SMART

1. Executive Summary

In this document, the Smart Blockchain team analyzed the cryptocurrency market state in 2023 and described the mission of Smart Blockchain in the market. You will get information about the mission, history, blockchain features, key technologies and products of the project from this document. You will learn about the strategy for maintaining the value of Ultima's native blockchain token, as well as the project plans for the near future.

The project is based on the creation of Smart Blockchain and its infrastructure. It offers publicly available blockchain support with high throughput, high scalability and high accessibility for all decentralized applications in the ecosystem.

2. Market Analysis

2.1 Current State of the Market

We are used to the fact that there are cycles in the financial markets: "bulls" replace "bears". However, it is easy to make assumptions and form plans for traditional markets, while forecasts are often a sure way to get disappointed and seem like an armchair expert when it comes to the cryptocurrency market.

In January 2023, at last, many assets came out of the narrow price corridor upwards. Bitcoin value has risen above the key level of $20 thousand, growing by 30% in a month. Ethereum value experienced similar growth, having risen above $1500. As before, the two "giants" lead the way for the rest of the market: many assets also started 2023 with rapid growth.

It could be caused by various factors: from relative stabilization of the energy crisis and absence of recent negative news in the market after the FTX collapse, to expecting easier rate policy from the Federal Reserve. There are also reasons for the growth limitation: from persisting stressful international context to the launch of new investigations into activities of crypto companies and prosecution of those who use cryptocurrencies for money laundering.

It must be noted however that January started with a vast outflow of BTC from the market, which, historically, often promises price growth. Hence, the new dynamics may have been provided by "whales", major coin holders.

Experts also note that interdependence of cryptocurrency prices and tech company stock prices has been not weakening at all, but rather increasing. Hence, the cryptomarket growth may be also related to the stabilization of major IT companies' position.

Steady growth of the number of venture deals in the market also gives grounds for cautious optimism. Investor support enables crypto startups not only to develop their products, but to maintain asset growth.

Irrespective of the growth reasons, Bitcoin and Ethereum once again show that skeptics have given up on them a little too soon. The current market situation offers opportunities for both short-term and long-term investments. However, it is understood that for further growth, "large" assets will have to overcome a number of resistance barriers.

Alternative coins may be a worthy element of any portfolio, but they still require a careful attitude, especially when it comes to speculative assets. A good example may be the BONK coin — its value recently collapsed by 100% in a day.

2.2 Advantages of Cryptocurrencies as a Payment Method

Digital assets are rapidly becoming not only a promising investment, but also a convenient payment means. Cryptocurrencies are accepted by various institutions and companies. And it is even easier to find private specialists who accept cryptocurrencies as payment for their services.

Moreover, in 2021, Bitcoin was for the first time recognized as a legal payment means at a national level. It is now used as a currency in El Salvador. Similar reforms are under discussion in other countries as well.

The main advantages of paying in cryptocurrencies are as follows:

- independence,
- guaranteed control over the funds,
- possibility to pay whenever and whomever,
- anonymity,
- low cost.

One of the main tasks of cryptocurrencies regulation is the fight against money laundering. Regulators often stress that in the absence of strict rules cryptocurrencies become a useful instrument for criminals and fraudsters.

Principal opponents of regulation have expressed fears that it may limit the freedom of transactions, which is one of the key advantages of cryptocurrencies. Experience has shown that these fears are most probably groundless. An example may be a case of Tornado Cash mixer blocking: despite the USA authority sanctions, the platform keeps operating.

But even within the new legal framework cryptocurrencies remain mostly free and decentralized. After all, it is not so easy to change one of the technological foundations of cryptocurrencies.

Owners of digital assets still can transfer them to any wallet in any part of the world without any limitations. No one can stop or freeze a transaction, no one can make you explain the purpose of payment or force you to issue reporting papers.

Non-exchange wallets, especially so-called “cold” wallets, cannot be blocked, the funds on them belong to the wallet’s owner only.

Cryptocurrencies can be sent to anyone at any time. Bitcoin payments do not require approval of banks or regulators. The only thing you need is the recipient’s wallet address.

Decentralization gives users not only anonymity, but far more opportunities to use and receive funds. For example, in the traditional financial system, if a first-time entrepreneur needs a loan with a convenient payment schedule, the entrepreneur has to turn to a bank and hope that the request will be approved.

But cryptocurrency users do not need large institutions. They may freely request and lend funds at their own discretion. They may do it directly, using smart contracts, or with the help of intermediaries, for the sake of guarantee. There are fewer and fewer barriers between ambitious ideas and the necessary funding.

Cryptocurrencies facilitate supporting charitable and public organizations, as well as business in the regions where financial services are not available to everyone. For example, in Africa, where banking services are still not widespread, cryptocurrencies can successfully replace fiat payments. Also, digital assets have been for a long time facilitating Cuba’s trade with the countries where capital flow is limited.

Those who are just starting to use cryptocurrencies as a payment means should bear in mind that, contrary to the popular opinion, transactions with digital assets are still traceable. It is not easy to do, but possible: principal information on transactions is recorded and kept in the public domain. Under certain conditions, it is possible to trace a connection between a network address and its owner.

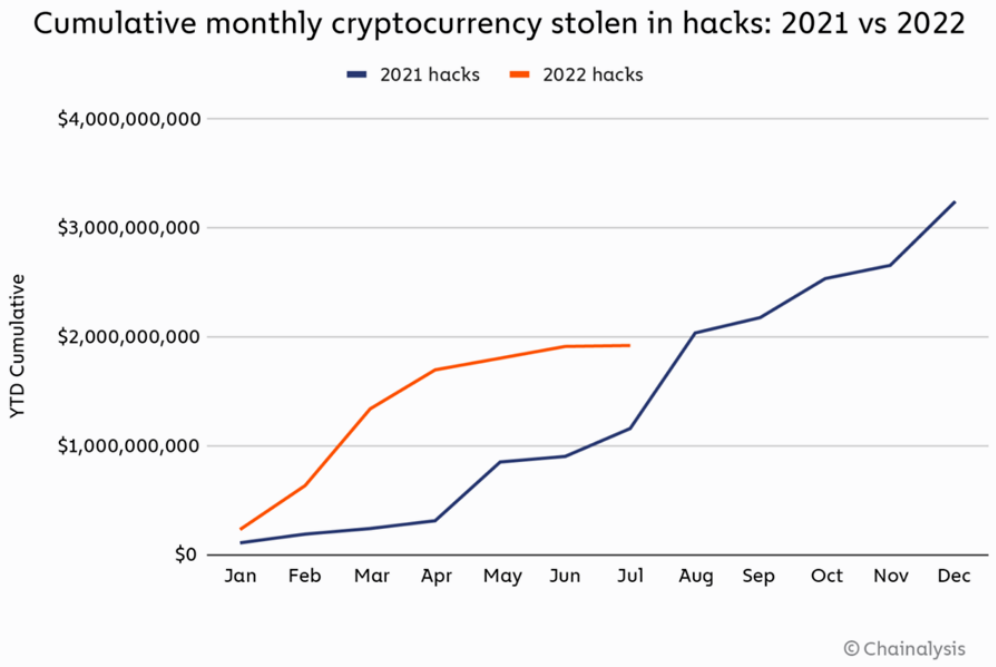
However, if cryptocurrencies users do not link their digital assets with the traditional financial system, for example, do not use their bank account to add funds to their account on the exchange, or do not withdraw funds from the exchange to the card, it is almost impossible to deanonymize them.

And finally, cryptocurrency payments are often cheaper than traditional ones. They are not taxed and do not require paying for payment systems services. The cost of miner services is often much lower than the cost of fiat payments, especially in case of international transfers.

Despite all these advantages, cryptocurrencies have not yet become a full-fledged payment means. Some companies have declared that they accept Bitcoin in exchange for their goods and services, but in fact these intentions rarely go beyond pompous announcements. Over 90% of operations with “the first cryptocurrency” remain market speculations.

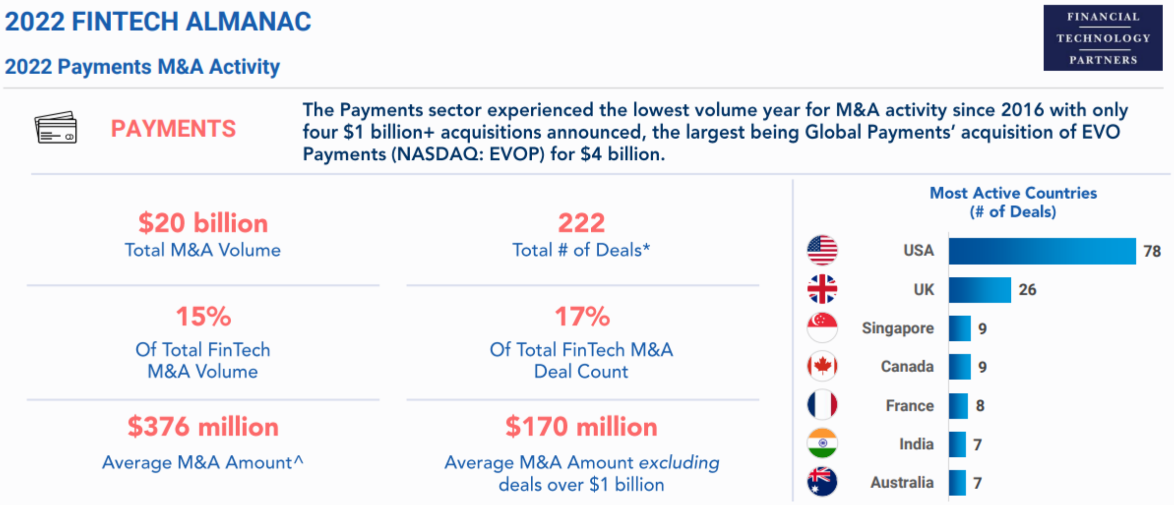
At the same time, due to the lack of full-fledged regulation, fraudulent activity still remains high in the crypto market. Attackers easily gain access to users’ wallets, and often hacks occur through the fault of cryptocurrency owners. The most common user mistakes are the following: storing passwords and other sensitive information in the emails and on the public servers, inattention when sending transactions, clicking on phishing links, and other reasons.

Cryptocurrencies give freedom of cross-border payments, but at the same time require high attention from market participants. Modern projects take a number of measures in order to protect their users as much as possible, but the risks of hacking are still relatively high. So, according to the Mid-year Crypto Crime Update by Chainalysis, as of July 2022, $1.9 billion in cryptocurrencies have been stolen. This figure is 60% higher than in 2023.



Thus, the true realization of the cryptocurrencies payment potential is still ahead. It is not an easy task, but realistic.

Especially since the conditions for it keep improving. A growing number of people get acquainted with cryptocurrencies and start using them; regulation and new startups make them more accessible and stable. And also a growing number of people get disappointed with traditional payment systems. Even investors are losing interest in them: in 2022, the amount of investments in payment systems sharply dropped.



2022 FINTECH ALMANAC

2022 Payments M&A Activity

FINANCIAL TECHNOLOGY PARTNERS

PAYMENTS

The Payments sector experienced the lowest volume year for M&A activity since 2016 with only four $1 billion+ acquisitions announced, the largest being Global Payments' acquisition of EVO Payments (NASDAQ: EVOP) for $4 billion.

$20 billion
Total M&A Volume

222
Total # of Deals*

15%
Of Total FinTech M&A Volume

17%
Of Total FinTech M&A Deal Count

$376 million
Average M&A Amount^

$170 million
Average M&A Amount *excluding* deals over $1 billion

Most Active Countries (# of Deals)

Country	# of Deals
USA	78
UK	26
Singapore	9
Canada	9
France	8
India	7
Australia	7

Volume of traditional payment systems financing in 2022 (https://ftpartners.docsend.com/view/yw9ece46c54ks6zp p. 103)

Analysts have also noted significant problems with B2B payments. This sector is suffering from outdated processes and technologies and needs modernization. According to the FT Partners report, many tasks still have to be fulfilled manually, which makes the work too time-consuming and increases the risk of error. In the USA, almost half of B2B payments are still made with the use of checks.

Notably, only the American business payment market amounts to $29 trillion. Thus, those who will be able to offer a simple and reliable solution of the issues, can get a big prize. And this solution will hardly be related to fiat payments.

Gradually, a vacuum is emerging in the financial market, which can only be filled with digital assets.

Anyway, cryptocurrencies are already coping with some tasks quite well. Arthur Hayes, an American businessman and a co-founder of BitMEX believes that cryptocurrencies are the best asset for the period of acute instability.

Even in the most pessimistic future scenarios, where governments severely restrict free capital flow, cryptocurrencies remain independent means of payment and saving. They cannot be limited, confiscated, or controlled like fiat money.

Your digital assets will always be yours.

2.3 Market Development Trends

It is worth remembering that this “crypto winter” differs from the previous ones by a number of factors. The most important of them is the role of institutional investors that has sharply increased. Just a year ago, institutional investors held $70 billion worth Bitcoin. Cryptocurrencies have been acquired by both large investment funds and corporations like Tesla and MicroStrategy.

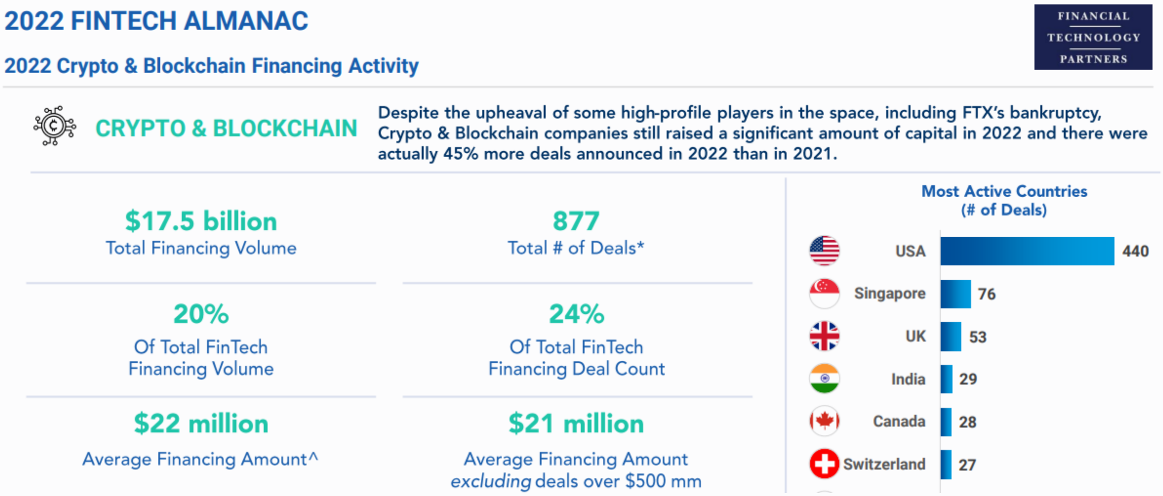
Many institutional investors presently remain interested in digital assets. Elon Musk has specially pointed out that Tesla has not sold the acquired Bitcoin and retains its assets. Institutional investors have great resources to support the new “bull run” when it starts. And their reputation supports the interest of cautious players in cryptocurrencies. This time, not only private traders will return assets to historical highs.

General distribution of cryptocurrencies also plays an important role. Over the last several years, digital assets have become much more popular and accessible to a large number of people. By the beginning of 2022, Bitcoin alone was owned by 106 million people.

Cryptocurrencies market is constantly expanding and attracting new investors with new funds. It lays the foundation for the new growth. Finally, critical technical updates also play a significant role. The Bitcoin network has been expecting a new halving: a regular decrease in the new coins generation rate and recalculating of mining rewards. It is believed that halvings positively affect the price of the first cryptocurrency and restore the balance in the system. Last halving occurred in May 2020, shortly after that the market began to grow quickly. The next halving is scheduled for 2024.

It’s noteworthy that despite all the off-the-wall issues of 2022, investor interest in digital assets and companies related to them has survived. According to the FT Partners report, cryptocurrency and blockchain startups collected $17.5 billion of investments over a year, and the number of transactions grew by 45% against 2021.

Transaction analysis also shows a global scale of the cryptocurrency market. Companies from the United States attracted the most investor interest, but startups from Singapore, Great Britain, India, Canada, Switzerland, France, Germany and China also received a significant share of the funding.



2022 FINTECH ALMANAC

2022 Crypto & Blockchain Financing Activity

FINANCIAL TECHNOLOGY PARTNERS

CRYPTO & BLOCKCHAIN

Despite the upheaval of some high-profile players in the space, including FTX's bankruptcy, Crypto & Blockchain companies still raised a significant amount of capital in 2022 and there were actually 45% more deals announced in 2022 than in 2021.

$17.5 billion Total Financing Volume	877 Total # of Deals*
20% Of Total FinTech Financing Volume	24% Of Total FinTech Financing Deal Count
$22 million Average Financing Amount^	$21 million Average Financing Amount *excluding* deals over $500 mm

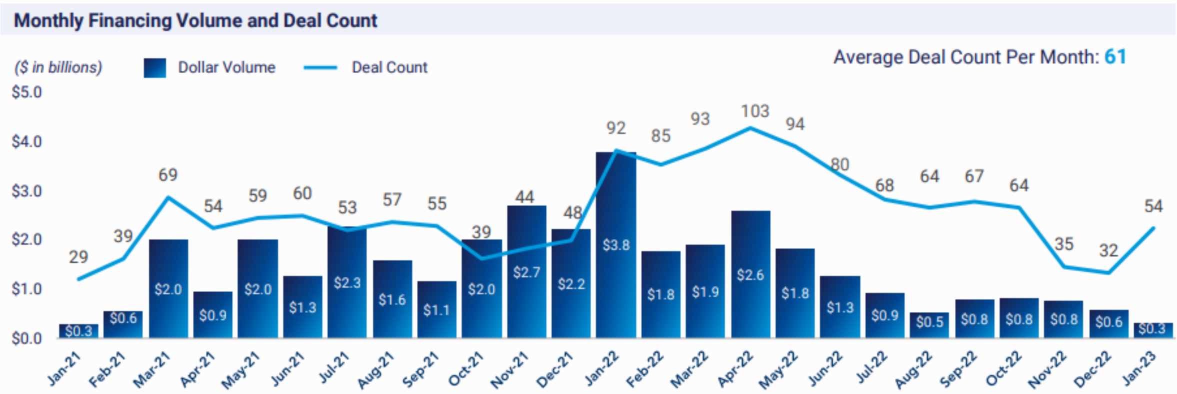
Most Active Countries (# of Deals)

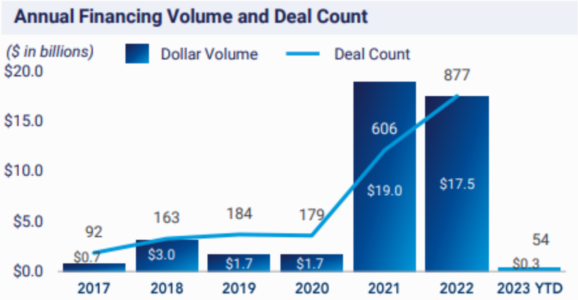
USA	440
Singapore	76
UK	53
India	29
Canada	28
Switzerland	27

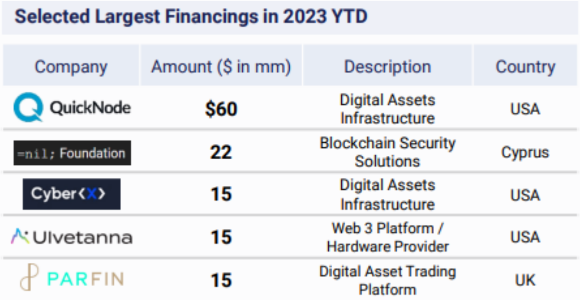
Deals in the cryptocurrency and blockchain market in 2022 (https://ftpartners.docsend.com/view/yw9ece46c54ks6zp p.83)

Investors are first of all attracted by projects that extend opportunities of using digital assets, and improve blockchain and Web3 platform safety. It may seem that this money does not go directly to the cryptocurrency market and has no influence on the assets' cost. But that is not true.

The amount of liquidity in the market is quite sufficient, it is much more important to make cryptocurrencies and blockchain more flexible, reliable and attractive for both the average user and the individual and institutional investors. Support of promising projects produces exactly this effect.






Selected Largest Financings in 2023 YTD

Company	Amount ($ in mm)	Description	Country
QuickNode	$60	Digital Assets Infrastructure	USA
=nil; Foundation	22	Blockchain Security Solutions	Cyprus
Cyber‹X›	15	Digital Assets Infrastructure	USA
Ulvetanna	15	Web 3 Platform / Hardware Provider	USA
PARFIN	15	Digital Asset Trading Platform	UK

Dynamics of latest deals in the cryptocurrency and blockchain market (https://ftpartners.docsend.com/view/46rtk3hyghm3jcpa p.38)

Assessments of the authorities' new regulation of the market differ a lot. Advocates of an absolutely free market are dissatisfied with the laws and strive to retain independence. Many investors and analysts though believe that cryptocurrencies will benefit from the regulation. After all, new legislation does not necessarily entail only limitations and losses for investors and companies.

The new rules of the game will make the market more transparent and stable. They will also help to get rid of the old association of cryptocurrencies with criminal activities, which still worries many regulators and investors. All of these are positive changes, which may attract new capital to the market and provide "fuel" for further growth.

2.4 Forecast for the Next 5 Years

It is impossible to accurately predict the dynamics of the cryptocurrency market for the period of 5 years. Digital assets are influenced by many external factors, and many of such factors can change at any time. However, there are still reasons to be optimistic.

Skeptics see the current market situation as a sign of cryptocurrencies weakness and believe that digital assets are to be avoided now. But other experts see them as an excellent opportunity to open new "long" positions and strengthen the existing ones.

Rick Edelman, a crypto enthusiast and the founder of Edelman Financial Services, a successful financial company, sees cryptocurrencies as "an opportunity to create wealth like nothing we have seen in 35 years." He explains such assessment by a huge potential for rapid growth, which digital assets retain against all the odds.

He sees the main reason for the latest correction in external factors and an oversupply of loans for margin trading in the market.

The rapid price fall allowed “clearing” the market, although at the cost of significant losses. Edelman compares the current situation with the crisis of 2008. At that time, the market meltdown was followed by the growth of almost all assets.

In his opinion, the current crypto winter may linger for several months more, but a quick recovery and the establishment of new highs will follow it. In his opinion, the price of Bitcoin may reach $100,000 in the short run.

Edelman is sure that cryptocurrency will gain a foothold in the next five years as an essential and widespread part of the portfolio of private and institutional investors.

Other analysts, primarily representatives of the traditional financial system, give more conservative market estimates. In their opinion, in 2023, digital assets will approach the highs of the past. In their view, the price of Bitcoin at that time will come approximately to $50,000. And by 2025, digital assets will reach a new level: the price of Bitcoin will come to $100,000.

Experts underline that the dynamics of cryptocurrencies are cyclic. In this respect, the digital asset market is similar to the stock market, where a downturn follows every upturn, and an upturn follows every downturn.

Cryptocurrencies have gone through several price drops, always returning to previous highs and set new records. Therefore, digital assets remain attractive to investors, especially for long-term investments.

3. Terminology

Address/Wallet

A private and public key pair generates an address or wallet consisting of account data on the Smart Blockchain network. The second is obtained from the former using an algorithm. A public key is typically used to encrypt a session key, verify a signature, and encrypt data that can be decrypted with the corresponding private key.

ABI

A binary application interface (ABI) is an interface between two binary program modules. Typically, one of these modules is an operating system library or function; the other is a program the user runs.

API

The application programming interface (API) is primarily used to develop custom clients. Thanks to API support, platforms for issuing coins can also be created by the developers themselves.

Bandwidth Points (BP)

To keep the network running smoothly, transactions on the SMART network use Bandwidth Points as fuel. Each profile receives 5000 free Bandwidth Points daily and can get even more by freezing SMART for Bandwidth Points. Smart contract deployment and execution transactions consume both Bandwidth Points (BP) and energy.

Block

Blocks contain digital records of transactions. A complete block consists of a magic number, a block size, a block header, a transaction counter, and transaction data.

Block Reward

Rewards for the production of blocks are sent to an additional account (address/wallet).

Block header

The block header is part of the block. Smart Blockchain block headers contain the previous block's hash, Merkle root, timestamp, version, and witness address.

Decentralized application

A decentralized application is an application that operates without a centrally trusted party. An application that enables direct interaction/agreements/ communication between end users and/or resources without an intermediary.

Hot Wallet

A hot wallet, also known as an online wallet, allows a user's private key to be used online so that it can be susceptible to potential vulnerabilities or interception by fraudsters.

Java Application Development Kit

The Java Application Development Kit is a software development kit for Java applications. It is the core of Java development, which includes the Java application environment (JVM + Java Class Library) and Java tools

KhaosDB module

The Smart Blockchain uses KhaosDB in full-node memory, which can store all newly forked chains generated over time, and supports witnesses to quickly switch from its active chain to a new primary chain. For more information, see Section 2.2.2, “State Store.”

Merkle root

The Merkle root is a hash of all hashes of all transactions included in a block on the blockchain network. See Section 5.2.1 for details. “Delegated Proof of Ownership (DPoS).”

Scalability

Scalability is a feature of the Smart Blockchain protocol, which is the ability of a system, network, or process to handle an increasing amount of work or expand its capacity to accommodate that growth.

Bandwidth

High throughput is a feature of the Smart Blockchain mainnet. It is measured in transactions per second (TPS), namely the maximum throughput per second.

SMART

It is the coin of the SMART Blockchain network.

4. Smart Blockchain’s Mission

Smart Blockchain is a project designed to address the challenges of the cryptocurrency market, ensure the utmost stable operation of a decentralized network, and simplify its scalability.

Our key features encompass instant transactions anywhere, anytime, without intermediaries, 24/7 operation, security, autonomy, anonymity, and conversion to other cryptocurrencies. Our protocol enables enthusiasts to initiate projects seamlessly and quickly within our network.

When developing the project, both the strengths of other cryptocurrencies and their mistakes were taken into account. But Smart Blockchain is not designed to compete with other digital assets but to create a new market for truly decentralized payments.

Cryptocurrency payments have almost endless potential. They can solve the problems of high cost, slowness, and limitation of traditional payments, as well as the inaccessibility of banking services. They can provide users with anonymity, independence, and confidence in the security of their assets.

A truly independent and accessible payment system can make life more convenient and become a tool for changing the world. It will be easier for people worldwide to start their own businesses. They can support others better and take complete control of their finances. Such a product can transform investment, trade, and even the attitude toward money.

This requires complex technical and organizational solutions. This is not an easy task, but that is why it needs to be addressed.

The goal of Smart Blockchain and the native coin of the SMART ecosystem is to turn dreams of an alternative payment system into reality. To do this, developers aim to facilitate fiat currency exchange for coins. Transparency and ease of operation will be ensured by maintaining transaction speed and low volatility. It is also planned to create and implement new convenient ways to convert and replenish the account.

The principles of Smart Blockchain are instant transactions anywhere and anytime without intermediaries, 24/7 operation, security, independence, complete anonymity, and free conversion into other cryptocurrencies. Cryptocurrencies are everything the dreamers who created the concept aspired to be.

5. Smart Blockchain Review

Smart Blockchain is a new blockchain that combines the best practices of other systems with new solutions. One of the project's main goals is to realize the dream of a free and accessible transaction system, which caused the emergence of cryptocurrencies.

Everyone can take advantage of this system. Anyone who owns at least one of the many popular programming languages can create their project on it. You can use the Smart Blockchain not only to transfer value but also to transfer and store any information, from personal data to media. Smart Blockchain is a scalable bon that uses innovative methods to solve the problems faced by traditional blockchain networks. The network offers the highest transaction speed in the crypto market — more than 2000 per second. In addition, the Smart Blockchain network offers a wide selection of more than 60 HTTP API gateways to interact with the network through full nodes and Solidity nodes.

The Smart Blockchain model is based on the Google Protobuf (Protocol Buffers) system, which allows you to split structured data conveniently and helps different platforms interact conveniently and quickly. Therefore, the Smart Blockchain allows the community to easily and quickly create decentralized networks and their coins and integrate them into existing products. Blockchain SMART uses the native coin of the same name, SMART, as a means of payment on the blockchain.

In planning the network, several technical decisions were made to prioritize the development of data storage methods in the network. The developed distributed storage system makes collecting, storing, and protecting data easy.

5.1 The key features

The total supply is 9 000 010 200 000 SMART

Maximum supply: not more than 100 trillion SMART

The block rate: ≈3 sec.

The block size: should not exceed 2,000,000 bytes

5.2 Advantages of Smart Blockchain

The Smart Blockchain has everything we value in cryptocurrencies: speed, accessibility, reliability, and independence. Moreover, the network is superior to analogs in the crypto market, even the “giants”: Bitcoin and Ethereum.

- High Throughput. The speed of operations on the blockchain is determined by its throughput: the limit of transactions that can be processed per second. For example, in the ETH network, this figure is 20-45 transactions, in BTC — up to 7 transactions, in Binance Smart Chain — 100, in Litecoin — up to 56. Smart Blockchain, on the other hand, processes up to 2000 transactions per second. Therefore, you can forget about the long wait.
- Low commissions. The usual transaction cost in the Smart Blockchain is less than $0.000005. This is significantly lower than the price of transactions in other networks and even in fiat counterparts. For example, a Mastercard transaction costs several hundred times more. You no longer need to wait for the “gas” on the ETH network to become cheaper or spend much money on a transfer.
- The Smart Blockchain uses Delegated Proof-of-Stake, a delegated proof of ownership. This is an algorithm in which transactions are confirmed by elected super representatives (SRs), who receive block rewards.

Representatives change every 6 hours. Each new block is mined, on average, in 3 seconds. This indicator indicates that Smart is outperforming its competitors. The Bitcoin network creates blocks every 10 minutes, Ethereum every 10-19 seconds, Litecoin and Qtum every 2.5 minutes.

- Since the Smart Blockchain uses the same version of Solidity as Ethereum, more coin standards can be easily transferred to the Smart Blockchain.

For the Smart Blockchain, decentralization and active participation of the community are significant.

In addition, the Smart Blockchain is easily scalable and gives developers almost unlimited options for deploying applications. DApps can be built in different languages; anyone can improve the network and run their own product.

The decentralization of the network and the significant role of SR help improve the blockchain faster, make the network more secure, and protect users' assets.

5.3 Consensus in Smart Blockchain

5.3.1 Delegated proof of ownership (DPoS)

The earliest consensus mechanism is the Proof of Work (PoW) consensus mechanism. This protocol is currently implemented in Bitcoin and Ethereum. In PoW systems, transactions broadcast over the network are grouped into nascent blocks for confirmation by miners. The confirmation process involves hashing transactions using cryptographic hashing algorithms until the Merkle root is reached, thereby creating the Merkle tree:

Rice. 2: 8 SMART transactions are hashed to Merkle root. This Merkle root is then included in the block header, attached to previously confirmed blocks, to form the blockchain. This makes tracking transactions, timestamps, and other related information easy and transparent.

Cryptographic hashing algorithms help prevent network attacks because they have several properties:

- Input/Output Length Size — The algorithm can transmit input data of any length and outputs a fixed-length hash value.
- Performance — The algorithm is relatively simple and quick to calculate.
- Resistance to image restoration—For a given output z, it is impossible to find an input x such that h(x) = z. In other words, the hashing algorithm h(x) is a one-way function in which, given input, only the output can be found. The opposite is not possible.

- Collision Resistance — From a computational point of view, it is impossible to find pairs such x 1 ≠ x 2 that h(x 1) = h(x 2). In other words, the probability of finding two different inputs hashing the same output is minimal. This property also implies resistance to the restoration of the second prototype.
- Resistance to the recovery of the second prototype — Given x 1 and, therefore, h(x 1), it is computationally impossible to find such x 2 that h(x 1) = h(x 2). Although this property is similar to collision resistance, it differs because it says that an attacker with a given x 1 will find it computationally impossible to find any hash of x2 for the same output.
- Deterministic — maps each input to one and only one output.
- Avalanche effect — a slight change in the input data leads to a completely different conclusion.

These properties give the cryptocurrency network its intrinsic value, ensuring attacks do not compromise it. When miners confirm a block, they are rewarded with coins as a built-in incentive to participate in the network. However, as the capitalization of the global cryptocurrency market grew steadily, miners became centralized and focused their computing resources on accumulating coins as assets rather than participating in the network. CPU-powered miners have given way to GPUs, which powerful ASICs have replaced. In one well-known study, the total energy consumption of bitcoin mining is estimated at 3 GW, comparable to the energy consumption of the whole of Ireland. The same study predicts that total electricity consumption will reach 8 GW shortly.

Many new networks have proposed a Proof of Stake (PoS) consensus mechanism to solve high power consumption. In PoS networks, coin holders lock the balance of their coins to become block validators. Validators take turns proposing and voting for the next block. However, the problem with standard PoS is that the influence of the validator is directly related to the number of coins blocked. This leads to parties accumulating large amounts of the network's base currency and exerting undue influence on the network's ecosystem.

The Smart Blockchain consensus mechanism uses an innovative DPoS system in which 27 super representatives (SRs) produce blocks for the network. Every 6 hours, Smart Blockchain account holders who freeze their accounts can vote to select SR candidates, and the top 27 candidates will be considered SR. Voters can choose SR based on criteria such as SR-sponsored projects to expand SMART adoption and rewards distributed to voters. This allows you to make the ecosystem more democratic and decentralized. SR accounts are regular accounts, but their accumulation of votes allows them to create blocks. Given the low throughput of Bitcoin and Ether due to their PoW consensus mechanism and scalability issues, Smart Blockchain's DPoS system offers an innovative mechanism that provides 2,000 transactions per second, compared to Bitcoin's 3 TPS and Ethereum's 15 TPS.

The Smart Blockchain protocol network generates one block every three seconds, each awarding 32 SMART SR coins. A total of 336,384,000 SMART will be awarded annually by 27 SRs. Each time SR completes the production of blocks, the rewards are sent to a sub-account in the super ledger. SRs can verify but cannot directly use these SMART coins. Withdrawals can be made by each SR once every 24 hours, transferring the reward from the sub-account to the specified SR account.

A Smart Blockchain network has three types of nodes: a witness node, a full node, and a Solidity node. The SR establishes witness nodes and is mainly responsible for block creation and proposal creation/voting. Full nodes provide APIs and translate transactions and blocks. Solidity nodes synchronize blocks from other full nodes and also provide indexable APIs.

5.4 Block

A block usually contains a block header and several transactions. Protobuf data structure:

```
message Block {
    BlockHeader block_header = 1;
    repeated Transaction transactions = 2;
}
```

5.4.1 Block header

The block header contains **raw**_data, **witness_signature**, and **blockID**. Protobuf **data** structure:

```
message BlockHeader {
    message raw {
        int64 timestamp = 1;
        bytes txTrieRoot = 2;
        bytes parentHash = 3;
        uint64 number = 4;
        uint64 version = 5;
        bytes witness_address = 6;
    }

    bytes witness_signature = 2;
    bytes blockID = 3;
}
```

5.4.2 Primary data

In Protobuf, raw data is denoted as raw_data. They contain the initial message data from 6 parameters:

1. **Timestamp**: The timestamp of the message — for example, 1543884429000.
2. **txTrieRoot**: the root of the Merkle tree — e.g., 7dacsa... 3ed.
3. **parentHash**: hash of the last block — e.g., 7dacsa... 3ed.
4. **number**: the height of the block — for example, 4638708.
5. **version**: known in advance — for example, 5.
6. **witness_address**: the address of the witness packed into this block — e.g., 41928c... 4d21.

5.4.3 Signature of the witness

The witness's signature is denoted in Protobuf as witness_signature, i.e., the signature of the witness node for this block header.

5.4.4 Block ID

The block identifier in Protobuf is denoted as **blockID**. It contains the atomic identifier of the block. The block identifier contains 2 parameters:

- **hash:** hash of the block.
- **number**: hash and height of the block.

5.5 Transaction as Proof of Stake (TaPoS)

SMART uses TaPoS to ensure that all transactions confirm the main blockchain while at the same time making it more difficult to forge fake chains. In TaPoS, networks require each transaction to include a portion of the hash of the last block header. This requirement prevents transactions from being replayed on forks that do not include a specified block and also signals to the network that a particular user and their stake are at a certain branching. This consensus mechanism protects the network from denial-of-service attacks, 51%, selfish mining, and double-spending attacks.

5.5.1 Transaction Confirmation

After being broadcast to the network, the transaction is included in the future block. The transaction is confirmed after 19 blocks (including its block) are mined on SMART. One of the top 27 SRs in a circle creates each block. Mining each block in the blockchain takes ~3 seconds. Each SR's time may vary slightly depending on the network's state and the equipment's configuration. As a rule, the transaction is considered fully confirmed after ~1 minute.

5.6 Smart Contract

A smart contract is a digital protocol that verifies contract negotiations. They determine the rules and penalties associated with the agreement and automatically enforce these obligations. A smart contract code facilitates, verifies, and ensures an agreement or transaction is negotiated or executed. In terms of coining, smart contracts also make it easier to automatically transfer funds between participating parties if specific criteria are met.

Smart Blockchain smart contracts are written in the Solidity language. Once written and tested, they can be compiled into bytecode and deployed on the network for a Smart Blockchain virtual machine. Once deployed, smart contracts can be queried at their contract addresses. The Contract Application Binary Interface (ABI) displays contract call functions and is used to communicate with the network.

5.7 The Potential of Smart Blockchain

Smart Blockchain boasts a robust technological base, the ability to change and improve flexibly, and effective methods of stabilizing the value of coins.

However, its most outstanding feature is its ability to store and transmit different forms of data. It can be used to trade or pay for goods and services for different purposes.

In the future, the Smart Blockchain can be used to decentralize the Internet and implement Web 3.0 plans. This, in turn, will help bring the project out of the cryptocurrency niche and interest even those investors who usually avoid digital assets.

Therefore, the blockchain already has serious potential. However, the project’s future depends mainly on the specific applications of its excellent base.

6. Coin

6.1 SMART Coin

On the SMART network, each account can issue coins for 1024 SMART. To issue coins, the issuer needs to specify the name of the coin, total capitalization, exchange rate for SMART, duration of circulation, description, website, maximum bandwidth consumption per account, total bandwidth consumption, and the number of frozen coins. For each issue, you can also configure the maximum daily number of throughput points, the ability to transfer coins for each account, the maximum daily number of bandwidth points for transferring coins across the network, the total number of coins, the duration of blocking in days, and the total number of blocked coins.

Since SMART uses the same version of Solidity as Ethereum, more coin standards can be easily migrated to SMART.

6.2 Smart Wallet

Smart Wallet is a convenient new-generation cryptocurrency wallet with an intuitive user interface, high security, and anonymity.

Smart Wallet has the great advantage of allowing you to create multiple wallets in one application, give them unique names, and switch between them quickly. It already supports ULTIMA, SMART, USDT, TRX, BTC, ETH, ADA, BNB, and other popular cryptocurrencies that will be added soon!

7. Management

7.1 Super Representative (SR)

7.1.1 General information

Each account on the SMART network can apply for and get the opportunity to become a Super Representative (designated as SR). Everyone can vote for SR candidates. The top 27 candidates with the most votes will be the SR with the right and obligation to generate blocks. Votes are counted every 6 hours, and SRs change accordingly.

A fee has been introduced to prevent malicious attacks on the SR role. When applying, 9999 SMART will be burned from the applicant’s account. If successful, such an account can join the SR election.

7.1.2 Election

The number of potential votes on the SMART network (denoted as ST) used to vote depends on the voter's frozen assets.

ST is calculated as follows:

$1\ ST = 1\ \text{SMART}\ \textit{frozen for increased throughput}$

Each account on the SMART network has the right to vote for their SRs.

After the release (unfreezing, available after 3 days), users will not have frozen assets and will lose all STs. As a result, all votes become invalid for the current and future rounds of voting unless SMART is frozen again for voting.

Please note that the SMART network only records the most recent vote, which means that each new vote cancels all previous ones.

7.1.3 Reward

a. Voting Reward

Also known as the "Candidate Reward," the top 127 candidates, whose list is updated every round (6 hours), will share as 168,192,000 SMART are mined. The reward will be divided according to the weight of the vote that each candidate will receive. Each year, the total remuneration for candidates will be 168,192,000 SMART.

THE TOTAL REWARD FOR VOTING FOR THE ROUND

Why 115,200 SMART per round?

$115{,}200\ \text{SMART} = \textit{total voting reward per round}\ (\textit{Reward}/\textit{round})$

$\textit{Reward}/\textit{round} = 16\ \textit{SMARTs}/\textit{block} \times 20\ \textit{blocks}/\textit{min} \times 60\ \textit{min}/\textit{hr} \times 6\ \textit{hrs}/\textit{round}$

TOTAL REWARD FOR VOTING PER YEAR

Why exactly 168,192,000 SMART per year?

$168{,}192{,}000\ \text{SMART} = \textit{total voting remuneration for the year}\ (\textit{reward}/\textit{year})$

$\textit{Reward}/\textit{year} = 115{,}200\ \text{SMART}/\textit{round} \times 4\ \textit{round}/\textit{day} \times 365\ \textit{days}/\textit{year}$

b. Block Reward

Also known as the “SR Award,” the top 27 candidates (SRs) selected in each round (6 hours) will be divided among themselves. It is approximately 230,400 SMART. The reward will be divided equally between 27 SR (minus the reward for blocks missed due to a network error). A total of 336,384,000 SMART will be awarded annually to 27 SR.

TOTAL BLOCK REWARD PER ROUND

Why 230,400 SMART per round?

230,400 SMART = *total block reward per round* (*reward per block*/*round*)

Vozn. per block/*round* = 32 *T* SMART/*block* × 20 *blocks*/*min* × 60 *min*/*hr* × 6 *hrs*/*round*

Total block reward per year

Why 336,384,000 SMART per year?

336,384,000 SMART = *total block reward per year* (*per block* / *per year*)

Reward per block / *year* = 230,400 *SMARTs*/*round* × 4 *rounds*/*day* × 365 *days*/*year*

c. Calculation of reward

Calculation of SR reward

total reward = *voting reward* (*VR*) + *block reward* (*BR*)

VR = *total VR* × (*votes received by the SR candidate* / *total number of votes*)

BR = (*total BR*/27) — *missing blocks* × 32

Note: The reward is calculated for SR per round (6 hours)

Calculation of the candidate’s reward from 28th to 127th place in the SR ranking

Total Reward = *Voting Reward* (*VR*)

VR = *total VR* × (*votes received by an SR candidate* / *total number of votes*)

Note: The reward is calculated per SR candidate per round (6 hours)

7.2 The Committee

7.2.1 General information

The committee is needed to change the dynamic parameters of the SMART network, such as block generation rewards, transaction fees, etc. The committee consists of 27 SRs of the current round. Each SR has the right to make proposals and vote on them. When a proposal receives 19 or more votes, it is approved, and the new network settings will be applied during the next maintenance period (3 days).

7.2.2 Creating an offer

Only SR accounts have the right to propose changes to dynamic network settings.

7.2.3 Voting on a proposal

Only committee members (SRs) can vote on the proposal, and a member who fails to vote in time will be considered dissenting. The offer is active for 3 days after creation. Voting can be changed or canceled during the 3-day voting period. At the end of this period, the proposal will either pass successfully (19+ votes) or fail (and end).

7.2.4 Cancellation of the offer

The proposer may cancel the offer before it takes effect.

8. Development of decentralized applications

8.1 Application APIs

The Smart Blockchain Network offers over 60 HTTP API gateways to interact with the network through full and Solidity nodes. In addition, SmartWeb is an extensive JavaScript library containing API functions that allow developers to deploy smart contracts, change the state of the blockchain, request blockchain and contract information, trade on DEXs, and much more. These API gateways can be routed to a local private network, testnet, or Smart Blockchain mainnet.

8.2 Networks

Smart Blockchain has a testnet and a mainnet. Developers can connect to networks by deploying nodes, interacting through SmartStudio, or using APIs through the SmartGrid service. The SmartGrid service consists of clusters of load-balanced nodes hosted on AWS servers worldwide. As the scale of decentralized application development expands, and the volume of API calls increases, SmartGrid successfully copes with the increase in API traffic.

8.3 Tools

Smart Blockchain offers development tools that allow developers to create innovative decentralized applications. SmartBox is a framework that allows developers to test and deploy smart contracts through the SmartWeb API. SmartGrid is a load-balanced hosted API service that allows developers to access the SmartBlockchain network without running their own node. SmartGrid provides access to both the testnet and the Smart mainnet. SmartStudio is an end-to-end integrated development environment (IDE) that allows developers to compile, deploy, and debug their Solidity smart contracts. SmartStudio contains an internal full node that creates a private local environment for testing smart contracts before deploying them.

9. Conclusion

Smart Blockchain is a scalable blockchain solution that uses innovative methods to solve the problems faced by traditional blockchain networks. Smart Blockchain is easily scalable and gives developers unlimited application deployment options. DApps can be built in different languages; anyone can improve the network and run their product on it.

The decentralization of the network and the significant role of SR help improve the blockchain faster, make the network more secure, and protect users' assets.

10. Disclaimer

The information in this analytical report cannot be exhaustive and does not imply any elements of a contractual relationship. The content of this analytical report is not binding on the parties of the company, and the company reserves the right to change, modify, add, or remove parts of this analytical report for any reason at any time before, during, and after the sale of coins by publishing the corrected analytical report on the website.

This analytical report is the company's property and may not be rewritten, copied, transferred to third parties, or distributed in any other way. This analytical report is intended for general information only as a guide to specific conceptual considerations related to the narrow issues it addresses.

This analytical report does not constitute investment, legal, tax, regulatory, financial, or accounting advice and cannot serve as the sole basis for evaluating a coin acquisition transaction. Before purchasing coins, a potential buyer should consult with their legal, investment, tax, accounting, and other advisors to determine such a transaction's potential benefits, liabilities, and other consequences.

Nothing in this analytical report should be construed as a prospectus of any kind or an invitation to invest, nor shall it relate to the offer or inducement to purchase any securities in any jurisdiction. This document is made without considering the requirements of laws or regulations of any jurisdiction that prohibit or in any way restrict transactions concerning or using digital coins and is not subject to them.

The coin is not a digital currency, security, commodity, or financial instrument. It has not been registered under the Securities Act of 1933, the securities laws of any state of the United States of America, or the securities laws of any other state, including the securities laws of any jurisdiction in which the potential holder of the coins is a resident.

Coins are not offered or distributed and may not be resold or otherwise disposed of by their holders to citizens, individuals, or entities whose permanent residence, location, or registration (i) is the United States of America (including the states and the District of Columbia), Puerto Rico, the United States Virgin Islands, any other possessions of the United States of America, or (ii) a country or territory where transactions with digital coins are prohibited or restricted in any way by applicable laws or regulations. If a person subject to these restrictions purchased coins, they did so on an illegal, unauthorized, and fraudulent basis, for which they are liable following the laws of their country.

The Company does not offer or distribute coins, nor does it conduct business (activities) as part of any regulated activity in Singapore, the People's Republic of China, South Korea, or other countries and territories where transactions concerning or using digital coins are subject to restrictive rules or require the company to register or obtain a license with any relevant government authorities.

We remind each coin buyer that this analytical report was submitted to him/her because he/she is the person to whom the document can be legally submitted by the country's laws under whose jurisdiction he/she is located. Each potential buyer of coins is responsible for determining whether they can legally purchase coins from a given jurisdiction and then resell them to another buyer in their country.

A number of the statements, estimates, and financial information in this analytical report are forward-looking. Such forward-looking statements or information involve known and unknown risks and uncertainties that could cause actual events or results to differ materially from those implied or expressed in such forward-looking statements or information.

The Company reserves the right to deny access to the cryptosystem to anyone who does not meet the criteria required to purchase coins, as set forth herein and by applicable law. In particular, the company may deny access to persons who do not meet the eligibility criteria set by the company at any time in its sole discretion.

The analytical report in English is the primary official source of information about the project. The information contained in this document may be translated into other languages from time to time. During such a translation, some of the information in this document may be lost or distorted. The accuracy of such alternative messages cannot be guaranteed. In the event of any contradiction or inconsistency between such translations and this English policy report, the provisions of this English document shall prevail.