“Navigating the Blockchain Landscape, Efforts to Demystify Distributed Ledger Technologies”

Authors: Mariana de la Roche (IOTA & INATBA) & Asa Dahlborn (IOTA) with the comments of Mar Meneses (Co-Chair of INATBA Education Working Group) and the support of the members of the Education Working Group of INATBA, the European Blockchain Observatory and Forum- EUBOF and Blockchain Bundesverband.

Addressing misconceptions in the blockchain and Distributed Ledger Technology (DLT) space is vital to achieve global scalability, allowing consumers and users to have informed decision-making processes, while also promoting trust and effective risk management. Individuals, businesses, and policymakers must understand these technologies to make strategic decisions, whether for investing, implementing a solution, or developing regulations.

Misconceptions often come from a combination of incomplete or simplified information, miscommunication, inappropriate generalisations, confirmation bias, and lack of contextual understanding. In complex subjects, such as blockchain the simplification of details for easier comprehension can unintentionally lead to partial or incorrect understanding. Misconceptions can lead to mistrust or misuse, hindering widespread adoption. Therefore, dispelling misconceptions ensures a safer and more effective use of these innovative technologies while also generating more trust and understanding in the general population, which can later on help to increase adoption worldwide.

Recognising the prevalence of misconceptions in the blockchain and DLT space, we are committed to advocate for blockchain education as it is important to help users, developers, businesses, and policymakers better understand and effectively leverage the potential of DLT, ultimately fostering a safer and more innovative blockchain ecosystem.

This paper presents and addresses some of the most common misconceptions about blockchain.

“All blockchain are the same”

Many people who are new to the concept of blockchain may not be aware of the variations and complexities of different blockchain networks. They may also be unaware that the technology can be adapted and customised for a variety of applications beyond just crypto assets.

Moreover, blockchain is part of a family of technologies named DLT which stands for Distributed Ledger Technology and it's a broader term that encompasses blockchain and other types of digital systems for recording transactional data across multiple sites, countries, or institutions without a central administrator or centralised data storage. **A blockchain is a type of DLT, but not all DLTs are blockchains**.

The main difference between them lies in how the data is structured. A blockchain organises data into 'blocks,' which are then 'chained' to each other in a linear, chronological order using cryptographic links. In contrast, other types of DLT may not necessarily organise or link data in the same way for example′, the IOTA Foundation uses a DAG called “Tangle”.

Furthermore blockchains can be different according to the consensus mechanism they have. This is the method by which a blockchain network agrees on the state of the distributed ledger. On one hand, Proof-of-Work (PoW), is a process that involves solving complex mathematical problems, while on the other hand, Proof-of-Stake (PoS), is a process where validators are chosen to create a new block based on the amount of cryptocurrency they hold and are willing to 'stake' as collateral. Moreover, there are other consensus mechanisms including Delegated Proof of Stake (DPoS), Proof of Authority (PoA), and Byzantine Fault Tolerance (BFT), each with its unique attributes.

Last but not least, it is important to consider that different blockchains can process different amounts of transactions per second (tps). For instance, Bitcoin can process around 7 tps, Ethereum can handle about 15-20 tps, the IOTA mainnet allows for approximately 1000 tps and Hedera’s native services can scale to 10 000 tps.

“All DLTs are publicly available and everyone can interact without permission”

While DLTs are commonly thought of as decentralised, public ledgers, DLTs can in fact be both public or private. DLT can be categorised into two main types: permissioned and permissionless.

- **Permissionless (or public) DLT**s: are indeed open to the public and allow anyone to participate in the network, create transactions, validate transactions (i.e., mining in case of PoW, validating in case of PoS), and view transaction history.

- **Permissioned (or private) DLT**s: require an invitation and must be validated by either the network starter or a set of rules put in place by the network starter. Examples include Hyperledger Fabric or R3's Corda. These systems are used typically by consortiums to efficiently process transactions or maintain a shared database.

So, not all DLTs are publicly available, and not everyone can interact with them without permission. This depends on the specific design and use case of the DLT.

"Blockchains are for big-data storage"

Despite blockchain technology's transformative potential, a common misconception exists: its efficacy for big-data use cases. This error arises from a misunderstanding of the inherent scarcity of computing resources in Distributed Ledger Technology (DLT) systems. To create an expansive network, the requirements of each individual node, including storage demand, must be minimized. As a result, resources such as throughput, computation, and storage become scarce due to the architectural preference for decentralization. Thus, the very nature of blockchain's design, constrains its ability to process large data volumes efficiently, directly countering the idea that it's well-suited to store vast amounts of data on-chain.

However, it's crucial to highlight that despite these limitations, blockchain technology still has a role to play in big-data scenarios. Notably, blockchain excels in preserving small yet essential pieces of information, such as hashes or digital signatures. These elements are pivotal in authenticating the integrity of data stored off-chain, effectively contributing to data security and trustworthiness. Furthermore, numerous projects are investigating decentralised file storage systems. While these systems diverge from traditional blockchain architectures, they can be used synergistically with a blockchain to enhance its applicability. Consequently, even though blockchain technology may not be the ideal solution for total big-data storage, it can still contribute significantly to securing and validating data within these environments.

"Blockchain consumes a lot of energy"

One common misconception about blockchain technology is that it consumes a significant amount of energy. While it is true that some blockchain networks, such as Bitcoin, do require substantial computational power and energy consumption, it is important to consider the broader context and potential benefits.

- **Energy Efficiency Improvements**: Many newer blockchain platforms and protocols are actively working on improving energy efficiency. For instance, there are Proof-of-Stake (PoS) consensus mechanisms that consume significantly less energy compared to traditional Proof-of-Work (PoW) algorithms used by Bitcoin. These advancements

reduce the environmental impact of blockchain technology. A study by the IOTA Research team found that the upcoming IOTA 2.0 prototype consumes significantly less energy than other DLTs. Built on a directed acyclic graph (DAG) architecture, IOTA 2.0 implements a novel access control algorithm that requires less energy by avoiding Proof of Work (PoW). According to tests on the prototype software GoShimmer, a single transaction on IOTA 2.0 uses less energy than lighting a festive light for a second. This research is promising for future energy consumption reductions in DLTs. The low energy use of IOTA 2.0 confirms its minimal environmental impact and its suitability for digital sustainability solutions.

- **Comparative Energy Consumption:** It is essential to compare the energy consumption of blockchain systems with the existing financial and banking infrastructure they aim to disrupt. Traditional financial systems involve numerous intermediaries, centralised databases, and physical infrastructure that also require substantial energy consumption. Blockchain technology, with its potential to streamline processes and eliminate intermediaries, may ultimately result in overall energy savings.

- **Renewable Energy Integration:** The growing awareness of environmental concerns has led to increased efforts to power blockchain operations using renewable energy sources. Some blockchain projects and mining operations are actively seeking ways to rely on green energy, such as solar or wind power, to mitigate their carbon footprint.

- **Off-Chain Solutions:** Not all transactions and processes need to occur directly on the blockchain. Off-chain solutions, such as payment channels and layer-two protocols, allow for faster and more energy-efficient transactions by reducing the computational burden on the blockchain. These solutions strike a balance between scalability, efficiency, and energy consumption.

"Blockchain / DLT and crypto are the same"

While all cryptocurrencies have their own DLT, not all DLTs use cryptocurrencies. DLT is the technology that enables the existence of cryptocurrency, but this technology has potential applications way beyond just cryptocurrencies. Use cases around supply chain tracking, voting systems, and self sovereign identities are a few examples.

It is important to note that DLTs are decentralised and distributed digital systems that record transactions across many computers in such a way that the registered transactions cannot be altered retroactively, while cryptocurrencies are digital or virtual forms of currency that use cryptography for security. The term 'cryptography' basically refers to tokens or currencies themselves, rather than the technology they are built on.

“Blockchain is more used than Cash for money laundering”

This misconception is mostly due to the fact that blockchain is often erroneously perceived as completely anonymous; this derives from the misconception that blockchain transactions are completely anonymous which largely contributes to the misunderstanding that blockchains can be used to conceal illicit activities. However the space counts with tools such as blockchain analytics that aid in identifying patterns and anomalies in transaction data that could signify activities like money laundering or terrorism financing. These tools can trace the flow of funds within the blockchain and DeFi ecosystem, spanning different decentralised applications and protocols. Furthermore, innovative solutions like Self-Sovereign Identity (SSI) and Decentralised Identifiers (DID) offer efficient, secure authentication methods for identification both in off- and on-chain applications. Such solutions allow service providers to meet their legally mandated Know Your Customer (KYC) obligations while offering their customers secure, user-friendly, and privacy-conscious authentication mechanisms. IOTA Foundation, for example, refers to this as "identity on demand" which implies that a Crypto Assets Service Provider - CASP has the ability to reveal the identity of authenticated subjects when requested by an authorised party (e.g. law enforcement) in case of a legitimate claim.

Moreover this misconception also has its roots in high-profile cases of illegal activities involving cryptocurrencies, such as ransomware attacks demanding payment in Bitcoin, or dark web marketplaces dealing in cryptocurrencies, that gained significant media attention. This reinforces the perception of cryptocurrencies being closely associated with illicit activities, even when they are not the majority of the cases. Finally, the complexity and novelty of blockchain technology can lead to misunderstandings, particularly among individuals that are not well-versed in the technology.

It is important to note however, that this assumption is unjustified, considering that cash remains the most common medium of exchange used in money laundering. According to the United Nations, roughly $800 billion to $2 trillion of fiat is used for laundering yearly while the respective use of Crypto in 2022, according to Chainanalysis, was close to $23.8 Billion.

“Custody is good / Custody is bad”

When discussing the custody of crypto assets, the question is not whether custody is good or bad, but rather what advantages and disadvantages custody comes with and the priorities of each user.

Custodial crypto wallets are hosted by a service provider (e.g. an exchange), as opposed to managed by yourself. The custodians of the hosted wallets offer a service by hosting the wallet and are responsible for your private keys. Since the private keys are required to prove ownership

and hence access and spend the funds, this means that you rely on an intermediary that is responsible for your keys and how they are stored. Custodial wallets are often managed by centralised exchanges that tend to store information of their customers both online and offline. Needless to say, pools of funds of numerous users are obviously a more attractive target for hackers than individual self-hosted wallets.

But while it might sound good to be responsible for your own keys from a security perspective, it is a bit trickier if something happens to them due to your own mistakes. With a self-hosted wallet, you are the one and only person in charge of your private keys, and this applies if you lose them as well - then there is no one that can help you recover them. The service offered by wallet custodians covers such situations with back-ups that allow you to access your funds again. Many also prefer custodial wallets due to the user experience. Self-hosted wallets can be quite overwhelming for someone with no technical background while the exchanges that host wallets offer an easier and more intuitive user interface.

Something else to take into consideration in the comparison between custodial and non-custodial wallets is the regulatory aspect. Custodians use processes such as Know Your Customer (KYC) and oversee and control the transactions of their users in order to comply with Anti-Money Laundering and other regulatory policies. A self-hosted wallet functions on a peer-to-peer basis, which means that transactions are free of monitoring from a third party.

In summary, the custodial vs. non-custodial wallet choice boils down to a trade off between user-friendliness and service - advantages typically offered by custodial wallets, and security and control - the advantages of non-custodial wallets.

"DLTs are only usable for payments and NFTs"

The crypto boom gave birth to the common misconception that blockchain/DLT is synonymous to crypto assets, and consequently the erroneous idea that the use of DLT is limited to payments and NFTs. In fact, DLT transactions do not even need to have any value at all. Any kind of data, for example the temperature in a room at a given time or the time at which a certificate was issued, can be recorded on DLTs. This opens up a countless number of use cases in any scenario that benefits from traceability and transparency. DLT can be used in a broad array of sectors, such as supply chain management, healthcare, real estate, carbon credits, transparent donations, digital identity, and many more. Its decentralised nature allows for transparency, immutability, and security, which can be harnessed to solve complex and systemic problems and create efficiencies in numerous industries. The versatility of DLT contributes to its disruptive potential and makes it a promising technology for future innovation, especially in supply chains. The Trade Logistics Information Pipeline (TLIP) is a good example of how DLTs can address shortcomings and increase efficiency in the global trade supply chain.

"DLT transactions are anonymous (or non-transparent)"

DLT transactions - especially crypto asset transactions - are often criticised for allowing anonymous or non-transparent transactions and thus facilitating illicit transactions and money laundering. Compared to traditional finance systems where transactions are tied to details such as names and account numbers of the parties involved in the transaction, transactions made on a distributed ledger provide less intuitively understandable information about those involved. But saying that transactions made on a distributed ledger are anonymous and non-transparent is misleading. DLTs use pseudonyms in the form of a combination of letters and numbers to record transactions. This string of numbers and letters is the pseudonym of your public address, which is comparable to your account number when you do a banking transaction. While these addresses are linked to crypto wallets rather than the actual identity of the trader, the transactions are recorded on a distributed ledger that generally is public. Hence, it is not correct to claim that DLT transactions are *anonymous* but rather *pseudonymous.* In fact, authorities in many regions have made KYC mandatory, which then even enables tracing of the identity tied to the wallet's owner. With regards to transparency, there is not much fact to support the statement that DLT transactions are non-transparent. A distributed system with public access provides a higher degree of transparency than transactions made through a centralised banking system as is the most common case in traditional finance. Moreover, the immutability of DLT systems ensures that transactions made on DLTs have not been tampered with.

"Every DLT is secure by default"

DLTs, including blockchains, do inherently feature certain security elements by virtue of their design. For instance, the use of cryptographic techniques provides some assurance of data integrity and authentication. Also, the distributed nature of these technologies, which involves maintaining multiple copies of the ledger across different nodes, makes it harder (but not impossible) for a single malicious actor to alter the records. While DLTs possess inherent security properties, they are not universally secure by default. The security of a DLT is influenced by many factors and needs to be continuously assessed and strengthened in response to emerging threats and vulnerabilities.

There are multiple factors that can influence the security of a DLT, including:

- **Consensus Mechanism:** This is the method a DLT uses to validate and confirm transactions. Different mechanisms offer varying degrees of security. For instance, the Proof of Work mechanism used by Bitcoin is generally considered secure but can be susceptible to a '51% attack', where an entity controlling the majority of the network's mining hash rate could manipulate the transactions.

- **Smart Contracts:** Many DLTs make use of smart contracts, self-executing contracts with the terms directly written into code. These can introduce security risks if they contain bugs or vulnerabilities, as seen in the DAO hack on the Ethereum network in 2016.

- **Network Size and Distribution:** The security of DLTs often relies on the number and distribution of nodes in the network. A larger, more decentralised network can be more secure than a smaller, centralised one. Smaller networks can be more vulnerable to Sybil attacks, where an attacker subverts the reputation system of a network by creating a large number of pseudonymous identities.

- **Protocol Design:** The overall design of the DLT protocol and its updates can introduce security vulnerabilities. Also, if the codebase is not open-source, it may not be subject to the same degree of peer review and auditing, potentially leaving unnoticed vulnerabilities.

- **Operational Security:** The security practices of the individuals and organisations operating the nodes can also impact the overall security of the DLT. This includes aspects like key management, software patch management, and response to incidents.

"Everything but Bitcoin is a scam"

Categorising all other cryptocurrencies and blockchain projects as scams is inaccurate and oversimplified. There are thousands of cryptocurrencies other than Bitcoin, many of which are legitimate projects with unique features, applications, and community support. For example, Ethereum is a well-established cryptocurrency and blockchain platform that supports smart contracts and decentralised applications (dApps). Other projects like IOTA (MIOTA), Binance Coin (BNB), Cardano (ADA), and Polkadot (DOT) also have distinct use-cases and substantial communities.

Moreover, blockchain technology itself has a wider range of applications beyond cryptocurrency. It is being explored and adopted in numerous industries, for its potential to provide transparency, security, and efficiency, including supply chain management, healthcare, finance, carbon markets and more.

For investors and consumers, it is important when looking at cryptocurrencies and projects to examine factors such as the project's team, the technology, the use case, and regulatory compliance among others.

"NFTs are only good for art"

Although the role of NFTs in art is important, their potential use cases extend far beyond the arts &culture sector. Below some examples to illustrate the variety of NFT trends and use cases as a demonstration of their utility for the economy:

- NFTs can improve transparency around ownership, authenticity, and remuneration for goods and services.

- Relevant value of NFTs (and blockchain technology in general) in developing digital skills and education. Given that there are over three billion estimated gamers worldwide, the potential for the gaming sector to draw young people into the digital economy is an opportunity to encourage younger generations to become innovators and entrepreneurs in digital solutions.

- NFTs disrupt the monopoly of big tech in Web2, where tech giants own digital objects and content like books and music instead of the individual. With NFTs, creators can reclaim ownership of their digital assets and avoid intermediary gatekeepers such as the Apple store, Facebook, or Amazon, who take large percentages of sales. NFTs empower individuals to exercise sovereignty over their digital objects and support the creator economy.

- NFTs can capture the intangible value and consumer goodwill of brands. Brands can create digital objects for their fans as a way of finding new revenue streams and engaging with their audiences through digital assets.

“Tokens are stored in wallets”

"Tokens are stored in wallets" might be one of the biggest and widespread misconceptions due to oversimplified language often used to describe complex blockchain operations. Tokens are stored on the DLT, not in wallets. What the wallet stores are the keys to prove ownership and hence access to the tokens. The tokens never leave the chain, they are just owned by different keys/accounts.

The public key is used to create a wallet address, which is shared with others to receive tokens, while the private key is kept secret and is used to sign off on transactions and access the tokens. Essentially, a wallet is more like a ***keychain*** that provides you access to your tokens on the blockchain.

The tokens themselves are stored on the blockchain, and ownership of these tokens is determined by the blockchain's record of transactions. When someone says they have tokens in their wallet, what they really mean is that they have a private key which allows them to transact with the tokens associated with their wallet's public address on the blockchain.

“Tokenized assets are available on-chain”

Tokenization is a process that converts rights to an asset into a digital token on a blockchain. Once the assets are tokenized, they indeed exist "on-chain," meaning their ownership records are kept on a blockchain, which ensures transparency, immutability, and accessibility. Examples of such tokenized assets include real estate, artwork, financial instruments, and even intellectual property rights.

However, it's important to understand that the on-chain token is a digital representation of the real-world asset. While ownership of the token can be easily transferred on the blockchain, transferring ownership of the actual physical asset that the token represents can be more complex, and might involve off-chain processes, legal procedures, and regulatory compliance.

Moreover, while the tokens are available on-chain, the actual assets they represent are not. For example, if a piece of real estate is tokenized, the token representing the ownership of that real estate exists on the blockchain, but the physical real estate itself does not. Also, the availability of the tokenized assets could be dependent on the blockchain network's permissions. Public blockchains are generally accessible to anyone, but private or consortium blockchains could limit who can access and transact with these tokenized assets.

So, while the statement is technically true, it can be misleading without understanding these nuances.

“Whatever is stored on the blockchain is THE truth”

No, blockchain is not a miracle technology that makes all details registered on the ledger true by default. What is true is that blockchain provides a high degree of immutability as it is extremely difficult and almost impossible for someone to tamper with whatever information or transactions that have been entered to a blockchain. (See the next section, 'Every DLT is secure by default', for more information on security.) In terms of transactions for example, if a transaction and a certain amount is viewable on the blockchain, it is most likely true that a transaction of that amount took place. But blockchains are not limited to registering data in the form of transactions of certain amounts (which is a common misconception among those who believe that blockchain is synonymous with crypto currencies). Blockchains can be used to register any kind of data, including temperature, emissions and ingredients of products. Such data could be inaccurate for many reasons, and if it was before it was registered on the blockchain, it will not become accurate because you save it on the blockchain. It is true that blockchain brings accountability as data cannot be tampered with once registered on a blockchain, which makes inaccurate data less likely, as someone entering inaccurate data to the

blockchain will never be able to tamper with the ledger and hence be held accountable if the inaccuracy is exposed. However, blockchain is not bulletproof to inaccurate data and it is important to separate the accountability and immutability aspect of blockchain from the truth aspect.

Final remarks:

In conclusion, misconceptions about DLT and blockchain primarily arise due to their complex nature, nascent state, and the rapid pace of development in this sector. Miscommunication, oversimplification, lack of contextual understanding, and confirmation bias further contribute to these misconceptions. This dynamic landscape, while exciting, can lead to information gaps and misunderstandings, which, if not addressed, could potentially hinder the productive adoption and evolution of these technologies.

Education plays a crucial role in demystifying DLTs and blockchain. Informed users are empowered to leverage the full potential of these technologies, while also mitigating associated risks. An educated community of developers, users, and policymakers is key to fostering a robust, secure, and innovative DLT ecosystem.

Organisations and individuals addressing common misconceptions and fostering education, play an instrumental role in navigating the blockchain landscape. It is only by dispelling these misconceptions and building a solid foundation of understanding, that we can ensure the safe, effective, and transformative use of blockchain and DLTs for the betterment of our digital future.

It is important to note that the misconceptions highlighted in this paper do not represent an exhaustive list. They merely represent the most prevalent misconceptions we've encountered in conferences, discussions, and within communities we engage with. The landscape of DLT and blockchain is vast and constantly evolving, meaning new misconceptions can arise as the technology develops and reaches new audiences. As such, continued education and dialogue remain essential to address and debunk these misconceptions as they emerge, promoting a clear and accurate understanding of this transformative technology.

Acknowledgements:

We extend our gratitude to the dedicated members of the IOTA Foundation in particular the regulatory affairs and the technical team for their ideas, participation and valuable contributions to this paper. Our appreciation also goes out to the members of INATBA education working group who generously dedicated their time to offer insightful feedback. Additionally, we'd like

to express our sincere thanks to the Blockchain Bundesverband and the EUBOF for their trust and support throughout this endeavor. Your collaborative efforts have been instrumental in shaping this work.