Adello

BY LAB51

Edition No. 37

TOP 50
BUSINESS & MARKETING
visionaries

THE BLOCKCHAIN TRILEMMA

Adello's focus of the week

SHIRLY VALGE

Board member & COO of Velas

Blockchain and Cryptocurrencies: from "Bubble" to Mass Adoption

EDITOR'S NOTE

Dear Reader,

In this issue, together with Shirly Valge, Board member &
COO of Velas, a blockchain technology company, we dive into the latest developments and trends in blockchain and cryptocurrencies, as well as the opportunities and problems on the way to their mass adoption.

As we look towards the future, the next several years promise to be a period of significant transformation for blockchain and crypto. Blockchain technology will increasingly be integrated into existing systems, facilitating digital identity adoption, creating new marketplaces, and streamlining cross-border transactions. At the same time, cryptocurrencies will continue to mature and expand, offering new use cases, greater liquidity, and a growing array of investment options.

Following the steps of innovation, regulatory frameworks worldwide will need to be revised to fit these new technologies, striking a balance between innovation, security, and consumer protection. As such, blockchain and crypto will undoubtedly become increasingly intertwined with traditional finance and the broader economy, creating new opportunities for innovation, investment, and growth.

Yours,

Anna Pak

Head of Marketing at Adello

The Blockchain Trilemma

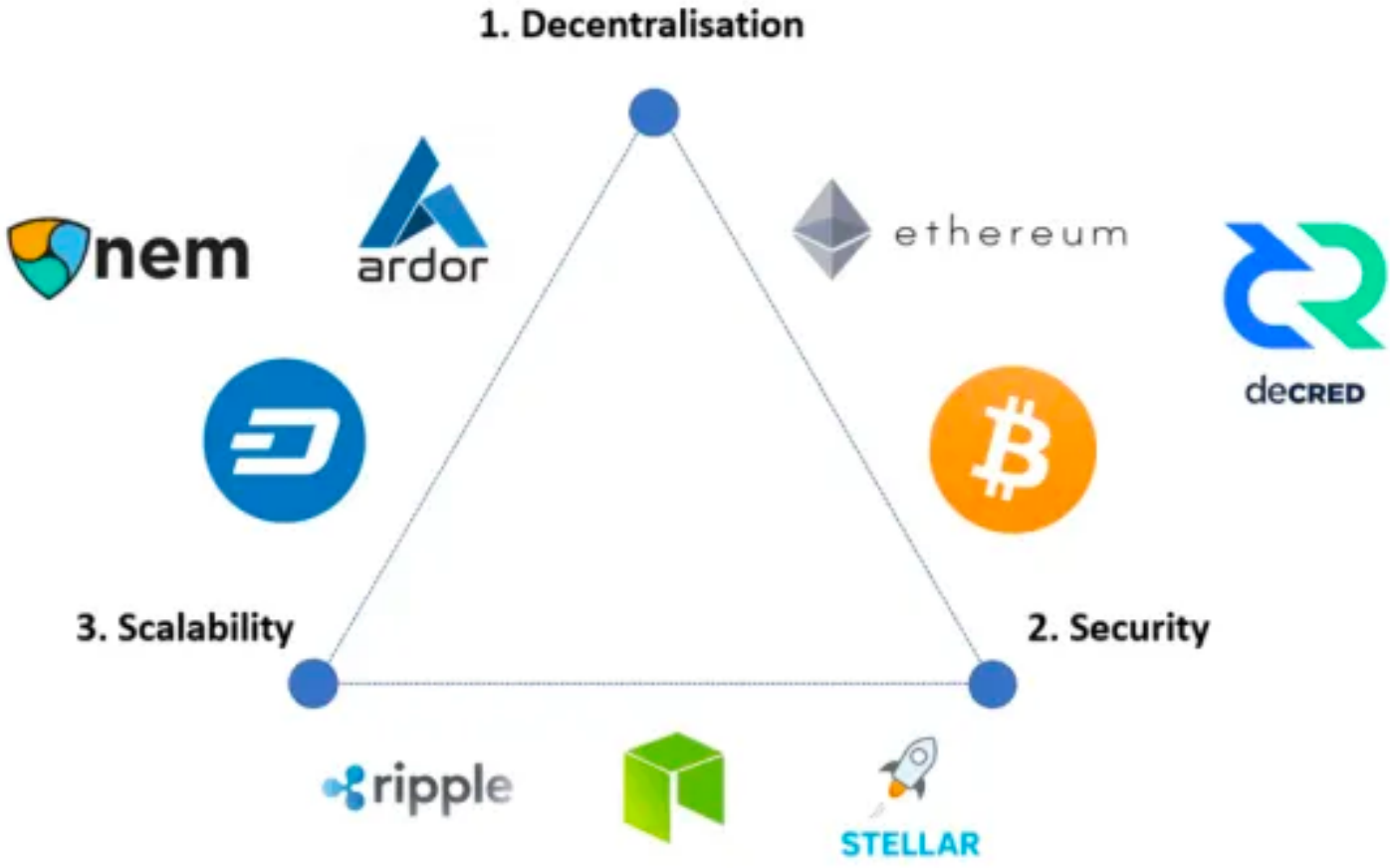
ADELLO'S FOCUS OF THE WEEK

Cryptocurrency and blockchain are interconnected. Blockchain is a digital ledger that records cryptocurrency transactions, while cryptocurrency is a digital or virtual currency secured through cryptography. Blockchain creates an incorruptible, permanent, and verifiable record of all cryptocurrency transactions, making them almost impossible to alter or counterfeit. The inviolability of blockchain also makes it almost impossible to hack into user profiles or move funds without permission. Cryptocurrency transactions are thus more secure and dependable than traditional payment frameworks.

The idea is that decentralized and secure blockchains will create a world where we do not need to rely on third parties to operate networks or markets. However, experts agree that for this technology to become more widespread, an underlying problem must be solved. This problem is known as the Blockchain Trilemma.

The term was popularized by Ethereum co-founder Vitalik Buterin. There must be three different elements that are desirable in a blockchain: Decentralization, security, and scalability. The blockchain trilemma refers to the idea that it is difficult for blockchains to achieve optimal levels of all three properties simultaneously. Strengthening one of them usually leads to weakening the other.

In this article, we will look at all three elements of the trilemma and explain in more detail what each represents.



As we know, decentralization is an essential part of the blockchain. Decentralized blockchain networks, like Bitcoin, are not owned by one person or organization. Data is shared openly and validated by all participants. This enables Web3, the decentralized Internet, which is secure and fast. Decentralization helps ensure that the blockchain remains resilient and unaffected by any potential malicious attackers. By decentralizing the system, each node (user) has an equal amount of power and authority, which helps to ensure fair and transparent transactions. Decentralization also keeps the system decentralized and prevents any one organization from having too much control over the network.

Blockchain security involves a combination of cryptography, consensus algorithms such as Proof of Work (PoW), and a large number of participants. Cryptography provides security by ensuring that blocks of data are linked and cannot be tampered with. Meanwhile, consensus algorithms, such as PoW, help protect the cryptocurrency registry by requiring miners to solve mathematical puzzles before new transactions are verified and added to the ledger. The larger the number of participants in a blockchain, the harder it is for one actor to take control and override the consensus.

Scalability is the ability of a blockchain to increase the number of transactions it can process per second (TPS) without sacrificing security or decentralization. Many blockchains struggle with scalability due to the need to prioritize decentralization and security, resulting in limited TPS compared to centralized networks. Blockchain scalability solutions are being developed to address this issue, such as through the use of different consensus mechanisms, sharding, and off-chain solutions.

Examples, reflecting this rule in different ways

Traditional blockchains: Bitcoin, Ethereum or Litecoin. Each of their participants manages a complete node that validates each transaction. Such networks have a high level of security and decentralization but low bandwidth.

High-speed blockchains, including those based on Delegated Proof-of-Stake algorithms. They have a small number of nodes (10-100). At the same time, there are high requirements for each of them - the need to have expensive server hardware or a large number of native coins. The majority of its nodes are hosted in one location or by one organization, leading to a limited distribution of trust and control. These are productive and secure, but not sufficiently decentralized networks.

Multichain systems enable applications to be connected to multiple blockchains, with communication across these blockchains occurring through cross-chain protocols. This is an example of a decentralized and scalable network, but not a secure one. After all, an attack needs to take possession of most of the nodes in just one blockchain of the system to "break" the usual structure and cause negative consequences for all other participants.

Why is there a blockchain trilemma

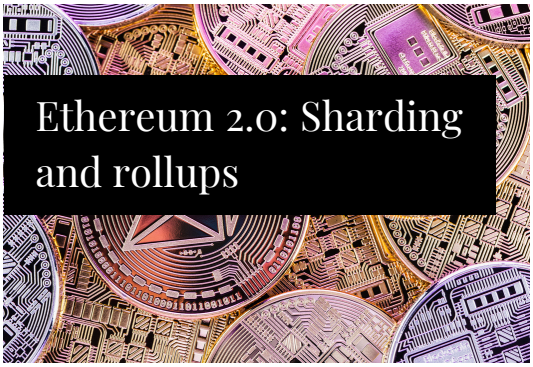
The most obvious and basic solution to the problem described above is to reduce the number of participants confirming and adding data to the network in exchange for greater scale and speed. However, this will lead to a weakening of decentralization when control is given to fewer participants. It will also lead to weakened security, as fewer participants mean a higher likelihood of attacks.

Thus, there is a trilemma: Given the relationship between the desired properties of decentralization and security, the fundamental design of the blockchain makes it difficult to scale. By increasing one, you weaken the other. How do you achieve scalability without sacrificing decentralization, security, or both?

The search for a solution

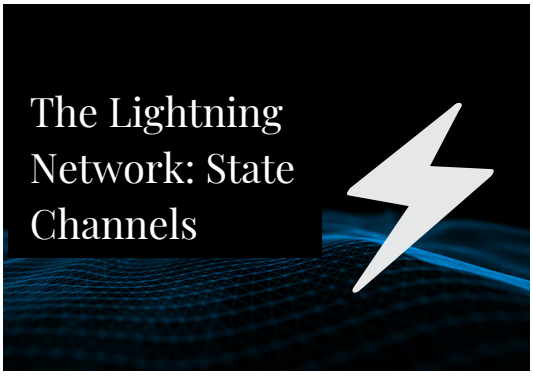
The problem, which presents a demanding challenge to resolve, has led to some interesting innovations in the blockchain industry. There are various ideas, depending on the foundation of the project and whether it relies on a different project to operate (like, for example, a Decentralized application needs Ethereum), and it's fascinating to see how they might impact the network in the future.

Without delving too deeply into the technology, here are a couple of interesting approaches that projects have taken:



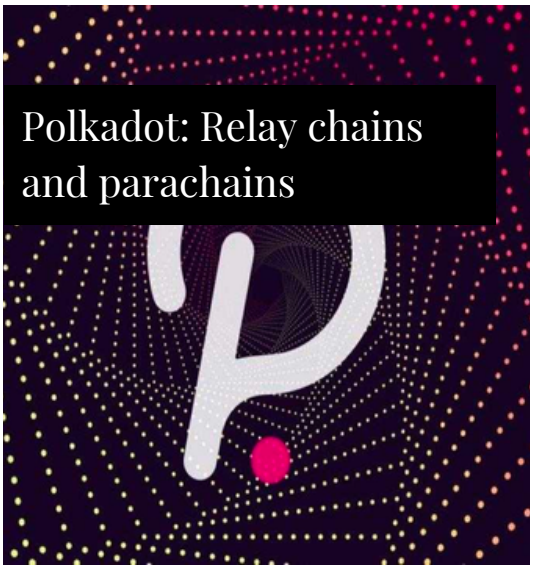
Sharding has become a popular solution for scaling projects that do not rely on another network, such as Ethereum. When a network “shards”, it breaks the transactions that run on the blockchain up into easier sets of data that can be processed by the network more quickly. This means more transactions can take place at the same time without causing congestion. Security is maintained because the different shards interact with each other and send information to the main blockchain, so information isn’t compromised.

Rollups allow networks on Ethereum’s blockchain to “roll up” multiple transactions into a single off-chain (with validated proof) and then submit the rolled-up data to the main chain. It's comparable to carpooling. Rollups are clever because they reduce the amount of data required for a transaction, thereby reducing traffic and increasing speed.



The Lightning Network is referred to as a "layer 2" solution because it offers an additional layer that sits over the main network. Bitcoin, as our primary example, "suffers from success" and struggles with transaction speed and cost. The Lightning Network allows you to conduct transactions without having to interact directly with Bitcoin's main chain.

Instead of transacting on the main blockchain, you set up “channels” with people to transact with. Inside the channels, which are run by smart contracts, you can transact directly, instantly, and at a far reduced cost than that on the main blockchain. With a state channel, you create a channel (kind of like opening a tab), which is recorded on the main blockchain. From there, all transactions will take place “off-channel” (not on the main chain) until the channel is closed. When a transaction is closed, only the opening and closing information is sent to the main blockchain, rather than all information. Because state channels operate through smart contracts, security is maintained.



Instead of offering a one-blockchain solution, Polkadot favors the idea of blockchains collaborating with other blockchains (interoperability). The network is designed with “a relay chain” as the backbone to offer a highly scalable network. It does this by using “parachains” which are independent blockchains that connect to the main relay chain.

It means that the chains operate independently in their governance, allowing the network to scale, but ultimately unite for additional security.

What tackling the trilemma means for the future of blockchain

Although most people are unaware of the blockchain trilemma, they are aware of the issues it presents (such as Bitcoin's slower transaction speed). If projects can successfully solve the trilemma, we may see new levels of blockchain adoption.

If there is a successful way to check the "decentralized" box without worrying about security or the inconvenience of a lack of scalability, we are looking at a scalable blockchain future in which individuals from multiple industries (from money to logistics, from legalities to property) can benefit. At its heart, blockchain offers a more fair and balanced playing field for individuals to thrive rather than relying on a traditional, centralized, and controlled system.

Weekly Highlight

Blockchain and Cryptocurrencies: from "Bubble" to Mass Adoption

BY SHIRLY VALGE

Many people treat everything related to the blockchain with distrust, keeping in mind cryptocurrency projects, which for the most part turn out to be scams. However, this decentralization technology is only the foundation for the development of many business sectors, as it can ensure the transparency of operations without the participation of third parties. Let's learn about the rise of the blockchain in detail.

Blockchain adoption is only a matter of time

According to Exploding Topics, about 1 billion people around the world (that is, about 12.5%) use cryptocurrencies in 2022, while 85 million of them are Bitcoin holders. For comparison, in 2019, the number of owners of this most popular cryptocurrency in the world was half that, which literally describes the doubling of demand for cryptocurrencies in general in just three years. Indeed, Fortune Business Insights claims that by 2029, the global blockchain market value will grow to $163.83 billion (currently, its global capitalization is about $7.18 billion).

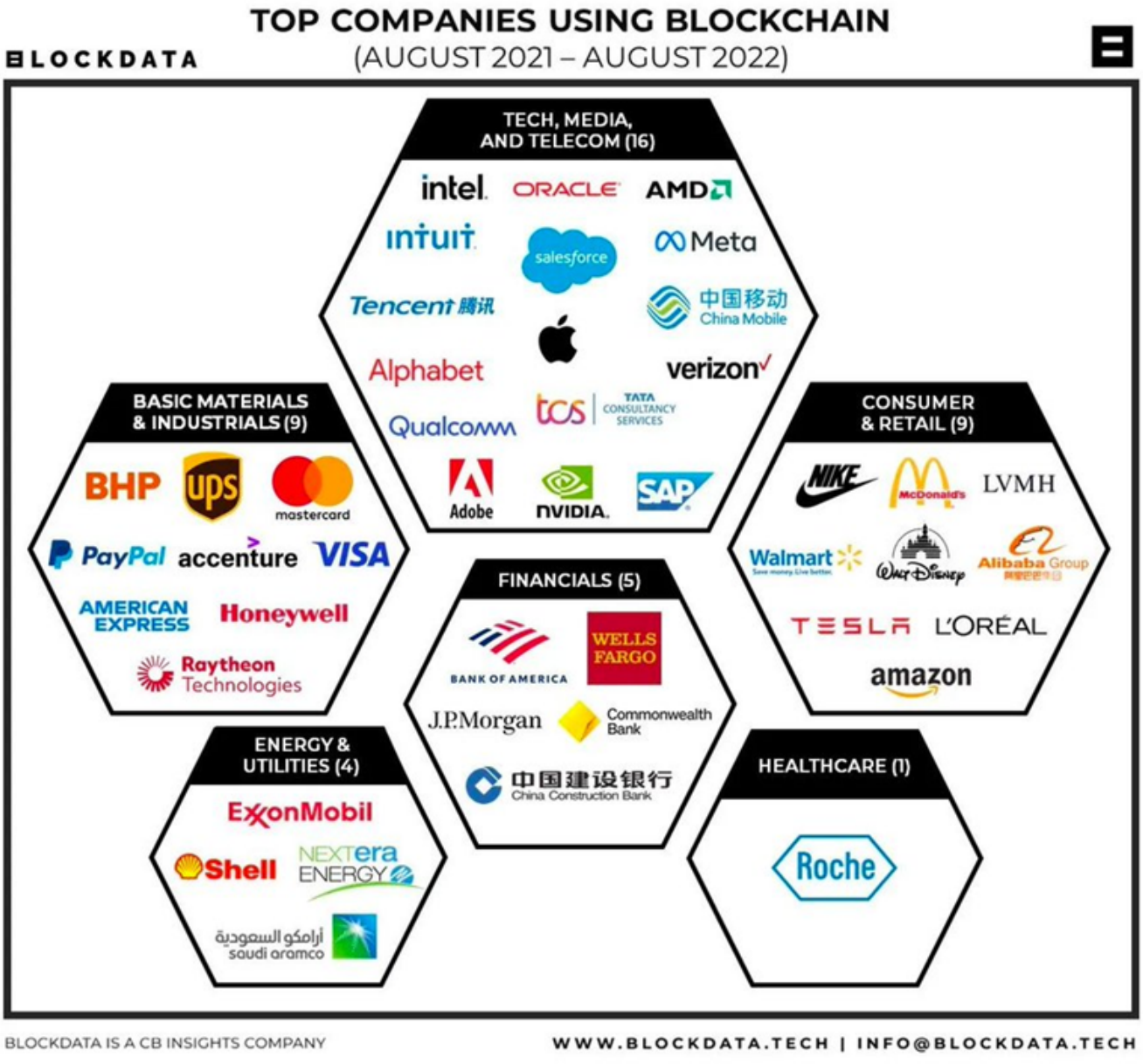
Also, Stash claims that the vast majority of crypto holders are residents of India, Nigeria, Vietnam, Australia, and Ghana. This is due in no way to loyalty to the crypto industry of the local government, since in India, for example, the use and purchase of cryptocurrencies is prohibited. Fortunately, there are only 6% of countries with such restrictions.

Cryptocurrency inquiries from financial advisors are also on the rise: last year, 9 out of 10 received questions about cryptocurrencies from their clients. All these factors indicate a positive growth in confidence in the crypto industry, regardless of the influence of local legislation and other factors that, in theory, could weaken the credibility of digital currencies per se.

At the same time, the entry threshold into the world of cryptocurrencies is quite high. This is due to the complexity of blockchain technology, as well as the prevalence of cryptocurrencies only in certain business sectors. Yes, blockchain and cryptocurrencies, as many other technologies like the Internet, are significantly ahead of the time in which they appeared, and it may take years for their global adoption. However, nothing is impossible – any, even the most complex technology can be adapted for mass use, you just need to show people that it can be as easy as paying with banknotes or a credit card.

And that's exactly what I've been doing for the last few years at Velas. Since my team and I are active users of this innovation as well, our main focus is to offer solutions that simplify the process of interacting with blockchain and decentralized services for companies and their clients.

It is important to understand that most of the way has already been overcome: more than ten years have passed since the appearance of the first and the most popular cryptocurrency, Bitcoin, and even the most notorious skeptics have ceased to perceive these digital assets as a bubble. On the other hand, in 2022, it is hard to imagine how one of our parents or grandparents will regularly pay with cryptocurrency, for example, in a bakery. Can this barrier be removed today? Undoubtedly.



Now crypto industry is of interest to big business players

Even though the crypto industry is still undergoing its formation, many large business players have already demonstrated their interest in it. In particular, according to the Blockdata report, 44 out of the top 100 public companies by market capitalization across six major sectors use blockchain to some extent.

These include META, the LVMH concern, American Express, Bank of America, Shell, Roche, etc. Some of them introduce NFT, some offer their users to pay with crypto, and some even use blockchain technology outside the context of digital assets.

Moreover, we have our own cases of big players getting involved, such as Velas, which recently entered into a long-term partnership with Ferrari to develop digital solutions for the Scuderia fans.

Be that as it may, the official adoption of the blockchain by such well-known companies proves the viability of this technology for the vast majority of business sectors.

Whether we like it or not, digital currency will soon become common

Whether society wants the globalization of digital currencies or not, it will anyway happen in the nearest future in many countries, through the introduction of central bank digital currency (CBDC), a new form of publicly available e-currency. In fact, this is an analog of the usual monetary unit, which is used as fiat money and serves as a legal payment method.

Indeed, an e-wallet for CBDC is no different from a regular bank mobile application and Apple Pay or Google Pay. Therefore, nothing will change for the end user with the advent of the new currency.

The popularity of CBDCs is growing all over the world for many reasons. In particular, the COVID-19 crisis triggered a shift in payment habits towards digital, contactless payments, and e-commerce due to the later disproved risk that banknotes could carry the virus. In this regard, cryptocurrencies developed by private organizations or informal communities have experienced significant development and an increase in value. In response, the vast majority of countries have begun to consider the introduction of digital currencies at the official level.

Obviously, if even states have taken up the introduction of digital currencies, very soon they will become as common as fiat. Thus, the matter remains small: To ensure the simplicity of software solutions operating with crypto.

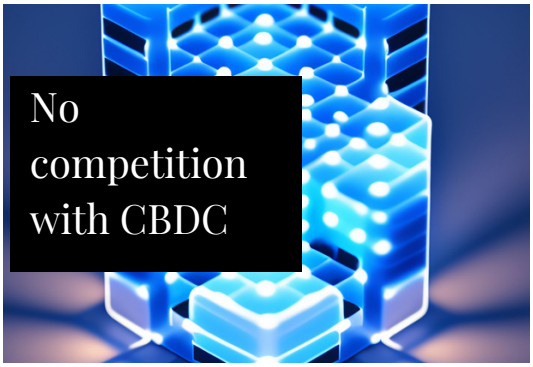
At what point did crypto cease to be considered a bubble?

ICOs were the first step toward the mass adoption of cryptocurrencies. For more than five years, initial sales have attracted millions of newcomers from all over the world to the crypto industry, allowing them to buy cryptocurrencies at a minimal cost. While many projects, unfortunately, turned out to be scams, today, thanks to ICOs, cryptocurrency is no longer perceived as something “alien”.

Cryptocurrency currently experience acceptance at the state level: the governments of many countries have finally concluded that crypto can no longer be outlawed and have begun to develop new laws related to its regulation. The next, final stage of crypto popularization will be its adaptation for all segments of the population, which consists, first of all, of the creation of convenient user interfaces for the software where it is used.

Let's look at several other factors that contribute to the introduction of cryptocurrency into the everyday life of the average person.

Since it is still quite difficult to buy some cryptocurrencies through fiat, the first ones still do not experience much distribution. This is primarily because the vast majority of states are still wary of crypto, protecting their residents from investing in scam projects. When this barrier is overcome (in particular through the legal regulation of the crypto industry), the crypto will be used by ordinary people much more often.



The above-mentioned CBDCs can become a "law-abiding" alternative to cryptocurrencies. While they can coexist with each other without any mutual detriment, some countries see the latter as direct competitors to their plans for CBDC introduction. For example, ICOs are prohibited in China, and crypto trading is strictly regulated.

To start understanding crypto, many people have to study relevant web resources for a long time. In addition, sometimes this studying does not give proper results, and new investors lose their money due to the wrong choice of subject for investment. Thus, to attract new target audiences, the crypto industry must ensure transparency.

Reducing volatility

The volatility of the vast majority of cryptocurrencies is already in the past, which is primarily due to the introduction of stablecoins. However, having learned from the bitter experience of unsuccessful investments, some representatives of the target audience still doubt the stability of the crypto and this obstacle needs to be removed through an explanation of how stablecoins work.

Regulation by law

To date, cryptocurrencies are poorly integrated into the modern financial system and are often used only for financial speculation. Even if the cryptocurrency market grows constantly, it still represents a kind of financial “chaos”: insider trading methods are actively used in the cryptocurrency market, market manipulations with cryptocurrency rates are carried out without any censure or punishment (let’s remember, for example, the so-called pump&dump technique), cryptocurrencies are used to circumvent various prohibitions by financial intermediaries to evade taxes and finance illegal activities and other prohibited activities, etc. Thus, the crypto industry needs to adopt a set of laws to stop being attractive to criminals.

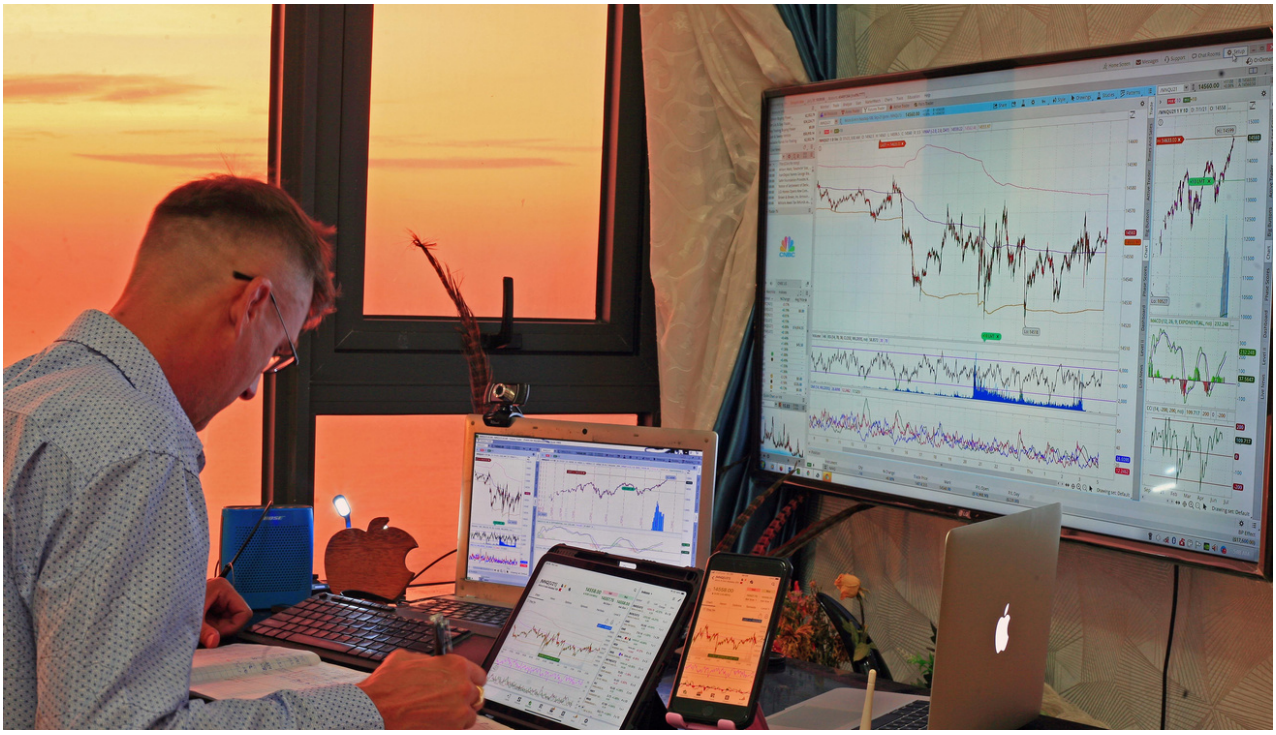
Ensuring usability

The management of 64-character private keys consisting of an arbitrary set of letters and numbers becomes another factor against the mass adoption of crypto. It is almost impossible to remember them, so for storing them in a safe place, you need to additionally use a password manager, which in theory, can become a single point of failure. That is why the modern crypto industry needs to simplify access to crypto wallets so much.

According to the Findstack survey, about 31% of respondents are worried about fraud related to their cryptocurrency assets. That is why the crypto industry needs additional tools and approaches that can guarantee investors the safety and integrity of their investments.

So far, projects using cryptocurrency have a limited range of integrations with third-party solutions, which reduces the convenience of their use. Therefore, when digital giants start to actively implement cryptocurrency in their products, this type of asset will become more widespread.

As you can see, neither government restrictions nor the risks associated with the volatility of the crypto no longer stop those who want to dive into the blockchain industry. Cryptocurrencies are going through their final stage of mass adoption, and what projects that operate with them now can do is to ensure the comfortable use of their products.



#persona

SHIRLY VALGE

Board member & COO of Velas

Shirly Valge is the founding team member and COO at Velas, a Swiss-based Blockchain technology company that has recently secured a $135 mln financial commitment from GEM. Up to this date, Shirly has been pushing Velas to grow partnership relations with well-known crypto companies, including Fireblocks, Spacechain, and Ledger, as well as traditional companies like Ferrari, Richemont Group, and Siemens.

In early 2022, she developed a methodology to evaluate the carbon footprint of a decentralized distributed Blockchain network for Velas to become a 100% carbon-neutral protocol.

Born and raised in Estonia, the #1 Country to use blockchain on a national level since 2007, Shirly is also part of the Forbes 30 under 30 DACH, class of 2021.

Prior to leading Velas, she served as a Chief Sales Officer responsible for marketing and fundraising in the largest Swiss Crypto Mining Investment firm. Shirly has been closely studying the developments of the crypto space across Switzerland and Europe since the end of 2016, also volunteering as an Expert in Crypto and Fintech for Kickstart Accelerator since 2018 by helping startup projects with in-depth knowledge in crypto and fintech.

Adello Group AG.

Forchstrasse 32, 8008
Zürich Switzerland

Adello Malaysia Sdn. Bhd.

Mid Valley City 59200
Kuala Lumpur, Malaysia

LAB51 Inc.

548 Market St, Suite 33114
San Francisco CA 94104, USA

For collaboration:

Marketing: *marketing@adello.com* (+1) 625 225 2446
Sales: *sales@adello.com* (+41) 44 50031 50