Crypto3-Blueprint library to TVC compilation

Introduction

Cryptocurrency is a kind of digital currency, accounting for the internal units of account of which is provided by a decentralized payment system (there is no internal or external administrator or any analogue thereof), which operates in a fully automatic mode. The cryptocurrency itself does not have any special material or electronic form - it is just a number indicating the amount of these units of account, which is recorded in the corresponding position of the information package of the data transfer protocol and often is not even encrypted, like all other information about transactions between system addresses. The term Cryptocurrency was fixed after the publication of an article about the Bitcoin system "Crypto currency" (Cryptographic currency), published in 2011 in Forbes magazine . At the same time, the creator of bitcoin, and many other authors, used the term "electronic cash" (English electronic cash).

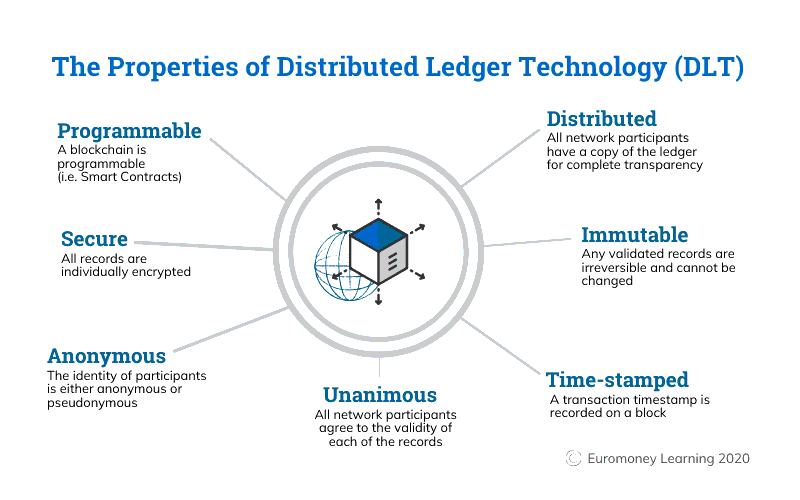
Cryptographic methods are involved in the mechanisms for generating an address and verifying the authority to operate with it (digital signature based on a public key system, the order is available only to the owner of the secret key corresponding to this address), as well as the formation of a transaction package and its relationship with other packages (sequential hashing, which makes it impossible to change information about the amount of cryptocurrency). At the same time, the system does not have any information about the owners of the addresses or about the fact that the address was created (an address can be generated completely autonomously, even without connecting to the network and not reporting anything to the network subsequently) - that is, there is no mechanism to verify that the recipient's address really exists or that the access key to it is not lost. The lack of information about the owner is the basis (but not limited to this) of the anonymity of the participants in transactions. In terms of their economic conditions and consequences, cryptocurrency payments are more similar to cash payments than cashless payment options, although cryptocurrencies are developed primarily for remote purchases (for example, via the Internet).

Crypto3-Blueprint library to TVC compilation will be a decent system for working with crypto data. Written in C ++, it provides reliability and quality in use. This will determine market demand. Payment (transfer of cryptocurrency between addresses) takes place without intermediaries and is irreversible - there is no mechanism to cancel a confirmed transaction, including cases where the payment was sent to the wrong or non-existent address, or when the transaction was made by third parties. No one can block (arrest) cryptocurrency either at a specific address or in general, even temporarily, it is always at the disposal of the owner of the private key to this address.

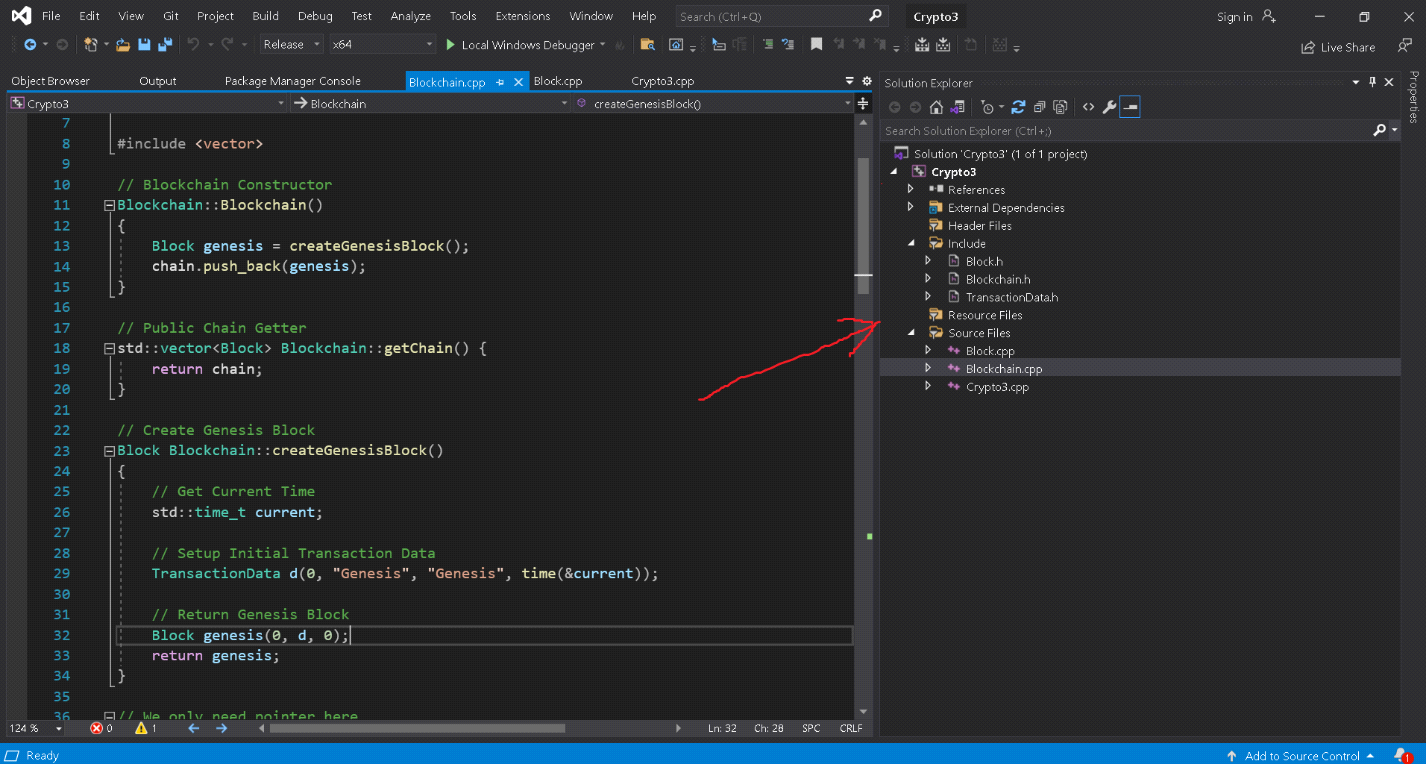
**Specification content**

* **High-level system description**

With the development of electronic systems, ideas have repeatedly arisen to create an electronic analogue of cash for remote payment. But the stumbling block was the potential for double spending of the same funds. When paying in cash, double spending never occurs due to the fact that the payment is accompanied by the transfer of money and the buyer can not pay them again to another seller - because he no longer has this money. But electronic systems are organically able to copy the status, which allows you to make full copies of the system and then make several payments from the same starting state, that is, spend the same money in different directions. The problem was solved only with the help of trusted intermediaries who keep records of payments and guarantee payments only within the funds. This is how all non-cash payment systems work - traditionally intermediaries are banks or other payment system operators. Cryptocurrency technology was originally aimed at the absence of a trusted node - one whose actions are guaranteed to be true and who can confirm the correctness of other people's operations (see the task of Byzantine generals). For the first time, this problem was solved in the Bitcoin system due to the artificial complication of making changes to the register of transaction history. To store information, transactions are combined into blocks, from which a continuous chain (blockchain) is formed. Continuity is ensured not so much by numbering as by including the hash sum of the previous block in the current block, which does not allow changing the information in the block without changing the hashes in all subsequent blocks. All hashes meet certain requirements, generating hashes that meet these requirements is time consuming or very expensive. Only the longest chain is considered true. In different cryptocurrencies, the right to form the next block is given to the one who has performed a certain job (Proof-of-work), has a certain amount in the account (Proof-of-stake), provided some resources (Proof-of-space) or is based on another procedure easy to check but difficult to perform or forge.



What is the importance of the blockchain: business depends on data. Data acquisition speed and accuracy are crucial. Blockchain is ideal for providing such information, as it offers authorized network members instant, shared and fully transparent access to information in a fixed registry. The blockchain network allows you to track orders, payments, accounts, goods and more. And because all participants share a single source of reliable data, you can view all transaction information at any time to work more confidently and gain new benefits and opportunities.

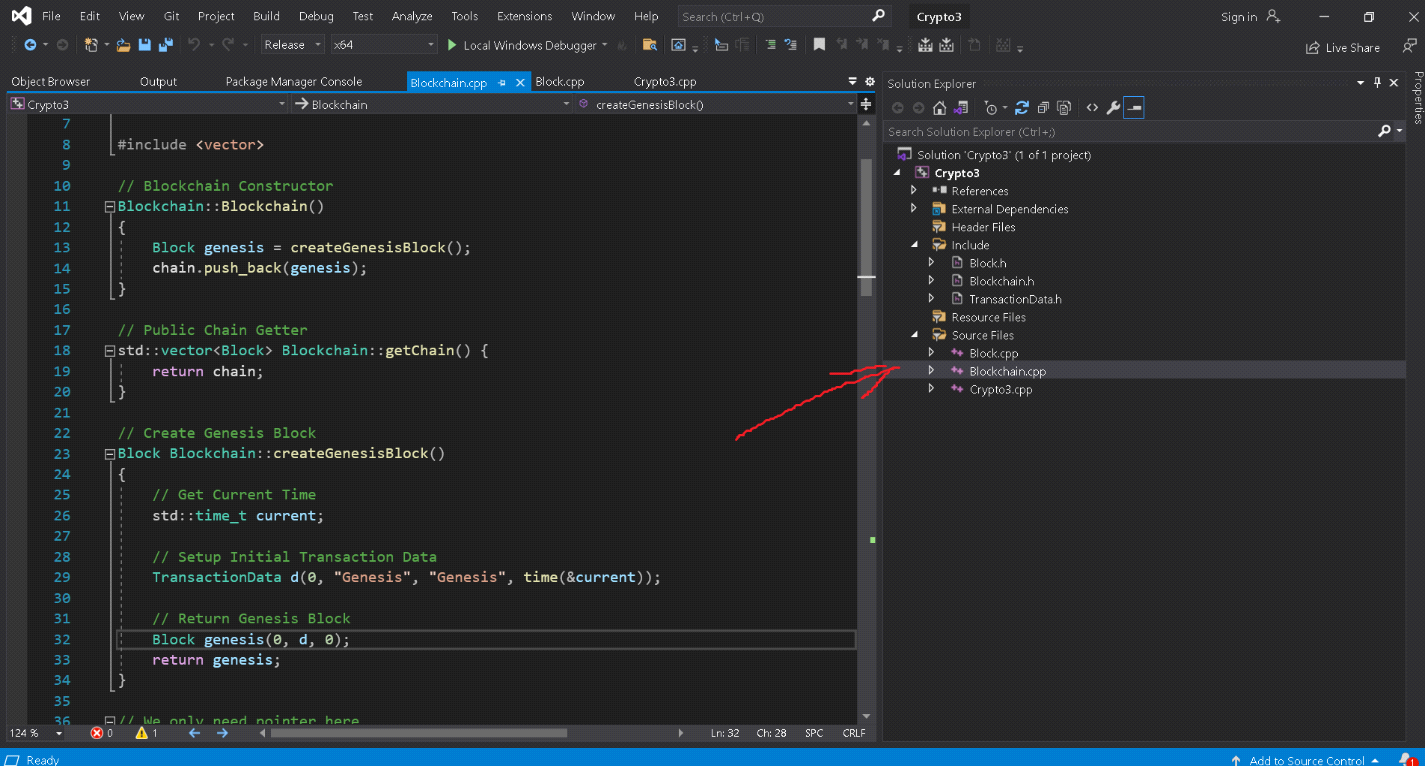


Crypto3-Blueprint library to TVC compilation consists of many elements of the system that provide a single whole work with data.

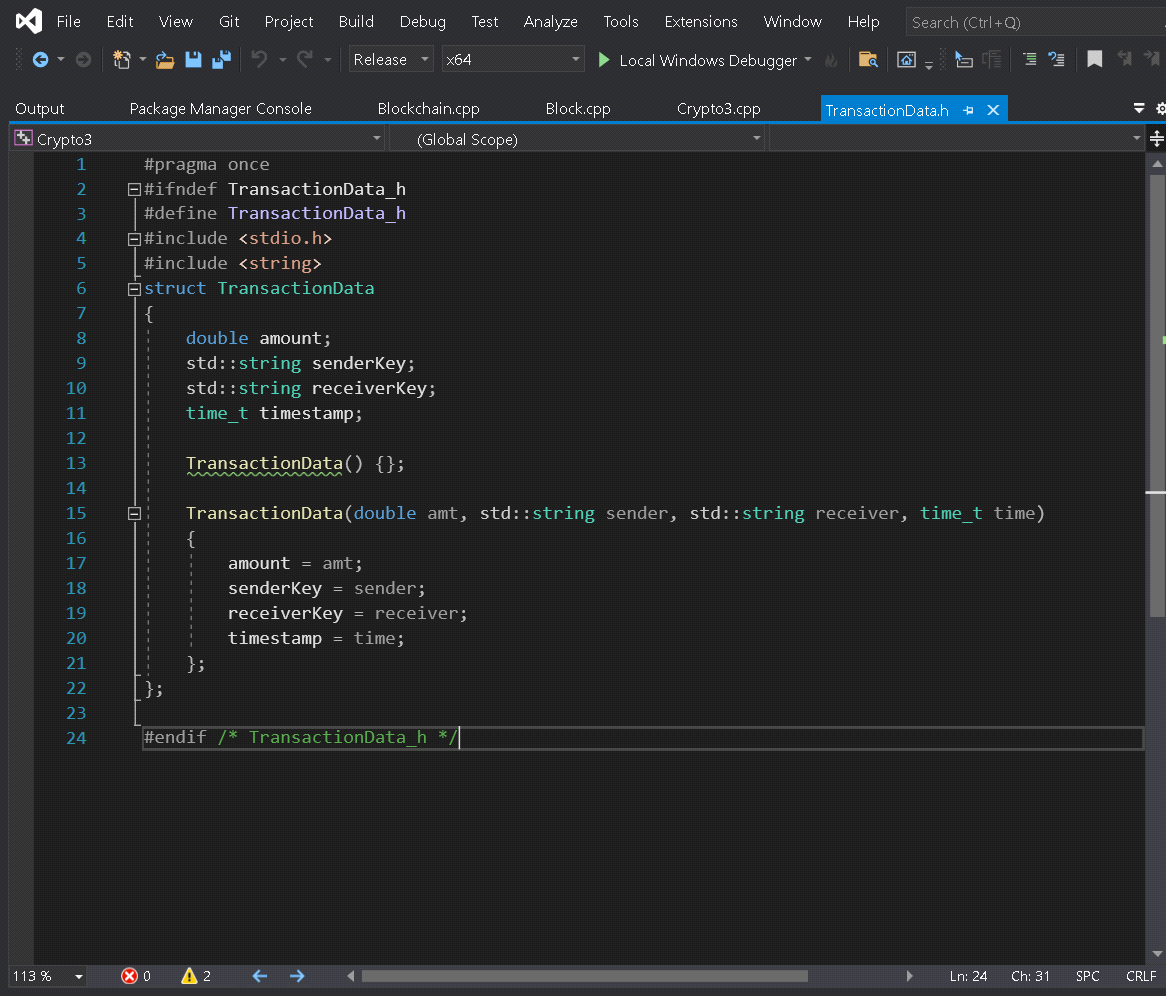
Blockchain , originally block chain - a chain of blocks - a continuous sequential chain of blocks (connected list) containing information, built according to certain rules. The connection between the blocks is provided not only by numbering, but also by the fact that each block contains its own hash sum and the hash sum of the previous block. Changing any information in the block will change its hash sum. To comply with the rules of chain construction, hash-sum changes will need to be written to the next block, which will cause changes to its own hash-sum. The previous blocks are not affected. If the unit to be changed is the last in the chain, then making changes may not require significant effort. But if after the changed block the continuation is already formed, change can appear extremely labor-consuming process. The fact is that copies of blocks of blocks are usually stored on many different computers independently of each other .

The term first appeared as the name of a fully replicated distributed database implemented in the Bitcoin system, which is why the blockchain is often identified with the registry of transactions in various cryptocurrencies. However, blockchain technology can be extended to any interconnected information block . Launched in October 2008, Bitcoin was the first application of blockchain technology.

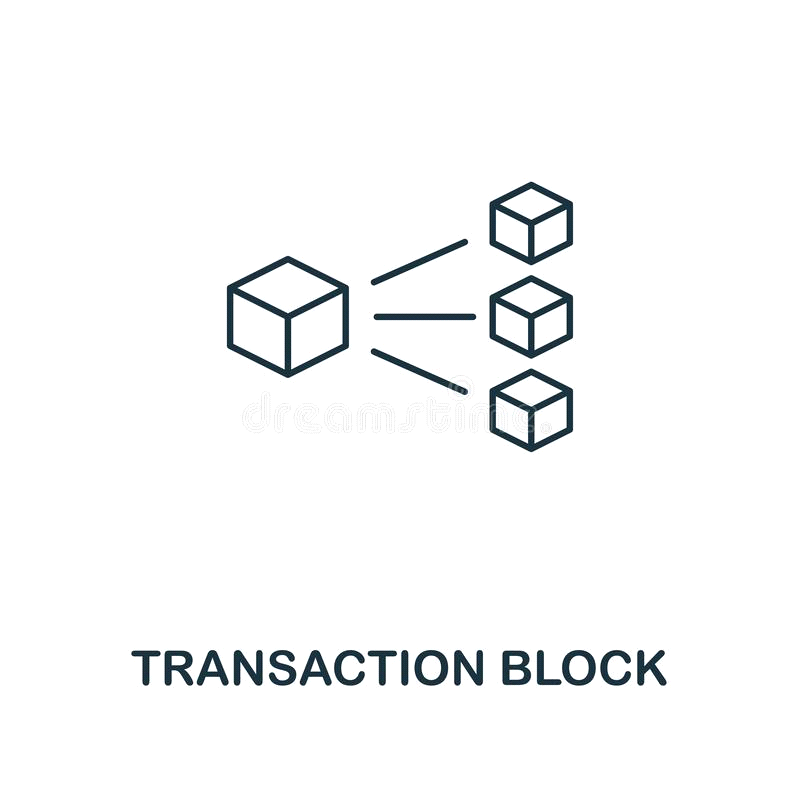
Nowadays, blockchain is used in such areas as financial transactions, user identification or the creation of cybersecurity technologies [6]. Blockchain technologies are relevant primarily to banking institutions and government organizations.



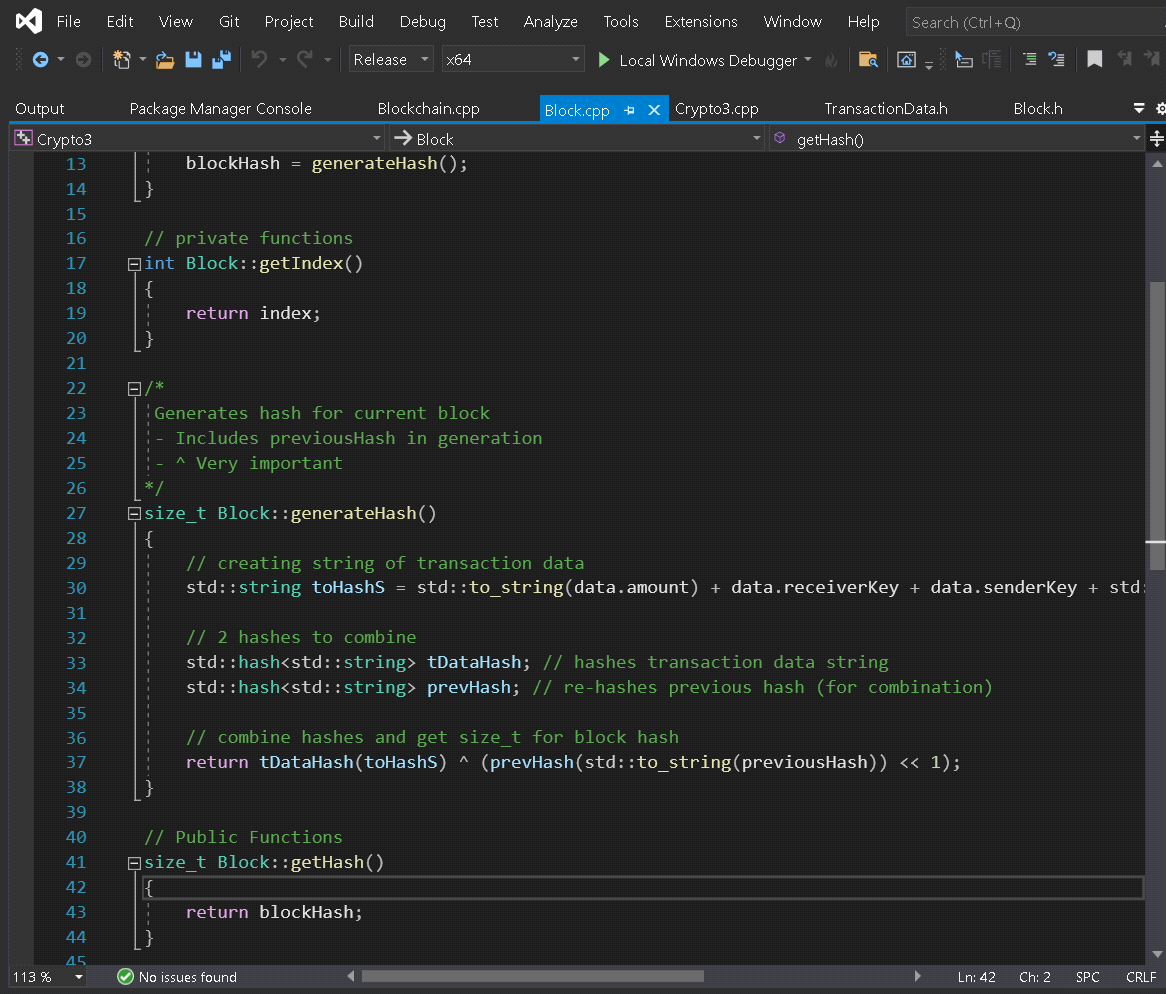
Transaction block is a special structure for recording a group of transactions in the Bitcoin system and similar. A transaction is considered complete and authentic ("confirmed") when its format and signatures are verified, and when the transaction itself is grouped with several others and recorded in a special block structure. The contents of the blocks can be checked, as each block contains information about the previous block. All blocks are built into one chain, which contains information about all the operations ever performed in the database. The very first block in the chain - the genesis block - is considered a separate case, as it has no parent block.



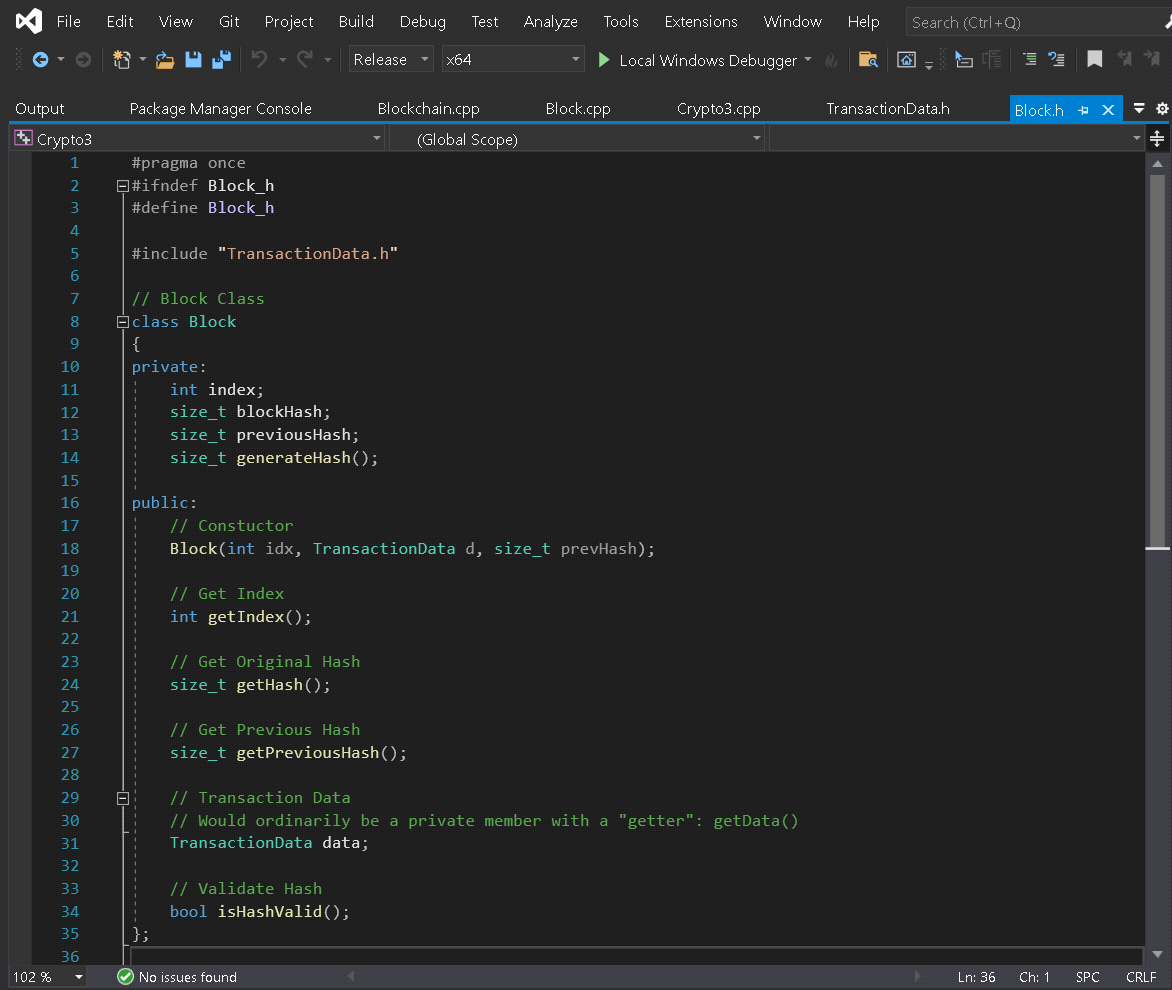
The block consists of a header and a list of transactions. The block header includes its hash, the previous block's hash, transaction hashes, and additional service information. In the Bitcoin system, the first transaction in a block always indicates the receipt of a commission, which will be a reward to the miner for the created block.



The following is a list of transactions formed from a queue of transactions not yet recorded in previous blocks. The criterion for selection from the queue is set by the miner himself. It doesn't have to be a timeline. For example, only transactions with a high commission or with a specified list of addresses may be included. The created block will be accepted by other users if the numerical value of the header hash is equal to or less than a certain target number, the value of which is periodically adjusted. Because the hash result of the SHA-256 function is considered irreversible, there is currently no algorithm for obtaining the desired result other than random search. If the hash does not satisfy the condition, the nonce parameter changes in the header and the hash is recalculated. Usually (statistically) a large number of recalculations is required. When the option is found, the node sends the received block to other connected nodes, which check the block. If there are no errors, the block is considered added to the chain and the next block must include its hash.



The created block will be accepted by other users if the numerical value of the header hash is equal to or less than a certain target number, the value of which is periodically adjusted. Because the hash result of the SHA-256 function is considered irreversible, there is currently no algorithm for obtaining the desired result other than random search. If the hash does not satisfy the condition, the nonce parameter changes in the header and the hash is recalculated. Usually (statistically) a large number of recalculations is required. When the option is found, the node sends the received block to other connected nodes, which check the block. If there are no errors, the block is considered added to the chain and the next block must include its hash.



* **Risks**
* Government agencies can negatively affect circulation and even ban them.
* Losing the password to the e-wallet will result in the loss of all cryptocurrencies.
* The more complex the algorithms (the tasks that computers solve), the harder it is to have cryptocurrency on home computers.

This software system, like any system, will always have its risks to deal with.

As a technology for building massively distributed databases, the blockchain experiences a number of specific problems that make it difficult to use. Among these problems are the following:

The development of new types of blockchain is often associated with overcoming or circumventing these problems and limitations. At the same time, there are a number of functions that no blockchain system can do without:

Data is stored in a block chain structure in which each block is linked to the previous one. Changing the information in a block is impossible without making changes to all subsequent blocks.

Each member of the network has a copy of all data (the entire block chain). Participants interact with each other in a peer-to-peer format ((peer-to-peer).

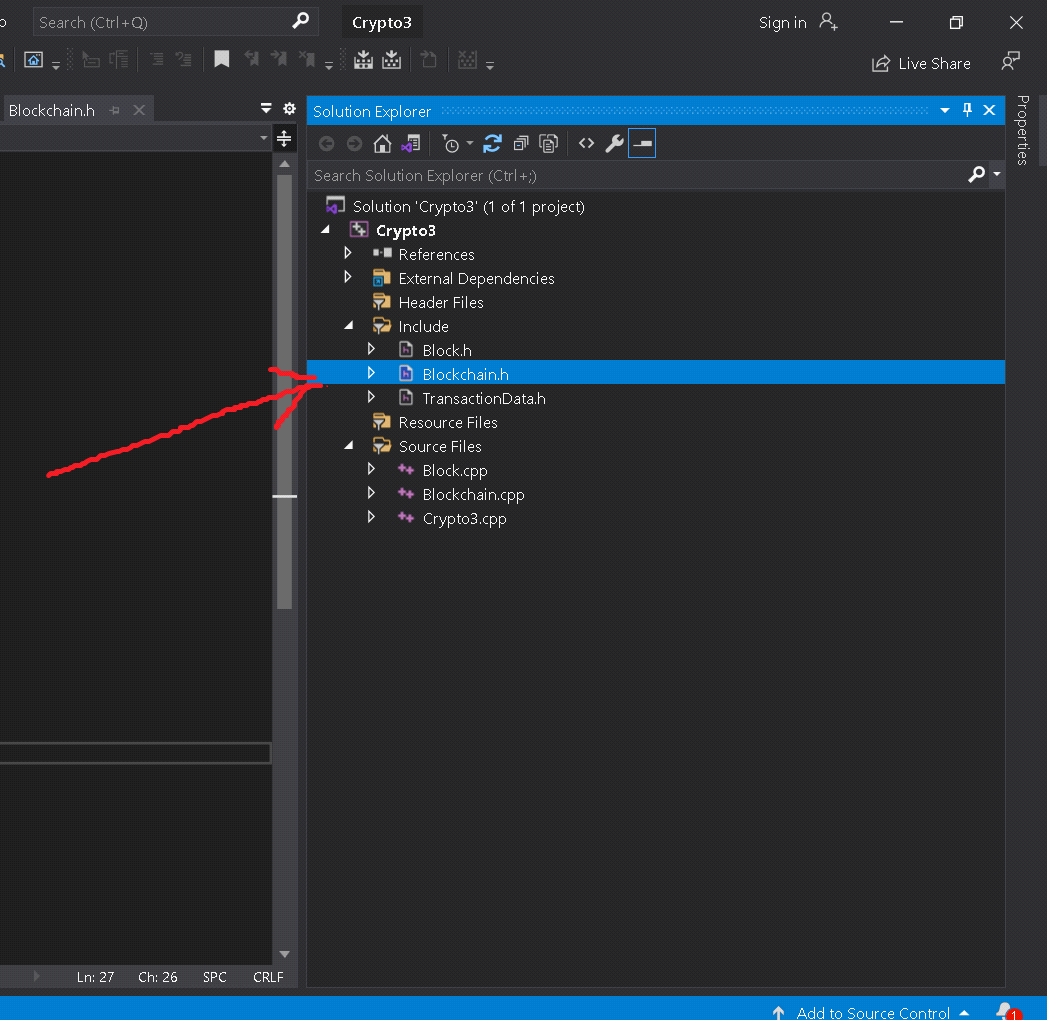
A consensus mechanism has been established - a certain interaction of nodes that ensures the achievement of agreement on the correctness of the information recorded in the next block of the chain and the choice of a block included in the chain from several possible alternatives.

Vitalik Buterin in his article “On Public and Private Blockchains”[28] (2015) identified three types of blockchains: public, private and consortium. Buterin notes that a wide variety of mixed forms are possible (for example, private smart contracts on a public blockchain, an exchange gateway between public and private blockchains) that are optimal for a particular industry or problem being solved. In some cases, openness is clearly better, in other cases, administrative control is simply needed.

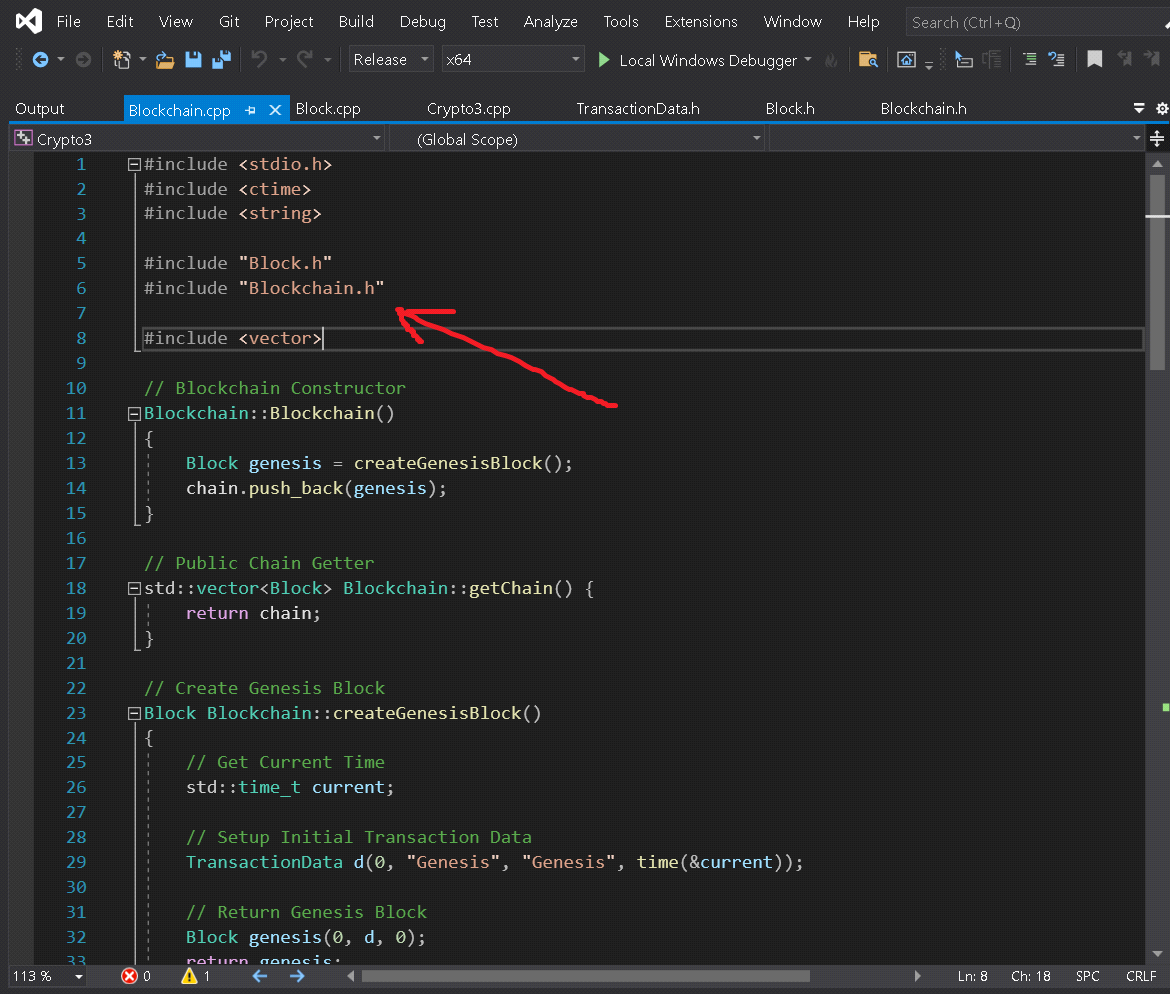
* **System Properties**

The blockchain is formed as a continuously growing chain of blocks with records of all transactions. Copies of the database or its part are simultaneously stored on multiple computers and synchronized according to the formal rules of building a chain of blocks. The information in the blocks is not encrypted and is available in the open, but the absence of changes is verified cryptographically through hash chains (digital signature element).

This software system consists of three files that always interact with the system without these files the system will not work properly.

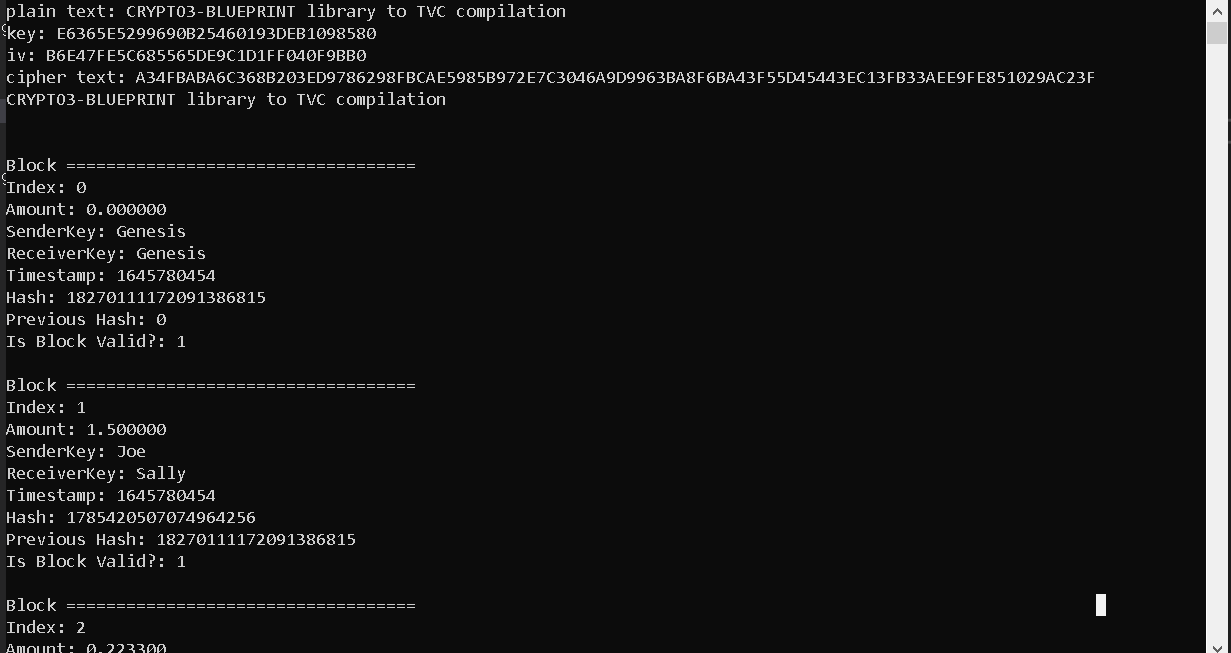


By importing them, we get access to all the features of header files. The database publicly stores information about all transactions signed using asymmetric encryption in an unencrypted form. To prevent multiple spending of the same amount, timestamps are used, implemented by splitting the database into a chain of special blocks, each of which, among other things, contains the hash of the previous block and its serial number.

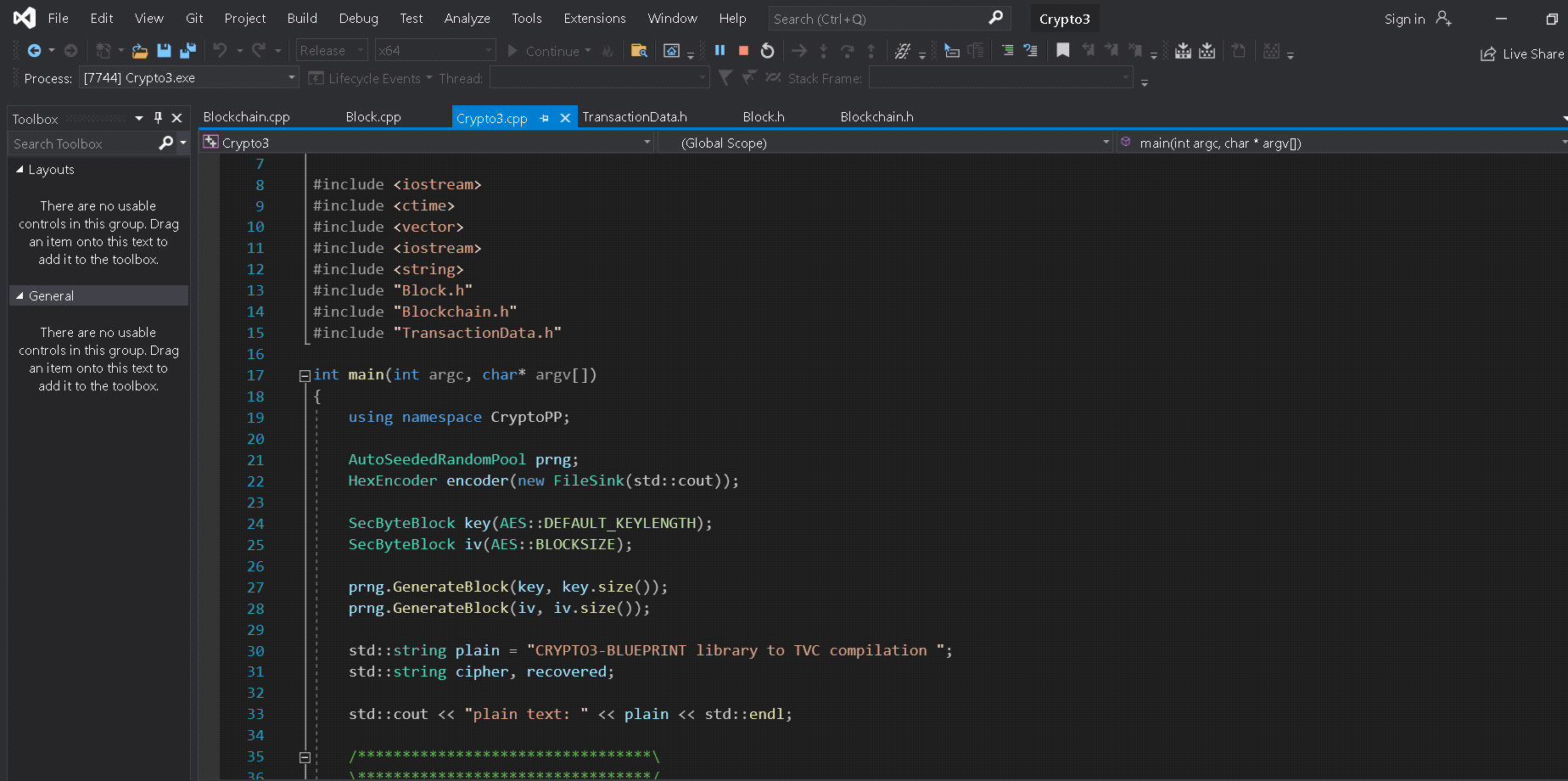


Currently, representatives of various fields are showing interest in blockchain technology. At the same time, the degree of interest of companies in different sectors of the economy varies significantly. The financial sector is actively preparing for the widespread introduction of blockchain, while manufacturing enterprises leave this technology unattended. Many authors consider exclusively options for decentralized public blockchains, considering centralized blockchains to be “wrong”, variations of outdated administrative technologies. Most often, objections to private or consortium blockchains are more of a philosophical or rebellious nature, although there are classes of tasks that managed or mixed blockchains cope with an order of magnitude better than decentralized ones.

This software system is presented in the form of a console program



In consortium blockchains, the negotiation process is provided by several predetermined peers. For example, a consortium of 15 banks agrees to validate a block with a multi-signature of at least 10 consortium members. The rate at which new blocks appear can be quite high. At the same time, the members of the concern can make access to information from the blockchain both publicly available and restrict it to a select circle or introduce other quantitative, content or time restrictions. These blockchains can be considered “partially decentralized.”



* **Appendix**

Crypto++ (also known as CryptoPP, libcrypto++, and libcryptopp) is a free and open-source C++ class library of cryptographic algorithms and schemes written by Wei Dai. Crypto++ has been widely used in academia, student projects, open source and non-commercial projects, as well as businesses. Released in 1995, the library fully supports 32-bit and 64-bit architectures for many major operating systems and platforms, including Android (using STLport), Apple (Mac OS X and iOS), BSD, Cygwin, IBM AIX and S/390, Linux, MinGW, Solaris, Windows, Windows Phone and Windows RT. The project also supports compilation using C++03, C++11, C++14 and C++17 runtime libraries; and a variety of compilers and IDEs, including Borland Turbo C++, Borland C++ Builder, Clang, CodeWarrior Pro, GCC (including Apple's GCC), Intel C++ Compiler (ICC), Microsoft Visual C/C++, and Sun Studio.

Crypto++ 1.0 was released in June 1995, but the download is no longer available. The Crypto++ 1.0 release was withdrawn due to RSA Data Security, Inc asserting a copyright claim over the RSA algorithm. All other versions of the library are available for download.

In a 2007 ECRYPT workshop paper focusing on public key implementations of eight libraries, Ashraf Abusharekh and Kris Kaj found that "Crypto++ 5.1 leads in terms of support for cryptographic primitives and schemes, but is the slowest of all investigated libraries."

In 2008, speed tests carried out by Timo Bingmann using seven open-source security libraries with 15 block ciphers, Crypto++ 5.5.2 was the top performing library under two block ciphers, and did not rank below the average library performance under the remaining block ciphers.[8]

Crypto++ also includes an auto-benchmarking feature, available from the command line (cryptest.exe b), the results of which are available at Crypto++ 5.6.0 Benchmarks.

As with many other cryptographic libraries available for 32-bit and 64-bit x86 architectures, Crypto++ includes assembly routines for AES using AES-NI. With AES-NI, AES performance improves dramatically: 128-bit AES/GCM throughput increases from approximately 28.0 cycles per byte to 3.5 cycles per byte.

* **Specification Purpose**

The algorithm of the blockchain system consists in the process of data encryption (hashing), which is carried out by a computer network consisting of a large number of computers. Data is distributed among network participants according to the principle of torrent distribution of files.

Computers perform calculations, get a certain result, and assign a unique signature (signature) to a block of data - this is something like a fingerprint. The registry is updated and a new block of data is formed, which will not be possible to change in the future. This means that it will be impossible to fake them. The only operation possible in a block is adding new records to it. The registry is updated simultaneously on all computers on the network.

* **Specification Evaluation**

People can send bitcoins to others using mobile applications or computers. With the help of bitcoins you can pay for goods and services on the Internet, or even for training: on the website of the Ukrainian platform for finding online teachers Preply you can pay cryptocurrency for classes with native English or any other language, or school lessons.

Risks in this area will always be the same as in any software system even more. You need to follow the rules and regulations when working with such systems as the government may prohibit their use.

Crypto3-Blueprint library to TVC compilation It will be a reliable system that will be able to overcome most opponents in the market and will be in great demand due to the reliability of the system and quality.