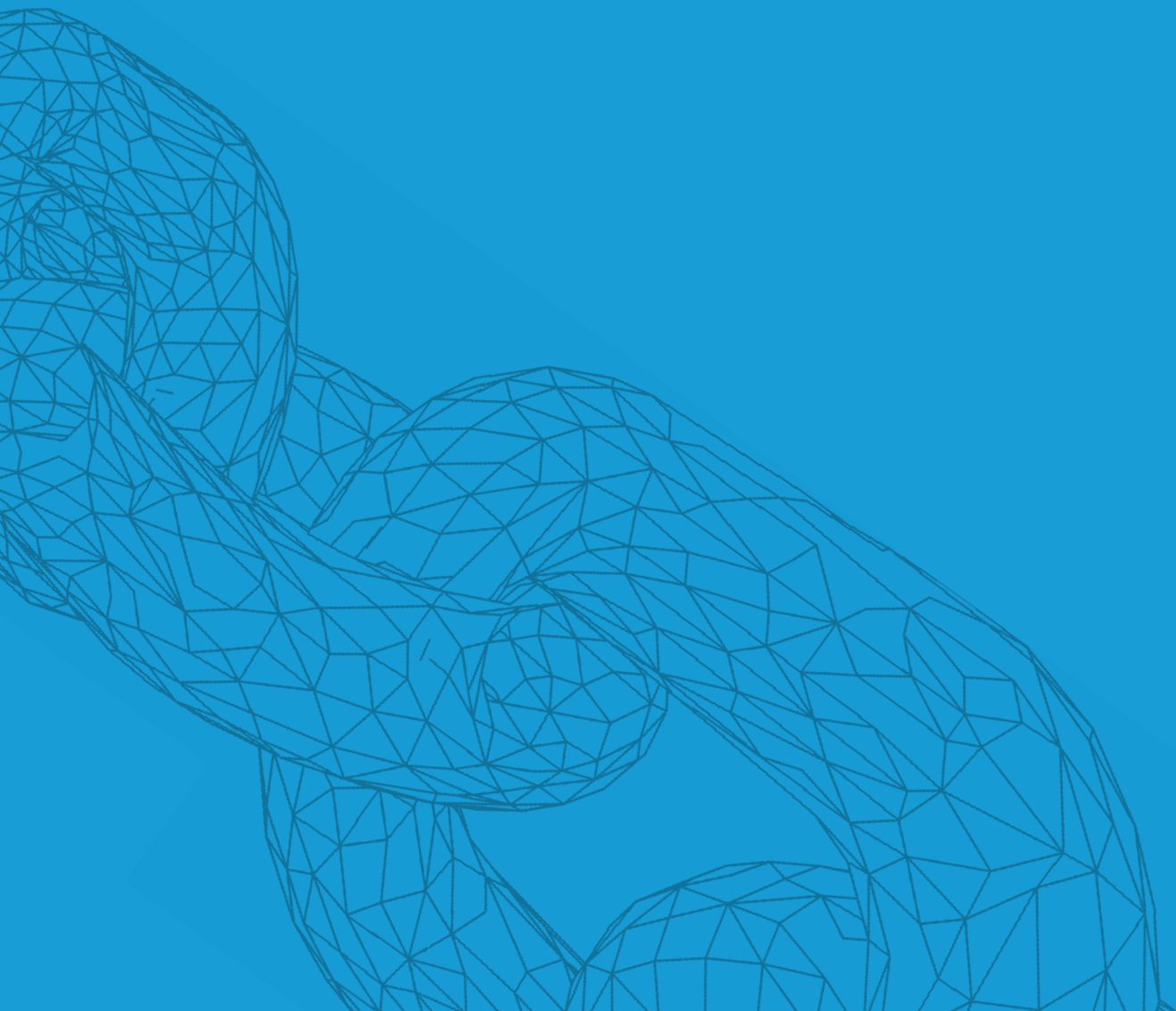
Table of Contents

White Paper 1: How Blockchain can enhance Data Integrity and Security in Compliance Processes.

White Paper 2: Blockchain for Compliance: Industry Case Studies.

White Paper 3: Blockchain Potential Challenges and Regulatory Considerations.

Expert Interview: Prof. Tawanda Mushiri, SIRDC





How Blockchain Can Enhance Data Integrity And Security In Compliance Processes

1. Introduction

The global telecommunication industry is experiencing a very profound change driven by technological advancements and shifts in consumer preferences. One of the cutting-edge emerging technologies is the blockchain technology which is being used by many organisations due to its potential to revolutionise various sectors including the telecommunication industry. Blockchain is a distributed system of data structures where the last data entry is linked to the next entry and then stored on a block (Sanda et al, 2022). In simple terms, blockchain technology refers to an advanced database mechanism that allows transparent information sharing within a business network. Blockchain technology has revolutionised the storage and management of data. According to Le and Hsu (2021), blockchain contributes to the process of changing low-trust centralised transaction ledger held by a single third party, to high-trust decentralised form held by different verifying nodes. Due to its decentralised nature and security robustness, blockchain has big potentials to be applied in various fields beyond cryptocurrency.

According to Deloitte's 2019 Global Blockchain Survey, 53 percent of respondents say that blockchain technology has become a critical priority for their organisations and 83 percent see compelling uses of Blockchain. In the ever-evolving landscape of compliance processes, ensuring data integrity and security stands as a paramount challenge for organisations across industries. Data integrity is the property that the data used in a solution is correct, reliable and useful for all participants and data security is

the practice of protecting digital information from unauthorised access, corruption or theft throughout its entire lifecycle. The advent of blockchain technology has emerged as a transformative solution, offering unprecedented levels of trust, transparency, and immutability in data management. Many auditors and regulators see the technology as a way to save time and improve compliance because it relies on self-executing smart contracts and once transactions are processed, they are irreversible (Kotze, 2018). According to Deloitte (2024), a wide range of organizations are already adopting blockchain-powered solutions to add efficiency and security across all areas of data management, including client onboarding, identity management, and transaction processing.

In compliance processes, ensuring data integrity is one of the top challenges in some organisations. The goal of this paper is to explore the improvements in compliance processes which result from the implementation of blockchain technology in the telecommunication industry. Traditional systems are often vulnerable to data tampering, unauthorised access, and single points of failure, leading to compliance breaches and costly repercussions. Blockchain technology presents a paradigm shift by providing a distributed ledger that securely records transactions across a network of computers, ensuring that data remains immutable and transparent. In addition to that, the decentralised nature of blockchain technology eliminates the need for central authority, reducing the risk of fraud manipulation in compliance processes.

2.4 Cryptography

data privacy and security

2.5 Timestamps

Timestamping is integral to the blockchain's structure; each block includes a timestamp cryptographically linked to the previous block. These digital timestamps on the front of the block make it easy to track and verify information. The chronological order, verified by the timestamps acts as a robust proof of time, preventing disputes about transaction order.

2.6 Resilience

A distributed database by its nature is more resistant to accidental failures or malicious attacks than a centralised system. Data is not stored on a single location, making it highly resistant to single points of failure. Multiple copies of the blockchain exist across the network, ensuring redundancy and fault tolerance. If one or more nodes on the blockchain fail or are hacked, the rest of the system can still function reliably

2.7 Smart Contracts

These are self-executing contracts with predefined rules encoded on the blockchain. Smart contracts execute transactions based on predefined conditions, reducing the need for intermediaries, which in turn lowers costs and streamlines operations (Abdul, 2024).

2.8 Security

This is a paramount feature which is achieved through a combination of robust cryptographic techniques and consensus mechanisms. Data is distributed among all nodes in the blockchain such that a hacker can only corrupt a blockchain only he seizes most of the nodes which much tougher than attacking a single and central server. Cryptographic hashing creates unique fingerprints for each block and digital signatures authenticate transactions, thus preventing unauthorised access and modifications of data. Consensus mechanisms also ensure that all nodes agree on the valid state of

the blockchain leading to the prevention of fraudulent additions or deletions.

3. Improvements In Data Integrity And Security In Telecommunication Compliance Processes

Telecommunication companies handle vast amounts of sensitive data which include customer information, call records, and network configurations. Data integrity and security is very important in these organisations, especially with the increasing regulatory requirements and cybersecurity threats. Blockchain technology presents unique opportunities to enhance compliance processes in the telecommunication sector. Capturing relevant data with integrity has been a priority for a long time and ensuring security from different threats has been a challenge. Blockchain technology, due to its features, has been able to tackle some of these challenges. Some of the improvements include:

3.1 Immutability and Transparency

It becomes virtually impossible to alter or delete data without consensus from participants, once data is recorded on a blockchain. All transactions on a blockchain are transparent and can be traced back to their origin. The immutability and transparency of data enables auditors and regulators to easily verify the authenticity of data and track its entire history thus enhancing trust and accountability in compliance processes since data integrity is well maintained

3.2 Data Security

The use of advanced cryptographic techniques enhanced data security. Each block is linked to the other using cryptographic hashes and this makes it extremely difficult to for malicious actors to tamper with the data stored. According to Nakamoto (2008), Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. This kind of security has improved data integrity in the telecommunication industry, simplifying compliance audits and enables stakeholders to access up to date and accurate information. Blockchain also enhances the

security of data that is being exchanged between parties. The use of encryption, digital signatures, and private keys secures the exchange of sensitive and private information such as customer data, and call records making it easier for telecommunication companies to comply with data protection regulations.

3.3 Network Security

Network security is the protection of the underlying networking infrastructure from unauthorised access, misuse, or theft. Blockchain technology, due to its decentralisation feature and the use of cybersecurity frameworks, can enhance the storage and management of cybersecurity data such as threats intelligence, security policies and access controls.

3.4 Smart contracts and Consensus Mechanisms

Smart contracts automatically enforce compliance rules, triggering actions based on predefined criteria and ensure all parties involved comply with the agreed terms and conditions for example service level agreements between telecommunication service providers and their customers. This is also similar to the consensus mechanisms where all nodes in a blockchain have to agree with each other before actions are made. This gives a room for a thorough data validation and multi-step verification before any action is made, thus ensuring data integrity.

3.5 Emergency Services and Location Tracking

Blockchain can enhance emergency services by securely storing and sharing location data during emergency calls. Emergency services are very common in some sectors especially in the health sector. According to Wu and Ho (2023), emergency-relevant medical data of patients can be securely uploaded to a TLS server integrated with the Fabric blockchain, using advanced tools for scheduling and automating the uploading process. Once stored on the ledger, the data is replicated and distributed to other authorised network members, such as hospitals or healthcare personnel, based on predefined policies, ensuring a consistent and comprehensive view of the patient's health data. This can help emergency responders to locate patients or individuals in distress more quickly and accurately thus improving compliance with regulations related to emergency service provision by telecommunication service providers.

3.6 Data Roaming Agreements and Authentication

Data roaming refers to the ability for a mobile device like a smartphone or tablet to access a cellular data network when it's outside its home network's coverage area. Blockchain can help in securing roaming agreements between telecommunication operators. This ensures the accurate calculation and settlement of charges between these operators in real-time. In addition to that, blockchain can also enhance the authentication of data roaming by securely validating user identities and authorising access to network services. This can improve compliance with data protection regulations in the telecommunication industry.

3.7 Quality of Service

Blockchain can be used to monitor and verify the quality of service provided by telecommunication networks. Smart contracts can enforce service level agreements and trigger penalties or incentives based on predefined performance metrics, improving compliance with service quality standards.

3.8 Decentralisation

Blockchain operates on a decentralised network of nodes, eliminating the need for a central authority to control or manage data. This decentralised structure reduces the risk of single points of failure and unauthorised

alterations, enhancing data security.

3.9 Fraud Detection

Blockchain's transparent and immutable nature can help in fraud detection by creating a secure audit trail of transactions. Telecommunication companies can use blockchain to identify suspicious activities, such as unauthorised access or fraudulent calls, and take immediate action to mitigate risks.

4. Conclusion And Recommendations

As explored in this paper, blockchain technology has improved data integrity and security in compliance processes across industries including the telecommunications industry.

As explored in this paper, blockchain technology has improved data integrity and security in compliance processes across industries including the telecommunications industry. Real-world use cases and expert insights has indicated that blockchain has the potential to transform compliance practices by providing secure data sharing, automating processes, enhancing network security, and facilitating regulatory compliance reporting. Organisations can now address key compliance issues, streamline operations, strengthen trust in data management, and ensuring an end-to-end security of information by using blockchain. To effectively harness the power of blockchain technology in telecommunication compliance, organisations are encouraged to consider the following factors:

- **Pilot projects and Proof of Concepts:** Organisations are encouraged to assess the feasibility and benefits of blockchain technology in compliance processes through the implementation of pilot projects and proof of concepts in sandboxes that are regulated, to ensure that performance and strategies are well refined before full-scale implementation.
- **Collaboration and Partnerships:** Organisations can collaborate with industry peers, technology providers and regulatory bodies to foster innovation and knowledge sharing in blockchain adoption. This help in navigating different opportunities and addressing interoperability challenges associated with blockchain technology in meeting the telecommunication industry standards.
- **Data Privacy and Compliance by Design:** Organisations are encouraged to incorporate privacy-enhancing technologies, data protection measures and regulatory compliance frameworks in their products and services to ensure the security and ethical use of blockchain in compliance processes.
- **Continuous Education and Training:** Education and Training programs are very vital in building internal expertise and awareness of blockchain technology in organisations. Imparting staff with the necessary skills and knowledge enables effective utilisation of blockchain technology.
- **Monitoring and Evaluation:** The performance and impact of this technology on compliance processes needs to be monitored to optimize its effectiveness in telecommunication compliance.

Organisations can unlock the transformative benefits of blockchain in compliance processes, paving the way for secure, efficient, and compliant future in the telecommunication industry. The adoption and effective implementation of blockchain in compliance processes is not an overnight process and it requires the integration of the stated factors.

5. REFERENCES

- Abdul S. S. M (2024), Navigating Blockchain's Twin Challenges: Scalability and Regulatory Compliance
- Cybersecurity on Blockchain Module, World Economic Forum, Available at <https://www.weforum.org>
- Data Integrity on Blockchain Module, World Economic Forum, Available at <https://www.weforum.org>
- Data Protection on Blockchain Module, World Economic Forum, Available at <https://www.weforum.org>
- Deloitte (2017), Applying blockchain in securitization: opportunities for reinvention
- Deloitte (2018), Tech Trends 2018: The symphonic enterprise
- Deloitte (2020), Audit transformation and opportunities in cognitive, blockchain, and talent
- Deloitte (2023), How blockchain can enhance PE operations | As adopters take early steps, the technology's potential comes into focus
- Harun A., Khan M. (2024), Leveraging Blockchain Technology for Enhanced IT Governance and Compliance Management
- <https://aws.amazon.com/what-is/blockchain/?aws-products-all.sort-by=item.additionalFields.product-NameLowercase&aws-products-all.sort-order=asc>
- <https://www.ibm.com/topics/data-security>
- ITU-T Focus Group Digital Financial Services (2017), Distributed Ledger Technologies and Financial Inclusion.
- Kotze D. (2018), The rise of Blockchain in Africa, African Blockchain Report 2018
- Le T and Hsu C. (2021), A Systematic Literature Review of Blockchain Technology: Security Properties, Applications and Challenges
- Nakamoto S. (2008), Bitcoin: A Peer-to-Peer Electronic Cash System
- Sanda O., Pavlidis M., and Polatidis N., (2022), A Regulatory Readiness Assessment Framework for Blockchain Adoption in Healthcare
- Shende A. (2024), Regulatory Compliance and Blockchain In Mortgages: Leveraging Transparency And Efficiency For A Secure Future
- United Nations Conference on Trade and Development (2023), Global Report on Blockchain And its Implications on Trade Facilitation Performance
- Wahab S. O. (2024), A Framework for Learning-Based Attack Detection and Regulatory Compliance in Blockchain Technology
- Wu T. C., Ho C. B. (2023), Blockchain Revolutionizing in Emergency Medicine: A Scoping Review of Patient Journey through the ED



Blockchain for Compliance: Industry Case Studies

1. Introduction

The telecommunications industry continues to face considerable challenges in addressing the increased need for data security while remaining compliant with the evolving landscape of regulatory mandates. With the expansion of the industry, telecommunications operators must secure terabytes of confidential information and at the same time, guarantee that their systems adhere to strict local and international regulations. With the introduction of 5G, Internet of Things (IoT), and cloud-based services, telecom networks have become more complex, creating a vast attack base for cybercriminals. One data breach can have destructive consequences, resulting in reputational damage, financial losses and regulatory penalties.

Telecommunications operators must prioritise data security and adopt solid measures to safeguard their networks, systems, and customer data from cyber threats. By taking a proactive approach to security and regulatory compliance, operators can not only protect their infrastructure but also encourage and create trust among their customers and maintain a competitive edge in the rapidly growing marketplace.

One promising solution to these problems is blockchain technology. The decentralised, unchangeable ledger that blockchain provides will offer better transparency, security, and efficiency and therefore, would be a good solution to many of the problems that are prevalent in the telecommunications industry, such as data privacy, identity authentication, roaming and interconnection and quality of service (QoS) management (Bhattacharyya, A., Chaturvedi, S. 2020). The use of blockchain technology would

greatly improve compliance, as it would provide permanent records that facilitate accurate and timely reporting, thus eliminating the risk of fraud and minimizing human error (Zwitter, A., Boisse-Despiaux, M., 2018).

All regulators require that telecommunications operators uphold the highest standards of data security and privacy, comply with all global data transfer laws and be transparent in all their operations. Blockchain can make compliance a lot easier as it automates the recording and reporting of vital information, makes audits simple, and allows for real-time tracking of transactions and agreements, which ultimately cuts down on operational costs.

Several telecommunications companies have already begun using blockchain to meet regulatory requirements and enhance data security. Blockchain has the capability to alter the industry by assuring compliance with global data protection requirements such as the General Data Protection Regulation (GDPR) and increasing the security of interconnected networks and systems. To gain an understanding of regulatory compliance using blockchain, we studied Swiss Post, Swisscom, and Vodafone. These case studies demonstrated the potential of blockchain to improve regulatory compliance and security in the telecommunications business.

2. Case Study 1: Swiss Post And Swisscom- Blockchain Infrastructure For Regulatory Compliance

2.1 Introduction

In 2018, Swiss Post and Swisscom, two of the largest and most trusted service providers in Switzerland's postal and telecommunications sectors announced the deployment of a blockchain infrastructure de-

signed to meet the highest standards of security and regulatory compliance. The initiative showcased the potential of blockchain technology to support diverse applications across industries while maintaining stringent adherence to regulatory frameworks. It was created as a result of the growing need for secure and efficient data management in “confidential” industries such as finance, healthcare, and utilities. This collaboration enabled the establishment of a private blockchain backbone in Switzerland, storing all the data within the country, which is a necessity for regulatory compliance with Swiss data privacy regulations.

2.2 Business Challenge

Swiss companies, notably those in highly regulated sectors, faced strict compliance requirements regarding data handling, security, and privacy. With rising cyber threats, organizations felt more and more obligated to protect the confidentiality, integrity, and availability of sensitive information. Traditional methods of data sharing and verification were not just vulnerable to breaches but also costly and time-consuming. Swiss Post and Swisscom realised that they needed a solution that would ensure secure, tamper-proof data handling and simultaneously comply with the Swiss legal requirements, including the General Data Protection Regulation (GDPR).

2.3 Blockchain Initiative

Swiss Post and Swisscom overcame these hurdles by merging their existing infrastructures to develop a proprietary blockchain solution, built on the Hyperledger Fabric2 architecture. Unlike public blockchains such as Bitcoin or Ethereum, this system operated as a permissioned network, meaning that only pre-approved users with contractual relationships could access and participate in the blockchain. Several features made this blockchain particularly attractive for regulatory compliance:



**Data
Sovereignty**

Every data processed within the blockchain remained in Switzerland, warranting compliance with national data protection laws.



**Energy
Efficiency**

By restricting usage to authorized users, the infrastructure operated with far less energy consumption than public blockchains, a key factor for sustainable development.



**Security and
Trust**

Swiss Post and Swisscom maintained a highly secure and trusted system, verifying each other's operations through distributed ledger technology (DLT), providing a trustworthy and tamper-resistant environment for sensitive digital business processes.

2.4 Applications

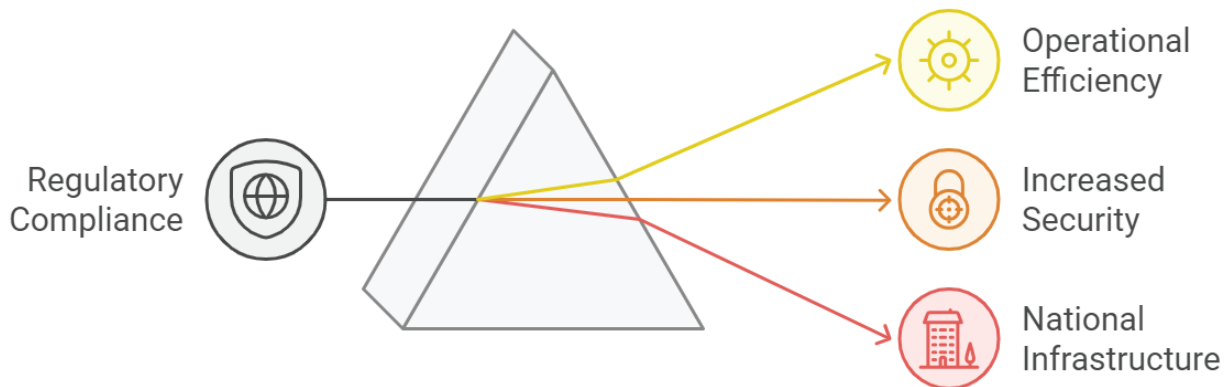
Swiss Post and Swisscom launched pilot applications of the blockchain in mid-2018, focusing on various use cases:

Pharmaceutical Transport: Swiss Post used blockchain as a method to record temperature readings when transporting pharmaceuticals in order to uphold health and safety laws.

Renewable Energy Billing: Swiss Post's PostFinance partnered with Energie Wasser Bern to trial a blockchain billing system that would simplify billing tenants in buildings with photovoltaic installations as the energy is distributed.

Digital Shares: Swisscom partnered with Daura AG, a Swisscom subsidiary, to create digital shares through blockchain technology allowing for the secure and convenient transfer of equity management.

2.5 Results



Its blockchain immutable ledger and data sovereignty (i. e. more regulatory compliance) allowed both corporations to comply with Swiss and European data protection laws. Also, automating many business processes (such as billing and data verification, helped smooth processes out, eliminating much of the manual intervention and administrative costs. The permissioned nature of the blockchain provided increased security by ensuring that only verified parties could access the system, significantly lowering the risk of data breaches and fraud. Additionally, the blockchain infrastructure served Switzerland's strategic interests in data sovereignty and national security by storing data within the country.

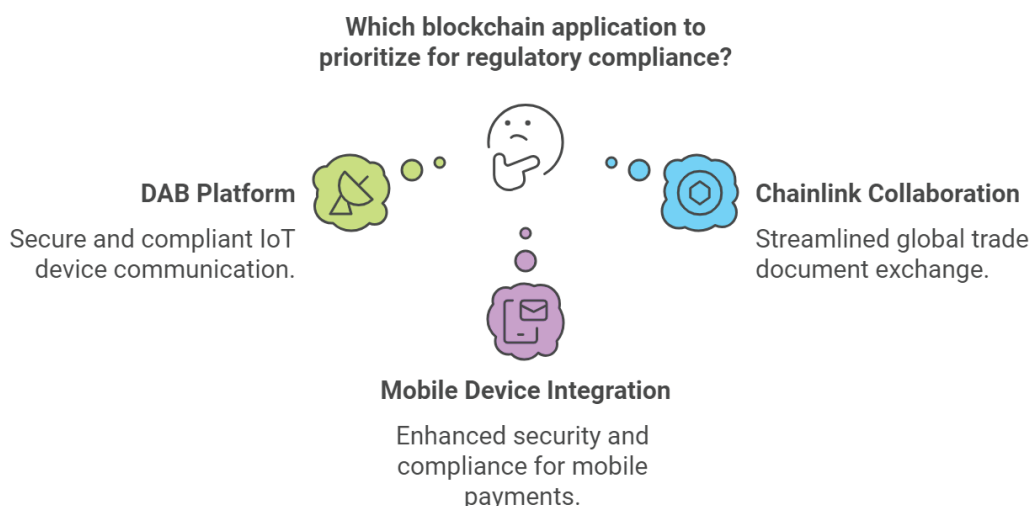
2.6 Conclusion

The partnership between Swiss Post and Swisscom to build a private blockchain infrastructure is an example of how telecommunication companies used blockchain technology to accommodate the growing demand for data security and regulatory compliance. The system increased operational efficiency and set a precedent for other telecom operators who wish to use blockchain in a regulated space.

3. Case Study 2: Vodafone's Blockchain Initiatives

3.1 Introduction

As an international leader in telecommunications, Vodafone has taken proactive initiatives toward integrating blockchain technology to meet the growing regulatory demands, particularly in data security, identity verification, and transparency. Blockchain's decentralisation allows for companies like Vodafone to have extra insurance that their customer data, transactions, and digital communications are in compliance with all global regulatory frameworks and that they are indeed following all of the legal and security standards.



3.2 Blockchain in Vodafone's Digital Asset Broker (DAB) Platform

One of Vodafone's biggest blockchain initiatives is a project called the Digital Asset Broker (DAB) which enables secure and autonomous communication between Internet of Things (IoT) devices. This blockchain approach allowed all of the enormous amounts of data exchanged between IoT devices to be transparent, auditable, and secure, which adheres to very strict data protection laws.

Regulatory Focus: The DAB platform assisted with regulatory compliance by ensuring that all transactions involving IoT devices followed GDPR (General Data Protection Regulation) and other data protection laws all over the world. With the use of blockchain's immutable ledger, Vodafone can make sure that all of the devices' communication is traceable and secure.

Results: The platform allowed Vodafone to track and record communications in a compliant fashion. Using blockchain for secure device transactions meant less risk of non-compliance for Vodafone, but also a faster, more efficient process for complying with regulations regarding data privacy and secure communications.

3.3 Blockchain and Vodafone-Chainlink Collaboration: Enhancing Cross-Border Compliance

Vodafone's partnership with Chainlink Labs allows for the ease of use of blockchain to facilitate the exchange of global trade documents, which in turn directly facilitates compliance with cross-border trade regulations. Trade documentations are always delayed or fraudulent, and that always seems to lead to regulatory problems. Immutabil-

ity and security are what blockchain offers to combat these issues.

Regulatory Focus: Vodafone utilizes blockchain to manage real-time trade document exchanges in order to maintain complete transparency and accountability over their global operations. This helps to adhere to laws of international trade (i.e., customs, and import/export laws).

Results: Vodafone's blockchain document handling would lead to fewer errors and fraud, thus better compliance with regulatory requirements. It makes it easy to check documents in real time and know that all the information is accurate, secure, and legal

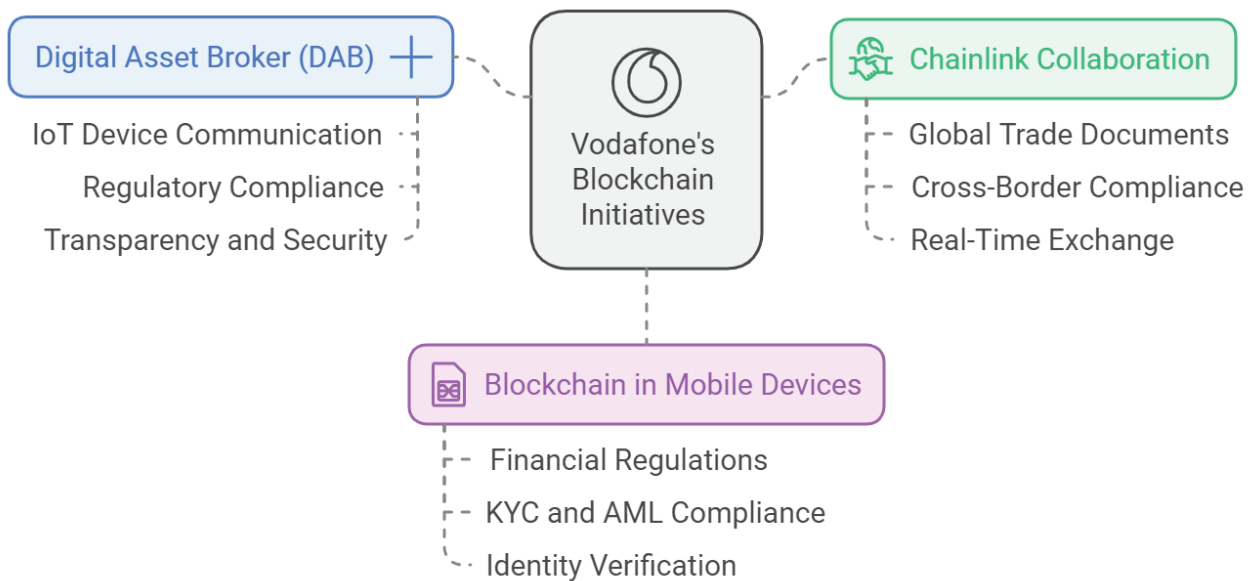
3.4 Embedding Blockchain in Mobile Devices for Regulatory Compliance

Vodafone research into putting blockchain-based wallets into SIM cards seems to be a good idea because it adds that extra level of security necessary for the management of digital assets that are required to comply with financial regulations regarding mobile payments and data transactions.

Regulatory Focus: This blockchain answer would allow Vodafone to comply with their KYC and AML regulations because it can securely verify identities and make sure that transactions are traceable. These are vital stipulations in financial compliance especially in areas with maturing regulatory structures for digital payments.

Results: With the use of blockchain, Vodafone could make an extremely transparent and secure system that makes it much easier to verify identities and track transactions, thereby making sure that all of the financial transactions are in compliance with the laws and regulations.

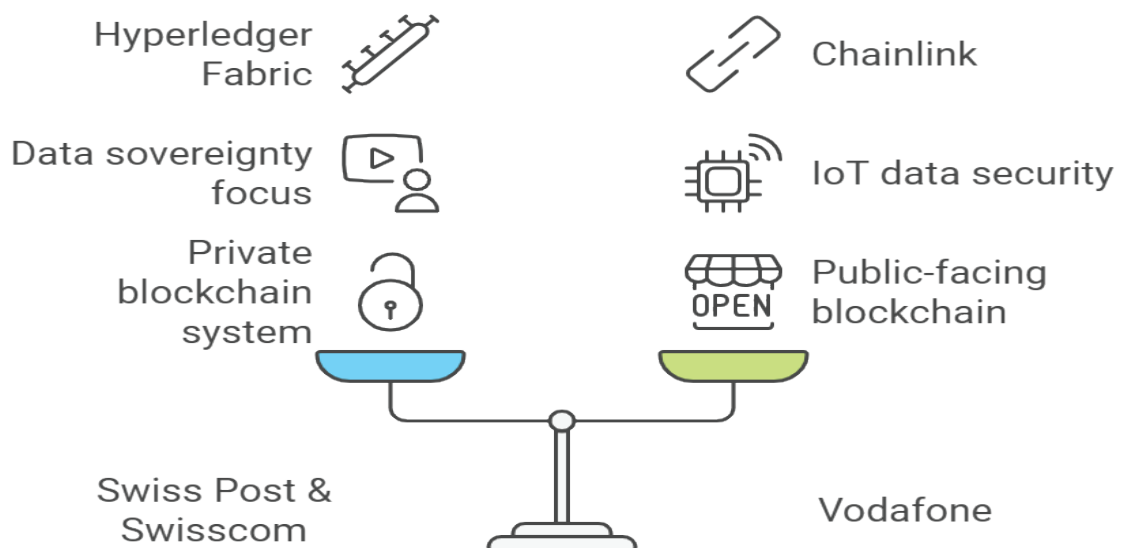
3.5 Outcomes and Regulatory Impact



Vodafone's initiatives demonstrate how blockchain technology can drive regulatory compliance in key areas such as data privacy, secure communication, identity verification, and cross-border trade. Vodafone can meet the growing and complicated compliance requirements of the telecom industry by using blockchain's immutable and transparent transaction history. These actions keep Vodafone at the top of the list of secure/compliant telecommunications companies.

4. Comparative Analysis

4.1 Blockchain Implementation Approach



Comparing blockchain implementations by Swiss Post & Swisscom and Vodafone.

Swiss Post & Swisscom: The partnership between Swiss Post and Swisscom to build out a private blockchain infrastructure centred around data sovereignty and security, performance. Their blockchain is a permissioned system, meaning only trusted, identified users with contractual relationships can access it. This solution is based on Hyperledger Fabric, which is a secure and efficient blockchain framework.

Vodafone: Vodafone has been using blockchain in some of its operations, mainly in its (IoT) platform, using it to secure SIM-based devices, and manage cross-border trade and identity verification. It is not as close as the Swiss Post and Swisscom private blockchain, but Vodafone has been doing some work with blockchain as well, but more public-facing, using things like chainlink to de-centralize and secure the flow of IoT data.

4.2 Key Regulatory Compliance Achievements

Swiss Post & Swisscom: One of the key regulatory accomplishments of Swiss Post - Swisscom is the fact that they can adhere to Switzerland's strict data privacy laws by ensuring that all blockchain data remains in Switzerland. This is especially important in financial services, where there are severe data privacy laws. They utilize a permissioned blockchain to create a transparent but secure ledger system to handle the sensitive data, i. e. pharmaceuticals and renewable energy billing.

Vodafone: Everything Vodafone has done has been geared towards global regulatory compliance, GDPR in the EU and all. Vodafone uses blockchain to secure IoT devices and manage identities, and therefore guarantees compliance over borders, especially in the EU. This allows them to comply with all of the international privacy and data protection laws, and it drastically decreases the possibility of data breaches and fines from regulatory agencies.

4.3 Efficiency and Scalability

Swiss Post & Swisscom: It's a permissioned blockchain solution so the transaction processing is much faster and more efficient because the network is closed and only needs verification from a limited number of parties. This is especially beneficial for corporations that have to have those high security standards and quick accurate compliance reports. But this system's expandability is somewhat inhibited because it's so private, it's more about the small, niche markets instead of broad-scale telecom acceptance.

Vodafone: Vodafone is using blockchain for IoT which provides a very scalable solution especially with the IoT continuing to explode. Their blockchain implementation is decentralized which allows for much larger, more global participation in the network and it is a flexible solution that could evolve as the number of connected devices grows. However, the problem is to handle the rollout on a grand scale, with thousands of devices being deployed in many different countries, all with differing local regulatory requirements.

4.4 Security and Risk Management

Swiss Post & Swisscom: The Swiss have the most advanced security precautions in their blockchain infrastructure because of the types of industries they have (banking, pharmaceuticals, energy). The blockchain is permissioned so that all participants are verified which eliminates the risk of fraud and unauthorized access. The infrastructure also facilitates immediate verification of compliance certificates, enhancing trust between partners and reducing regulatory risks.

Vodafone: Vodafone is focusing on IoT security which is a big pain in the telecommunications industry because they must secure these huge networks of interconnected devices. Blockchain authentication and securing of sim-based devices provides a strong security layer, reduces telecom network vulnerabilities and also improves compliance with global cybersecurity regulations. Their lack of centralization also eliminates many single points of failure which is very important when it comes to protecting large amounts of customer and operational data.

4.5 Outcomes and Impact

Swiss Post & Swisscom: The results have been very good, especially with regards to regulatory compliance in the industries where high standards of data security and privacy are required. With the use of blockchain in logistics and energy markets, the process of tracking pharmaceutical data or energy billing has become much simpler, making it easier to comply and more transparent. That's hurt Switzerland's reputation as a safe and secure place to do digital business.

Vodafone: Vodafone's blockchain endeavours have come a long way in enhancing IoT security and regulatory conformity, especially regarding international commerce. With blockchain's secure management and tracking of IoT devices, Vodafone can comply with strict data protection laws in all countries. But, at the same time, their international scope makes their operations a bit more difficult because they must deal with several different regulatory agencies.

4.6 Comparative Strengths

Swiss Post & Swisscom: Their blockchain solution is strong because of its high security, and energy efficiency, and because it is good for industries that are highly regulated and sensitive. Their permissioned block chain architecture does perform better in secure closed systems, but it may not have the flexibility required for wider, international telecommunication usage.

Vodafone: The greatest advantage Vodafone has is that they can scale a blockchain for global IoT use, and that's perfect for telecommunications. They can do this because they use decentralized networks, which gives them the flexibility and the ability to comply with more regulations across borders, but this could eventually mean that the standards that they will have to maintain to ensure worldwide consistency will become extremely complicated.

5. Opportunities For Zimbabwe: Lessons From Case Studies

In Zimbabwe, the adoption of blockchain in the telecom sector is still in its budding stages. Although people are becoming more aware of the capabilities of the technology, it has not been integrated into mainstream operations. Instead of using blockchain technology to solve the problems of data sovereignty or operational transparency, the emphasis has currently been on constructing regulatory structures such as the Data Protection Act. Zimbabwe is rapidly expanding its mobile-based financial services and other ICT initiatives, hence the need for secure digital services is evident.

Zimbabwe's telecom industry can learn enormously from the Swiss and Vodafone case. The private blockchain model of Swiss Post and Swisscom can be a template for Zimbabwean telecommunications companies to follow in addressing issues of data sovereignty and privacy. Considering that Zimbabwean laws stress the importance of keeping confidential information within the country, a private blockchain network would allow that information to remain under the country's control and comply with continental stipulations such as those in the African Union Convention on Cyber Security and Personal Data Protection.

The traceability and transparency achieved by Vodafone through blockchain could also be relevant to Zimbabwe's efforts to improve regulatory compliance and billing transparency. By implementing blockchain, local operators could create an immutable record of transactions, ensuring that billing practices and tariff structures are clear and easily auditable by regulatory bodies. This method would not only allow operators to comply with POTRAZ regulations but also make consumers feel that the telecom services are impartial.

Zimbabwe is still in its infancy of blockchain in telecoms, but there is no shortage of opportunities to apply lessons learned from international case studies. With the focus on capacity building, collaboration, and regulatory congruence, Zimbabwe can take full advantage of blockchain to overcome some of its most pressing problems in the telecommunications industry and become a

leading force in the area.

6. Conclusions And Recommendations

Blockchain technology has shown great potential in addressing the telecom industry's most compelling data security issues, regulatory compliance, and operational efficiency. Swiss Post, Swisscom and Vodafone have shown that blockchain can indeed be implemented strategically to meet the stringent requirements of data privacy and secure communication, while at the same time increasing transparency and trustworthiness.

The case studies emphasize the need for blockchain technology in the telecom industry in order to comply with regulations and strengthen data security. Each of the solutions has its own strong points, but the general result is a more secure, open, and streamlined telecom structure. With the growth of 5G and IoT, blockchain will probably play a bigger part in how these issues are addressed, allowing telecom companies to stay ahead and gain the trust of their customers.

- Telecom providers who handle personal data should be incorporating permissioned blockchain networks, like the ones Swiss Post and Swisscom use. These types of networks are more secure as they only allow access to users that have been verified, making transactions quicker and reducing the chances of fraud or unauthorized access.
- Operators should focus on scalable blockchain solutions for future technologies, particularly with the growth of IoT networks. Vodafone's decentralized blockchain model demonstrates scalability, offering a flexible approach for managing regulatory compliance in an increasingly interconnected world.
- Continuous investment in blockchain R&D is essential for telecom operators to explore emerging use cases. Staying ahead in blockchain innovation will enable operators to maintain competitiveness and adapt to evolving regulations.

7. References

- Accenture. (2023) Blockchain in Telecommunications: Unlocking New Revenue Streams. Available at: <https://www.accenture.com> (Accessed: 19 September 2024).
- Bhattacharyya, A., & Chaturvedi, S. (2020). Blockchain technology in the telecom industry: Benefits, applications, and future. *Telecom Journal*, 32(4), 120-134.
- Colangelo, G. (2019). Blockchain technology and GDPR: A clash of interests? *European Data Protection Law Review*, 5(3), 316-323.
- Ernst & Young. (2022) Regulatory Considerations for Blockchain Adoption in Telecoms. Available at: <https://www.ey.com> (Accessed: 8 October 2024).
- European Telecommunications Standards Institute (ETSI). (2022) Blockchain Standards for 5G Networks and Beyond. ETSI White Paper, No. 46.
- GSMA. (2022) Blockchain for Mobile Operators: Opportunities and Challenges. Available at: <https://www.gsma.com> (Accessed: 25 September 2024).
- ITU-T. (2023) Blockchain in the Telecommunications Sector: Standards and Best Practices. Available at: <https://www.itu.int> (Accessed: 8 October 2024).
- Machina Research. (2022) Blockchain in IoT: Implications for Telecom Operators. Machina Research White Paper.
- PwC. (2023) Telecommunications Trends 2023: The Role of Blockchain in 5G and IoT Integration. Available at: <https://www.pwc.com> (Accessed: 8 October 2024).
- Swan, M. (2015). *Blockchain: Blueprint for a New Economy*. O'Reilly Media.
- Telecoms.com. (2023) Top Blockchain Use Cases in the Telecom Sector.
- Vodafone Business. (2023) Transforming Supply Chains with Blockchain: Lessons from the Telecom Industry. Available at: <https://www.vodafone.com> (Accessed: 8 October 2024).
- World Economic Forum. (2021) Blockchain for Supply Chains and International Trade: Technology Architecture, Operations, and Use Cases. Available at: <https://www.weforum.org> (Accessed: 19 September 2024).
- Zwitter, A., & Boisse-Despiaux, M. (2018). Blockchain for GDPR Compliance: A technological solution to regulatory hurdles. *Journal of Data Protection & Privacy*, 5(2), 91-104.



Blockchain Potential Challenges and Regulatory Considerations

1. Introduction

Blockchain technology has gained global attention for its potential to revolutionise various sectors, including telecommunications, by improving transparency, security, and operational efficiency. In the context of regulatory compliance, blockchain offers a reliable way to record, verify, and audit telecommunications data, such as customer records, billing information, and spectrum management, which are critical areas for the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ). However, despite its promise, blockchain adoption presents significant challenges that Zimbabwe must address, particularly considering the country's unique socio-economic and regulatory environment. This whitepaper explores the challenges and regulatory considerations for adopting blockchain in Zimbabwe's telecommunications sector. It focuses on interoperability, scalability, energy consumption, data privacy, regulatory frameworks, and the financial costs of transitioning to blockchain.

2. Challenges Of Blockchain Adoption In Zimbabwe's Telecommunications Sector

2.1 Interoperability Issues

While the development of different blockchain networks shows great potential for blockchains, the isolated networks have led to data and asset silos, limiting the applications of this technology (Ghaemi, S., et al 2021). Cross-chain interoperability is one of the crucial challenges preventing widespread adoption of blockchain applications. Cross-chain interoperability represents the ability for one

blockchain network to interact and share data with another blockchain network (Madine, M., et al 2021). Interoperability is a critical issue when considering the integration of blockchain technology into Zimbabwe's telecommunications sector. Zimbabwe's telecommunications operators use a variety of legacy systems that may not be easily compatible with blockchain platforms. Blockchain technologies, such as Ethereum, Hyperledger, and Corda, each have distinct frameworks, consensus mechanisms, and capabilities (Kaur, M. and Lnu, N., 2022). For the blockchain to function fully, it requires components such as the Node, Transaction, Block as a data structure, Chain of the blocks, Miners to perform the block verification process, and Consensus (consensus protocol) (Gabriel Kabanda., 2021). If operators adopt different platforms, cross-platform communication and data sharing become complex, making it difficult for POTRAZ to uniformly monitor and enforce regulatory compliance.

In Zimbabwe, telecommunications operators like Econet, NetOne, and TelOne have invested heavily in proprietary infrastructure. Blockchain integration requires seamless communication between these systems to allow effective data sharing and auditing. The lack of established blockchain standards in Zimbabwe's telecommunications sector compounds this problem, as different operators could end up using incompatible platforms, leading to data silos. Interoperability challenges are not unique to Zimbabwe. In Nigeria, where multiple telecommunication operators use different digital frameworks, cross-platform integration has also proven to be a significant challenge (Nsabimana et al., 2021). POTRAZ can play a pivotal role in developing blockchain standards for the telecommunication industry in Zimbabwe. Drawing inspiration from regional initiatives like Smart Africa, Zimbabwe can establish a

standardized blockchain protocol specifically for the telecommunications sector.

2.2 Scalability Constraints

When discussing scalability in the context of blockchain technology, the term refers to the transaction processing speed (Carlo R.W., 2023). Blockchain scalability has to do with the capacity of a blockchain network to handle a growing volume of transactions, store data and increasing the number of nodes running in the blockchain network efficiently and in a timely manner, without compromising on its core features such as security, decentralisation, and consensus (Khan, D., et al 2021 & Carlo R.W., 2023).

Today, one of the major challenges associated with blockchain is scalability (Khan, D., et al 2021). The ever-increasing demand for blockchain applications has resulted in significant scalability challenges, resulting in transaction latency, making the system slower and less efficient, thereby hindering their widespread adoption and utility (Carlo R.W., 2023). Blockchain scalability problems basically refer to the challenges in the blockchain network. These challenges include limited throughput, high fees, and long confirmation times (Carlo R.W., 2023 & Khan, D., et al 2021). Scalability issues can arise when a blockchain network is unable to process enough transactions when there is a significant increase in the number of transactions, leading to slower confirmation and processing times and higher fees (Carlo R.W., 2023). Slow transaction times, high transaction fees and poor user experience may hinder the usability and practicality of blockchain networks, especially for applications that require high transaction volumes (Carlo R.W., 2023 & Khan, D., et al 2021).

Blockchain networks face a fundamental challenge known as the scalability or blockchain trilemma. It refers to the idea that it is challenging to simultaneously achieve three key features of a blockchain system: decentralization, security, and scalability, thus requiring trade-offs to improve scalability

(Carlo R.W., 2023 & Khan, D., et al 2021). The trilemma suggests that obtaining increased scalability would come at the expense of decreased security and decentralization. At the same time, it is critical to remember that only scalability can enable blockchain networks to compete successfully with traditional, centralized platforms (Carlo R.W., 2023 & Khan, D., et al 2021). This trilemma highlights the need to find the right balance between these three critical aspects of blockchain technology being essential for blockchain's growth. It is therefore essential to find a balance between all those three aspects of the blockchain and to consider the requirements of public blockchain applications (Khan, D., et al 2021). The diagram below illustrates the scalability trilemma.

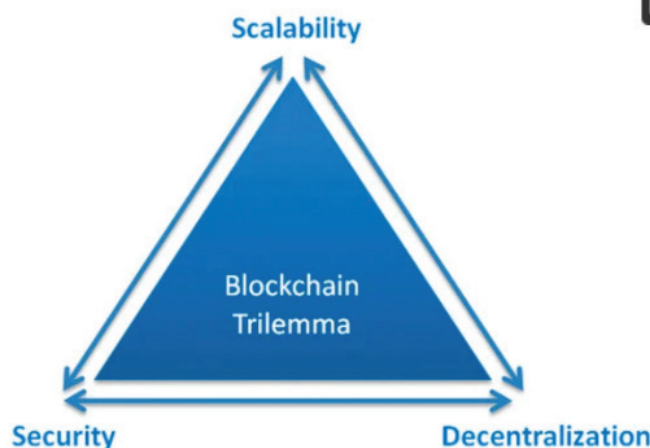


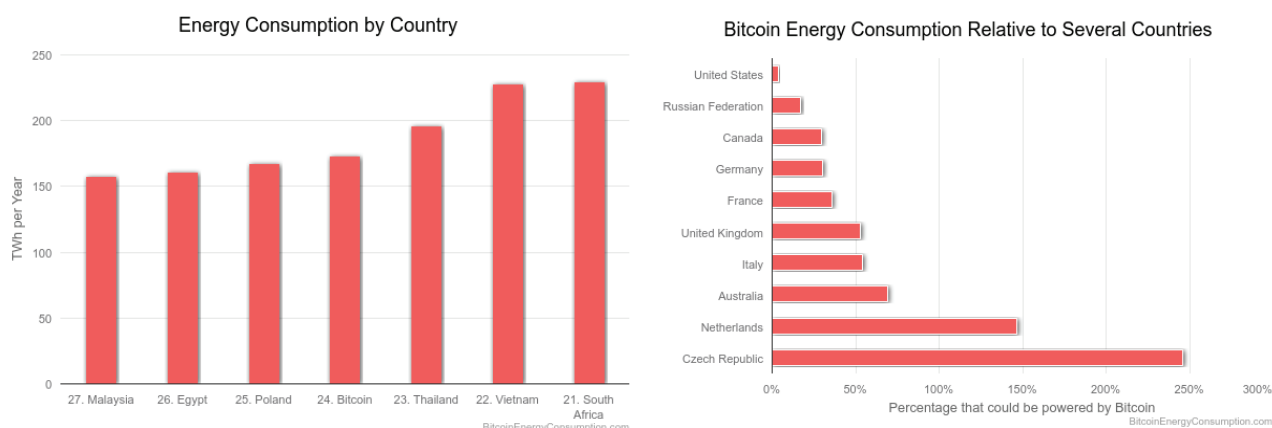
Fig 1: Scalability Trilemma

Given the large volume of data processed by Zimbabwe's telecommunications operators, scalability becomes a pressing issue. For example, in sectors like mobile payments, call detail records, and spectrum allocation, large volumes of data must be stored, analyzed, and audited regularly. Public blockchains may struggle with this volume, leading to slower transaction processing times and potential bottlenecks. Telecommunication operators like Econet process millions of transactions daily through services like EcoCash. Implementing blockchain for regulatory compliance in such high-volume environments may lead to significant slowdowns unless scaling solutions are implemented.

2.3 Energy Consumption and Sustainability

Energy consumption is a significant issue for blockchain technology, particularly those that rely on Proof-of-Work (PoW) mechanisms like Bitcoin. These systems require vast computational power to secure the network, making them energy intensive. The proof-of-work (PoW) algorithm has enabled bitcoin to perform transactions among peers in a trustless distributed decentralized environment. However, while doing this work, miner computers are consuming a huge amount of electrical energy (Monrat, A.A., et al 2019). Zimbabwe's energy supply is inconsistent, with frequent power cuts and it rely on non-renewable sources. Adopting energy-hungry blockchain solutions in the telecommunications sector can exacerbate the country's energy challenges. Zimbabwe's energy sector is already under pressure to meet the demands of households and industries. Adding the energy burden of blockchain-based telecommunication operations may make the situation unsustainable. Other African countries, such as South Africa, have also faced difficulties in adopting energy-intensive blockchain technologies due to energy shortages and high costs (Nsabimana et al., 2021).

According to Bitcoin Energy Consumption Index (2023), the continuous block mining cycle incentivises people all over the world to mine Bitcoin. As mining can provide a solid stream of revenue, people are very willing to run power-hungry machines to get a piece of it. Over the years this has caused the total energy consumption of the Bitcoin network to grow to epic proportions, as the price of the currency reached new highs. The entire Bitcoin network now consumes more energy than a number of countries. If Bitcoin was a country, it would rank as shown below:



Source: Bitcoin Energy Consumption Index 2023

2.4 Data Privacy and Security

Privacy and security in blockchain applications face several significant challenges due to the very nature of the technology. For instance, the immutability of blockchain ensures data integrity but raises concerns over privacy because once data is recorded, it cannot be easily altered or deleted (Fanti & Viswanath, 2018). This is problematic when sensitive personal information is stored on-chain, as it may conflict with privacy regulations like the Data Protection Regulations, which mandates the right to erasure. Zimbabwe's Data Protection Act emphasizes the importance of safeguarding personal information, and this is particularly relevant in the telecommunications sector, which handles sensitive customer data. Additionally, the public nature of blockchains like Bitcoin or Ethereum means that all transactions are visible to anyone on the network, which can compromise user privacy. Although users operate under pseudonyms (public keys), sophisticated data analysis can link these keys back to real identities (Fanti & Viswanath, 2018). This creates tension between the need for transparency and decentralisation and ensuring privacy for users.

The security of smart contracts, another blockchain feature, also poses risks. Smart contracts, once deployed,

are immutable, meaning errors or vulnerabilities in the code can lead to security breaches or exploitation (Eskandari et al., 2018). This creates a significant challenge in ensuring secure code deployment in decentralised applications. Blockchain relies on cryptographic keys for identity verification and transaction security, but losing access to a private key can result in irreversible losses (Eskandari et al., 2018). At the same time, stolen keys can lead to unauthorised access and control of assets. While blockchain offers security advantages like decentralization and encryption, its inherent transparency and immutability present considerable privacy and security challenges. Striking a balance between ensuring user privacy, regulatory compliance, and maintaining blockchain's core functionalities is an ongoing challenge for the industry.

2.5 Regulatory Uncertainty

Regulatory uncertainty poses a significant challenge to the adoption and growth of blockchain technology in Zimbabwe's telecommunications industry. The absence of a clear regulatory framework for blockchain in Zimbabwe creates confusion about how the technology can be used within the telecommunications industry. Without specific legal guidelines, telecommunications companies are uncertain about how to implement blockchain-based innovations while remaining compliant with the law. Zimbabwe has data privacy regulations but lacks a framework tailored to blockchain, therefore there is concern that blockchain could either violate or conflict with existing data protection laws. Zimbabwe's regulatory framework for the telecommunications industry has often been slow to catch up with technological advancements, and blockchain is no exception (Zhou, 2021). This delay discourages telecommunications companies from experimenting with blockchain applications such as smart contracts for inter-operator agreements or blockchain-based automated billing systems.

The lack of a coordinated approach to blockchain regulation between Zimbabwe and other countries complicates the adoption of roaming services and

cross-border data sharing systems (Butcher, 2020). The absence of clear regulatory support for blockchain's role in fraud prevention leaves telecommunications operators uncertain about how to incorporate the technology into their anti-fraud systems (Goredema, 2020). Countries like Uganda and Botswana are similarly grappling with regulatory uncertainty around blockchain, which has slowed adoption in their telecommunications sectors (Nsabimana et al., 2021). Regulatory uncertainty in Zimbabwe's telecommunications industry creates hesitation around blockchain adoption. Addressing these challenges with a comprehensive and flexible regulatory framework would help unlock blockchain's potential for innovation in telecommunications.

2.6 High Transition Costs

Transitioning from traditional systems to blockchain-based solutions requires significant investment, particularly for smaller telecommunications operators. Costs include blockchain infrastructure, staff training, and system integration, which can be financially burdensome for telecommunications operators in Zimbabwe (Nsabimana et al., 2021). Given the country's challenging economic environment, these costs could be prohibitive. Similar financial constraints have been observed in other African nations, such as Ghana, where the high cost of blockchain adoption has deterred smaller telecommunications operators from investing in the technology (Kugonza & Mukisa, 2020). Responsible authorities may introduce financial incentives, such as tax breaks or grants, to encourage telecom operators to adopt blockchain solutions. Alternatively, operators may form consortia to share the costs of blockchain infrastructure and implementation, thereby reducing the financial burden on individual companies.

3. Regulatory Considerations For Blockchain Adoption In Zimbabwe's Telecommunications Sector

3.1 Legal Recognition of Blockchain Records

For blockchain to be fully integrated into Zimbabwe's telecommunications regulatory framework, legal recognition of blockchain-based records, smart contracts,

and audit trails is essential. The current regulatory framework does not explicitly address these technologies, which presents a challenge for operators using blockchain for compliance. Without legal recognition, blockchain records may not be accepted in court or by regulatory bodies. In Ghana, for example, the government has taken steps to recognize blockchain records, creating a more conducive environment for blockchain adoption in its telecom sector (Nsabimana et al., 2021). Responsible authorities should collaborate with lawmakers to draft blockchain-specific regulations that provide legal recognition for blockchain-based records and smart contracts. This would give telecommunications operators the confidence to adopt blockchain for regulatory compliance (ITU, 2022).

3.2 Data Sovereignty and Cross-border Regulations

Zimbabwe's telecommunications operators often engage in cross-border data transfers, particularly when dealing with international telecommunication agreements and mobile money services. Blockchain's decentralised and global nature could conflict with data sovereignty laws that mandate local storage of certain types of data. Zimbabwe should ensure that blockchain solutions comply with these laws while maintaining the benefits of decentralisation. South Africa has implemented strict data sovereignty laws, which have created challenges for cross-border blockchain operations (Mutembei & Kaburu, 2021). Responsible authorities should develop guidelines that clarify how blockchain can be used while adhering to Zimbabwe's data sovereignty laws. Collaborating with regional regulatory bodies may also help harmonize cross-border blockchain operations.

3.3 Consumer Protection

Blockchain's complexity and immutability pose risks to consumers, particularly regarding data accuracy and dispute resolution. In the event of an error in a blockchain record (such as incorrect billing), it can be difficult to alter or correct the data. This may lead to consumer dissatisfaction and potential legal challenges. Responsible authorities should introduce consumer protection regulations specifically for blockchain-based services, ensuring that telecommunication operators provide mechanisms for dispute resolution and data rectification (Chirume & Nyemba, 2023). This may include the introduction of off-chain mechanisms for error correction, ensuring consumer rights are protected.

4. Conclusion And Recommendations

Blockchain offers significant potential to enhance regulatory compliance in Zimbabwe's telecommunications sector by improving transparency, security, and operational efficiency. However, the challenges associated with interoperability, scalability, energy consumption, data privacy, regulatory uncertainty, and transition costs must be carefully managed to ensure successful adoption. Addressing these issues is essential for leveraging blockchain's full potential and fostering an innovative regulatory landscape.

Key Recommendations

- Develop a comprehensive legal framework to enable the seamless integration of blockchain technology. This framework should outline the permissible use of blockchain in telecommunications, define data privacy standards specific to decentralized systems, and establish guidelines for the use of digital assets within telecom services. Regulatory certainty will not only provide telecom operators with the confidence to adopt blockchain but also attract investment and foster innovation in the sector.
- Encourage collaboration among telecommunications operators, technology providers, and regulatory bodies is essential to overcome technical challenges and develop interoperable solutions. POTRAZ may facilitate forums and workshops where industry stakeholders can share best practices, discuss technical

hurdles, and pilot blockchain-based projects in a controlled environment. This collaborative approach will allow stakeholders to align their efforts and create standardized solutions that benefit the entire industry.

- Implement scalable and energy-efficient solutions. Scalability and energy consumption remain significant barriers to blockchain adoption. To mitigate these challenges, the telecommunications sector may explore blockchain platforms that use energy-efficient consensus mechanisms.
- Invest in technical expertise and infrastructure to build the necessary technical expertise crucial for a successful transition to blockchain-based solutions. The government should fund research, providing training programs and technical workshops to enhance the knowledge of telecommunications professionals about blockchain technology and its applications. Additionally, investments in infrastructure, such as secure data centers and reliable energy sources, will support the deployment of blockchain solutions and ensure consistent performance.
- Blockchain's immutable nature poses unique challenges to data privacy, especially in light of data protection regulations. To address these concerns, POTRAZ may develop specific guidelines that reconcile blockchain's transparency with the need for data privacy. Approaches such as zero-knowledge proofs and permissioned blockchains can provide transparency while safeguarding sensitive information.
- Transitioning to blockchain technology may involve significant initial costs, which can be a deterrent for telecom operators. The government may provide financial incentives or subsidies to encourage the adoption of blockchain-based systems. This support may come in the form of grants for pilot projects, tax incentives for early adopters, or public-private partnerships aimed at reducing the financial burden of implementation..

5. REFERENCES

- Bitcoin Energy Consumption Index., 2023. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjpgCd1KGJAxWzQ_EDHRR0MysQFnoECBMQA-Q&url=https%3A%2F%2Fdigiconomist.net%2Fbitcoin-energy-consumption%2F&usg=AOvVaw1mn-WOVlmlWVBTCzVl1upy&opi=89978449
- Butcher, J., 2020. Global regulatory approaches to blockchain. *International Law Review*, 18(1), 23-45.
- Carlo R.W. De Meijer 2023. Blockchain and the scalability challenge: solving the blockchain trilemma. Available at: <https://www.google.com/url?>
- Chirume, M., & Nyemba, S., 2023. Exploring the Legal Framework for Blockchain Technology in Zimbabwe. *Zimbabwe Legal Journal*, 12(3), 45-58.
- Eskandari, S., Clark, J., Barrera, D., & Stobert, E., 2018. A first look at the usability of bitcoin key management. In *NDSS Workshop on Usable Security (USEC)*.
- Fanti, G., & Viswanath, P., 2018. Anonymity vs. privacy: Challenges in decentralized networks. In *Communications of the ACM*, 61(10), 35-37.
- Gabriel Kabanda., 2021. Model Structure for Block Chain Technology and Cryptocurrency for the financial services sector in Zimbabwe. Zimbabwe Academy of Sciences, University of Zimbabwe Harare, ZIMBABWE: <http://orcid.org/0000-0001-6699-080X>
- Ghaemi, S., Rouhani, S., Belchior, R., Cruz, R.S., Khazaei, H. and Musilek, P., 2021. A pub-sub architecture to promote blockchain interoperability. *arXiv preprint arXiv:2101.12331*.
- Goredema, P., 2020. Blockchain for fraud prevention in telecommunications. *Zimbabwe Telecom Review*, 9(2), 102-117.
- ITU., 2022. Blockchain Technology and Telecommunications: Regulatory Challenges and Recommendations. International Telecommunication Union. Retrieved from <https://www.itu.int/>
- Kaur, M. and Lnu, N., 2022. Ethereum, Hyperledger and Corda: A Side-by-Side Comparison of Capabilities and Constraints for Developing Various Business Case Uses. In *The Auditor's Guide to Blockchain Technology* (pp. 105-126). CRC Press.
- Khan, D., Jung, L.T. and Hashmani, M.A., 2021. Systematic literature review of challenges in blockchain scalability. *Applied Sciences*, 11(20), p.9372.
- Kugonza, A., & Mukisa, J., 2020. Blockchain Adoption in Africa: Opportunities and Challenges. *African Journal of Digital Innovation*, 8(2), 21-34.
- Madine, M., Salah, K., Jayaraman, R., Al-Hammadi, Y., Arshad, J. and Yaqoob, I., 2021. appxchain: Application-level interoperability for blockchain networks. *IEEE Access*, 9, pp.87777-87791.
- Monrat, A.A., Schelén, O. and Andersson, K., 2019. A survey of blockchain from the perspectives of applications, challenges, and opportunities. *IEEE Access*, 7, pp.117134-117151.

- Mutembei, R., & Kaburu, G., 2021. Data Privacy Regulations and Blockchain in Africa: A Case of Kenya and South Africa. *African Data Protection Review*, 5(1), 33-48.
- Nsabimana, J., Kamugisha, R., & Mugabe, J., 2021. Blockchain Integration in Africa's Telecommunications Sector: Regulatory Challenges and Technological Hurdles. *Journal of African Telecommunications*, 7(4), 57-65.
- Zhou, K., 2021. Navigating regulatory lag: Blockchain in Zimbabwe. *Technology and Policy Quarterly*, 7(3), 88-104.



EXPERT INTERVIEW: PROF. TAWANDA MUSHIRI



Professor Tawanda Mushiri

Who is Prof Tawanda Mushiri

Prof. Tawanda Mushiri is an Associate Professor in Artificial Intelligence, Medical Robotics and Biomedical Engineering. He is the Executive Director – Technical for **Scientific and Industrial Research and Development Centre (SIRDC)** Zimbabwe managing 12 institutes. SIRDC was established in February 1993 by the Government of Zimbabwe through the Research Act [Chapter 10:22]. Its mandate is to carry out strategic Research & Development for the benefit of the manufacturing, service, agricultural as well as to commercialize the Research & Development outputs. For more information check here <https://sirdc.ac.zw/management/>

Interview

General Understanding of Blockchain in Telecommunications.

1. Can you briefly describe how you see blockchain technology transforming the telecommunications industry, particularly from a regulatory compliance perspective?

Blockchain is a distributed database or ledger technology that enables transparent and secure information sharing across a network of computers. Each record, or “block,” is linked to the previous one, forming a chain that ensures the integrity of the data stored. Because of the decentralized, transparent, and immutable nature of blockchain, it has the potential to revolutionize our telecommunications sector by enhancing security, efficiency, and compliance.

I will give a few examples. In recent news, sim swapping, where a scammer takes control of someone else’s phone number by tricking the mobile carrier company into transferring the number to a SIM card that they own, has become common place. Blockchain can put an end to this kind of fraud. With the promulgation of the Data Protection Act Chapter 11:23, Act 5 of 2021, the government of Zimbabwe is putting emphasis on data protection and privacy. The telecommunications industry is one area that holds a lot of such private data, you think of a person’s biodata, physical address, real-time location, etc. Blockchain has the potential to help telecom operators comply with regulations related to data privacy and customer protection. There are several other advantages such as ensuring network neutrality and even simplifying data handling for the operators. This is not just a hypothetical assumption, there are companies that have tried it and met with success. An example is T-Mobile in the USA, they collaborated with Intel to create a blockchain database for internal use.

In a nutshell, blockchain can enhance transparency while guaranteeing customer data privacy and protection, improve traceability, reduce fraud and simplify reporting for telecoms companies.

2. What do you think are the key advantages of using blockchain over traditional methods for regulatory compliance in telecom?

It provides enhanced transparency, traceability, efficiency, security, and trust. By automating processes, reducing overhead, and ensuring data privacy, blockchain can help telecom companies streamline their compliance efforts, reduce costs, and build stronger relationships with customers and regulators.

Data Integrity and Security

3. How can blockchain enhance data integrity and security in telecom compliance processes, especially when dealing with sensitive customer and operational data?

Blockchain technology significantly enhances data integrity and security in the telecommunications industry through its decentralized architecture, which eliminates single points of failure and reduces the risk of unauthorized access and data tampering. By employing advanced cryptographic techniques, blockchain ensures that any alterations to data are easily detectable, thereby safeguarding sensitive customer information. The use of consensus mechanisms, such as Proof of Work or Proof of Stake, validates transactions and prevents fraudulent activities, while real-time data accuracy allows telecom companies to maintain reliable and up-to-date information.

4. From a technical standpoint, what specific features of blockchain do you believe are most beneficial in securing data within a telecommunications network?

Blockchain offers several key features that can significantly enhance data security within telecommunications networks. Its decentralized nature reduces the risk of data breaches by distributing information across multiple nodes, while immutability ensures that once data is recorded, it cannot be altered without consensus, maintaining accurate and tamper-proof logs. The transparency and auditability of blockchain enable real-time monitoring, making it easier to detect fraud and unauthorized access. Moreover, smart contracts can automate processes such as service provisioning and billing, ensuring secure and auditable transactions. Enhanced authentication through cryptographic techniques protects against unauthorized access, and the use of cryptographic hashing ensures data integrity by linking blocks securely. The resilience to attacks provided by its distributed structure makes compromising the network significantly more challenging, while interoperability among different systems can facilitate secure data exchange across networks.

5. Do you think blockchain can adequately address concerns regarding data breaches and unauthorized access in telecommunications? If so, how?

Blockchain does have significant potential to address data breaches and unauthorized access in telecommunications. Through its immutable ledger system, it ensures that data cannot be altered or deleted once recorded. This reduces the risk of data breaches and unauthorized modifications. Blockchain can also be used to create secure digital identities, thereby reducing the risk of identity theft and unauthorized access. However, like any other technology, its implementation is not without challenges. The regulatory landscape for blockchain globally is still evolving, and compliance can present a significant hurdle. Its implementation also requires specialized knowledge, which as a country, we may need to invest in. By addressing these issues, our telecoms industry stands to benefit from this cutting-edge technology.

Audit Trails and Reporting

6. What role do you think blockchain can play in improving the auditability of telecom operations, particularly in areas like billing, fraud prevention, and customer data management?

By providing a decentralized and immutable ledger, blockchain ensures that all transactions, such as billing records and service usage, are securely recorded and cannot be tampered with. This transparency allows for real-time auditing, enabling operators to track and verify transactions easily, which is crucial for accurate billing and dispute resolution. In terms of fraud prevention, the ability to maintain a single source of truth helps eliminate discrepancies and reduces the potential for fraudulent activities, as every transaction can be traced

back to its origin. Additionally, blockchain enhances customer data management by allowing customers to have greater control over their personal information, with secure access and consent mechanisms built into the blockchain. This ensures compliance with data protection regulations and fosters trust between telecom providers and their customers. Overall, the integration of blockchain technology in telecom operations significantly strengthens auditability and accountability, leading to improved operational efficiency and customer satisfaction.

7. How can blockchain-based solutions simplify and automate regulatory reporting in telecommunications? Can you provide examples of current use cases?

By providing a single, immutable ledger for all transactions and data exchanges, blockchain ensures that data is consistent, it is accurate, and easily accessible for regulatory purposes. This allows telecom companies to efficiently and timeously compile and submit reports to regulatory bodies. This can even be done in real-time. Because it uses smart contracts, it can automate many aspects of reporting by self-executing and collecting, verifying, and reporting data as required, which reduces manual data entry and at the same time minimize human error. This in turn enables continuous auditing and compliance checks, allowing telecom companies to maintain compliance proactively rather than relying on periodic audits by POTRAZ, thus preventing potential compliance issues. To the advantage of the telecom companies, automating these processes can reduce compliance costs by minimizing the need for third-party internal auditors and decreasing the time spent on manual tasks. Another area where blockchain has been used with success is managing records. Given that telecommunication industry involves many different players, like telecom companies, infrastructure providers, and third-party services, there are various records and databases that need to be managed. Distributed ledger technology, an extension of blockchain techniques, has proved to be a handy solution.

8. Could you explain how blockchain creates immutable audit trails and how this might enhance transparency for telecom regulators?

Immutable audit trails are created through the unique structure of blockchain technology. Each transaction is time-stamped and linked to the previous one, forming a chain of blocks. This means that once data is recorded, it cannot be altered or deleted without altering all subsequent blocks. Of which that would require consensus from the network participants. What that means in a telecom context is that there will be a permanent, tamper-proof and verifiable record of all transactions and activities within the telecommunications network. It makes it easier for oversight audits and conversely build trust among all stakeholders involved.

Case Studies

9. Are there any telecommunication companies or projects you are aware of that have successfully implemented blockchain to improve regulatory compliance? What results or benefits have they observed?

An India based company called Coforge developed a blockchain solution to streamline number portability. Number portability is a service that allows you to keep your existing phone number when you switch from one telecommunications provider to another. They reported that their solution has improved the efficiency, security, and transparency of the customer experience. This is just one example that shows the potential that blockchain has in revolutionizing telecommunications.

10. Can you provide insights into how blockchain has been used to address specific regulatory challenges, such as roaming agreements or inter-carrier settlements?

Deutsche Telekom, from Germany, has used blockchain to streamline the otherwise complex process of es-

establishing and managing roaming agreements. They found that it reduced the time required to finalize these agreements and minimized disputes through a transparent, immutable ledger. Closer to home, Vodafone teamed up with Deutsche Telekom and Telefonica, and they were exploring the use of blockchain to speed up their inter-carrier settlements.

11. How do blockchain-based telecom projects in your experience compare in terms of success when it comes to regulatory compliance?

Blockchain-based telecom projects have generally shown greater success in enhancing regulatory compliance compared to traditional methods. Companies using blockchain reported faster and more transparent processes.

Challenges and Considerations

12. What do you see as the biggest challenges telecommunication companies face when adopting blockchain for regulatory compliance? Are these technical, regulatory, or operational challenges?

The challenges are multifaceted. On the technical side there is the complexity of integrating blockchain into the already existing legacy systems. Our telecom companies have long-standing billing and operational systems that may not easily connect with new blockchain solutions, which will require substantial adjustments and investments. On the regulatory end, the governance of blockchain, relatively new as it is, is still evolving and hence there are some uncertainties to deal with. Operationally, blockchain will need certain skills. The question is, are those skills already there in the telecom companies?

13. In your opinion, how ready are regulatory bodies to embrace blockchain technology in telecommunication compliance? What needs to change for widespread adoption?

Conversations around these cutting-edge technologies are getting louder in corridors. This means that various stakeholders are beginning to realize the potential that is there. In my opinion, regulatory bodies are currently at a cautious stage, where they see the advantages that blockchain has but are not really sure of how to deal with the possible challenges it presents. In order to successfully implement blockchain, there is need for clear regulatory frameworks, collaboration between stakeholders, training to close the skills gap and thorough pilot programs to ensure that robust testing before full implementation. As a nation, we may also need to channel more funds towards research and development in this area. The will is already there, as can be seen in recent efforts, it's perhaps a question of just finishing what has been started.

14. What are the potential legal concerns surrounding blockchain's immutability, particularly with regards to data privacy regulations like GDPR or data localization laws?

Article 17 of the GDPR guarantees the right to erasure, also known as the right to be forgotten. This means that if an individual requests to have their personal data deleted, it should be granted without reservation. Similarly, our own Data Protection Act, section 8, entitles data subjects with the same right. However, blockchain's immutable nature makes it challenging to delete data once it's recorded. The GDPR, again, also requires that only necessary data be collected and processed. This is not the case with blockchain, every transaction is recorded. Additionally, Blockchain networks often operate across multiple jurisdictions, complicating compliance with data localization laws that require data to be stored within specific geographic boundaries.

15. How can blockchain solutions in telecommunication deal with regulatory differences between countries, especially for cross-border data sharing?

It starts right from the architecture. The blockchain solutions may be designed such that they adjust and comply with the various jurisdictions. For instance, different modules may be created for different legislations. The smart contracts may also be used to enforce compliance rules automatically, ensuring that data handling adheres to local regulations. Additionally, sensitive data can be stored on private blockchains within specific jurisdictions, while less sensitive data can be shared on public blockchains.

Regulatory and Policy Insights

16. What policy changes or regulatory frameworks would you recommend to facilitate the adoption of blockchain in telecommunication compliance?

Comprehensive legislation will need to be developed, as an extension to what we already have, explicitly covering issues like cross-border sharing and the blockchain technology itself. It may also help to create regulatory sandboxes, established by a legal instrument, to allow telecom companies to test their solutions in a controlled environment that simulates the real-time. This will ensure compliance before rolling out their solutions.

17. How can telecommunication operators collaborate with regulators to develop blockchain-based solutions that meet compliance requirements?

The best way is dialogue, regular communications between the telecom operators and the regulator to discuss, specifically, blockchain initiatives, share insights and address concerns. This can be facilitated through workshops and seminars. The regulatory sandbox I mentioned earlier also proffers such collaboration and feedback loops. Joint task forces can also be formed in coming up with regulations, monitoring and implementing this technology.

18. How do you see the role of regulatory sandboxes or pilot projects in testing blockchain for telecom compliance before full-scale implementation?

Regulatory sandboxes go a long way in mitigating risk and providing feedback. They also stimulate innovation and stakeholder collaboration. The proof of concept is done to ensure viability and scalability before taking the solution to market.

Future of Blockchain in Telecom Compliance

19. Looking ahead, where do you see the most promising opportunities for blockchain in telecommunication compliance over the next five years?

The quick returns of blockchain technology lie in fraud prevention, automated compliance and audits. This means there will be more transparency, trust and compliance from all players. On the other hand, the telecom operators will be able to lower their costs as more manual processes become automated which by ripple effect will give room to lower product and service prices to the consumers.

20. In your view, will blockchain become a standard technology for regulatory compliance in the telecom sector? If so, what factors will drive this shift?

Blockchain is a great technology that if implemented right stands to significantly benefit the telecom industry. With its enhanced transparency, enhanced security and cost efficiency, it is an attractive solution. Sooner or later, it may become the convention. What is key is to ensure that the challenges associated with its adoption are adequately addressed, the risks mitigated and the advantages maximized.

I THANK YOU



'creating a level playing field'

1110 Performance Close
Mt Pleasant Business Park
P.O. Box MP843
Mount Pleasant
Harare,
Zimbabwe

tel: +263 242 333032

fax: +263 242 333041

toll free: 0800 4303

e-mail: the.regulator@potraz.gov.zw

web: www.potraz.gov.zw

Facebook: @POTRAZ

Twitter: @POTRAZ

EDITORIAL COORDINATION:

Professor Maxwell Sandada-POTRAZ

Rumbidzai Panavanhu-POTRAZ