Secure System for Crypto Currencies based on Virtual Accounts and Virtual Currencies

Author: Sead Muftic
BIX System™ Corporation
sead.muftic@bixsystem.com

ABSTRACT

The paper describes the concept and details of the design of the new system that supports secure, reliable, instantaneous, and peer-to-peer transactions with crypto currencies. The most popular crypto currency is Bitcoin, but this system is also applicable to any other crypto currency. Current concepts, implementations, and operational experiences with Bitcoin and other crypto currencies have many problems. Some of them are so serious that they jeopardize future large-scale use and even survival of crypto currencies. Thus far, some solutions proposed for these problems have had unacceptable consequences, such as splitting Bitcoin into two systems, extending the block size, and speeding up validation procedures. This paper describes an innovative system with two major characteristics: (a) it solves most of the problems with current crypto currency systems, and (b) it is compatible with current systems, i.e. it does not require any of their modifications or hard fork splits. The new system is based on four innovations. First, the system introduces an additional meta-system based on the use of *virtual accounts* for crypto currencies. With this new approach all transactions are performed within the meta-system. Transactions with the original systems are used only occasionally for "cash-in" and "cash-out" transfers between any crypto currency and its virtual equivalent. Second, the system uses special cryptographic protocols of *multi-party signatures* and *cryptographic enveloping* to validate users' addresses, identities, and transactions. Therefore, it does not use blocks, their chaining, miners, or any other trusted third parties. Third, the arrangements for trading crypto currencies is based on *community auctions* and not on centralized or distributed exchanges. Therefore, the system does not use any centralized components and performs instantaneous, truly peer-to-peer transactions. All users have full privacy and anonymity. Fourth, the system uses the method of *sponsored encapsulation of accounts* and *user identities*, which eliminates the possibility of illegal transactions such as money laundering or collecting of ransom payments.

THE FIELD OF RESEARCH

This paper is related to a general category of secure transactions with crypto currencies in an open digital communication environment. The paper is focused on use of special types of virtual accounts, cryptographic protocols, and secure, global, distributed, append-only financial ledger to eliminate the problems associated with current standard systems for payment using crypto currencies.

1. BACKGROUND – THE CONCEPT OF THE BITCOIN SYSTEM

1.1. Introduction and General Description of the Bitcoin System

Various authors describe the Bitcoin system in many ways, as an innovative currency, as a form of peer-to-peer electronic cash payment, or as a decentralized and anonymous payment system. In this paper, the Bitcoin system is treated as a payment system. It has its own features, currency, protocols, and components, all of which support payments between two parties—the party that makes a payment and the party that receives the payment. This approach is based on the description of the Bitcoin system in one of its standardization documents: "*It is a decentralized digital currency that enables instant payments to anyone, anywhere in the world. Bitcoin uses peer-to-peer technology to operate with no central authority: transaction management and money issuance are carried out collectively by the Bitcoin network.*"

The system is decentralized since users are globally distributed and they can perform transactions within the global community of registered users. The digital currency used in the system is not an electronic form of real currency, but a special type of currency generated and used only within the Bitcoin system. This concept is based on the notion that money or value can be interpreted as any digital object or digital asset accepted as payment for goods and services and repayment of debts in a given country or socio-economic context. In addition, the Bitcoin system uses cryptography to control the creation and transfer of money rather than relying on central authorities and classical financial institutions.

There are several important requirements for any type of payment with any currency. The best example of a "perfect" payment transaction that meets all these requirements is payment using cash over the counter. The transaction is *instantaneous*, as the paper bill is transferred from the consumer's hand to the merchant's. It is *cheap*, with no overhead charge to perform the transaction, so the merchant receives the full amount. It is *irreversible*, which is beneficial to merchants. It is *legal*, as the merchant can verify the legality of the paper bill. And, finally, it is *anonymous* for the consumer, as he/she does not need to reveal his/her identity in order to make the payment. The only practical problem with payments using cash is managing cash itself, as using and handling cash has many disadvantages. The Bitcoin system solves all the issues regarding the use of cash as well as provides advantages for transactions using digital and communication technologies. In this way, bitcoins are effectively a type of "digital cash" that may also be used for payments over the counter.

One of the most significant features of payment transactions using cash over the counter is that *no third parties* participate in or assist the transaction. This feature makes execution of transactions very efficient for both parties and cheap for the merchant. Other common types of payment systems, such as bank-to-bank account transfers or bankcards, involve many additional parties and use very complicated background infrastructures in order to validate and clear payment transactions. These infrastructures are complex and expensive to establish and operate and vulnerable to attacks by hackers. The Bitcoin system does not use a complex infrastructure, which allows its transactions to be efficient and cheap. Transactions involving third parties also require complete *trust* in these parties without any means to verify their functionality, correctness, or security. Moreover, with these types of transactions and third-party infrastructures, none of the parties have privacy.

The Bitcoin system uses public-key cryptography to protect its users, currency and transactions. The logical relationships between transaction parties are direct and peer-to-peer, and the process of validating transactions is based on a cryptographic proof-of-work system. In such a system, a certain number of bitcoins are transferred from one cryptographic address (the Bitcoin account of the sender) to another address (the Bitcoin account of the recipient). Each user may have and may use several Bitcoin accounts simultaneously. When making a payment the sender sends the transaction to its associated Bitcoin network server. That server broadcasts the transaction to all other servers in the Bitcoin network of distributed transaction processing servers, which collect individual transactions, package them into blocks, submit them to miners for validation, and then, after validation, distribute them back to all members of the Bitcoin system.

Each block of transactions created during the last ten minutes is cryptographically processed by a large number of so-called "miners," which attempt to create special cryptographic hash values. This is computationally a very difficult and time-consuming task and therefore is very difficult to repeat. Individual blocks are validated using cryptographic processing procedures that require a substantial amount of work and computing power.

Approximately an hour or two after submitting the transaction for validation, each transaction is locked in time by cryptographic processing due to the massive amount of computing power that was used to complete the hash of the block. When the block is validated, it is added to the chain of all previous blocks, which serves as a public archive of all blocks and transactions in the Bitcoin system.

One of the most important problems with uncontrolled digital currency, for which there are no third parties to validate and approve transactions, is so-called *double spending*. Since the currency is digital and stored on users' local workstations, mobile phones, or network servers, the same amount of currency can be easily copied and sent to multiple recipients multiple times. The Bitcoin system is the first effective example of a solution to the double-spending problem without the assistance of any third party. It keeps and distributes an archive of all transactions among all users of the system via a distributed Bitcoin network. Every transaction that occurs in the Bitcoin system is recorded in that publicly distributed transactions ledger. Since the components in that ledger are blocks containing transactions and the blocks are "chained" in time and a cryptographic sequence, the ledger is called the *blockchain*. The full blockchain of all transactions using bitcoins performed before the specific transaction is used to verify the validity of new transactions and prevent double–spending. In essence, transactions are verified by testing the balance of the sending account; a payment can be made only if the balance of the outgoing account is equal to or larger than the payment amount. The current balance of an account is established by tracing the history of all incoming and outgoing transactions for that account.

The procedure to verify the validity of individual transactions and prevent double spending is based on the use of a special cryptographic protocol called *public-key cryptography*. With this type of cryptographic system each user has two cryptographic keys. Whatever one key encrypts, the other key decrypts. One of the two keys is a *private key* that is kept secret, and the other is a *public key* that can be shared with all other users in the system.

When a user wants to make a payment to another user, the sender transfers a certain amount of Bitcoin from his/her account to the receiver's account. The sender creates payment message called a "payment transaction," which contains the sender's public key—the sending Bitcoin address—and the recipient's public key—the receiving Bitcoin address—as well as the payment amount. The transaction is cryptographically processed by the sender's private key, an operation that is called *digital signing*, and the resulting digital signature is appended to the transaction. Using sender's public key allows every other user in the Bitcoin system to verify that the transaction was indeed initiated by the indicated sender as his/her public key can successfully decrypt the content of the digital signature contained in the payment transaction object.

In addition, the exchange is authentic since the transaction was also cryptographically processed with the recipient's public key, an operation called *digital enveloping*. This guarantees that the payment can be accepted and processed only by the holder of the corresponding private key, which is the intended recipient.

Every transaction, and thus transfer of ownership of a specified amount of bitcoins, is inserted, time-stamped, and displayed in one "block" of the blockchain. Public-key cryptography ensures that all computers in the network have a constantly updated and verified record of all transactions within the Bitcoin network, preventing double-spending and fraud.

1.2. Claimed Features and Properties of the Bitcoin System

There are many concepts for payment systems and even more in operation. Some are paper–based and others are digital and network-based. Bitcoin's core characteristics are what make it unique and distinctive compared with all other payment systems in use today.

First, the system uses *its own currency*, called a *bitcoin*. This is a *crypto currency*, meaning that new amounts of currency are generated and used based on the execution of certain cryptographic algorithms and protocols. Specific cryptographic protocols are used to create new Bitcoins, transfer them between parties, and validate the correctness of payment transactions.

Second, the relationship between the two parties involved in a transaction is direct and *peer-to–peer* (i.e. no other parties participate in the transaction). This contributes to the efficiency of the system compared to current common financial payment infrastructures and protocols, which are complex and expensive. However, the process of distributing transactions to their validators and then to all other members in the Bitcoin system is very complex and includes many parties. Therefore, the claim that Bitcoin is a peer-to-peer payment system is not correct.

Third, Bitcoin system claims *anonymity of users*, including their accounts and transactions; the identities of participants in the system are not known even to their transaction partners. All other system operations (receiving payments, making payments, validating transactions, etc.) are also claimed to be anonymous. However, in actuality, participants in the Bitcoin system have *pseudo-anonymity*. When validating transactions all previous transactions of the sender are traced back to the initial transaction. If that initial transaction was the purchase of bitcoins at a Bitcoin exchange, then the user's identity can be known. Therefore, the claim that Bitcoin transactions are anonymous is also not correct.

Fourth, the Bitcoin system is *not controlled* by any institution, regulatory body, group, or financial authority. This means that the currency and all transactions are exempted from all legal and financial rules and regulations. However, there are rules controlling Bitcoin transactions built into the code of the Bitcoin network servers, a phenomenon usually called "*rule by technical code*" and sometimes described as "control by the community" (i.e., by the users participating in the system). However, even this claim is not correct, as the Bitcoin network recently introduced a network fee without Bitcoin users' input.

1.3. Claimed Innovative Contributions of the Bitcoin System

In addition to an effective procedure for transferring an amount of crypto currency from one user (sender's Bitcoin account) to another user (receiver's Bitcoin account), the major essential contributions of Bitcoin are its method of validating credibility of two mutually unknown and otherwise unrelated parties and ensuring that transactions are anonymous and secure in the open environment of the Internet. In all current large-scale financial systems, these problems are solved by using third parties. Those third parties are often integrated and linked into a large, complex, expensive, and vulnerable operational infrastructure. Current examples of such infrastructures are the infrastructure for authorizing and validating bankcard payments, the infrastructure that supports international financial transfers (SWIFT), Public–Key Infrastructures (PKIs), various global identity management systems, and large and popular social websites. It is generally agreed that such infrastructures are inefficient, expensive, and, most importantly, vulnerable to external and internal attacks. In addition to the complexity and vulnerabilities of such operational support infrastructures, users must put complete trust in third parties in order to use their services.

Bitcoin, however, effectively solves these problems.

Bitcoin allows an Internet user to transfer or share not only bitcoins but also any other form of digital asset to another Internet user. The transfer is guaranteed to be safe and secure, as everyone knows that the transfer has been performed and nobody can challenge the legitimacy of the transfer.

Other new, creative, and innovative ideas similar to the Bitcoin system have been used to perform secure and reliable transactions of digital assets between users in an open community. Examples of such applications include commercial transitions, real estate transactions, energy trading, electronic voting, medical applications, and many others. That is the main reason why the concept of a blockchain, a technology supporting validation of all such transactions, is considered an innovative and disruptive technology.

However, as will be shown in the next section, the Bitcoin blockchain is very limited and can be used only for Bitcoin payments. Furthermore, due to various conceptual, operational, and technical problems, at the time this paper was created, the Bitcoin community is becoming aware of many serious problems with Bitcoin and actively working on solutions. The next section will also show that most of the potential solutions at the time of this paper were not efficient or satisfactory, and some introduced new problems.

2. PROBLEMS AND CURRENT (INADEQUATE) SOLUTIONS

2.1. False and Incorrect Claims of the Bitcoin System

It is interesting to emphasize that most, if not all, of the claimed features of the Bitcoin system, are inaccurate. First, Bitcoin payment transactions are not peer-to-peer; they are performed between the sender and Bitcoin network. Second, payment transactions are not instantaneous, but have a delay of at least one hour until they are finally approved. Third, the Bitcoin system does involve third parties (miners and exchanges). Furthermore, in order to operate as designed, the members of the Bitcoin system must put complete trust in miners and their operations. So, the Bitcoin system is, in fact, based on trust. Additionally, transactions are not anonymous, as users can be traced either to miners, who must be registered before validating blocks, or to exchanges, where users must be registered to buy or sell bitcoins. As listed in the next three sections, the current Bitcoin system's deficiencies, problems, and weaknesses jeopardize the long-term stability and use of the Bitcoin system. Thus, it is necessary to create a new Bitcoin system that actually possesses the properties claimed by the original Bitcoin system and can support both Bitcoin and other crypto currencies. This new system is described in this paper.

2.2. Problems with the Concept of the Bitcoin System

The problems associated with the Bitcoin system are listed below:

Problem C-1: Block Size – The blocks used in the Bitcoin system are too small; one block can accommodate only a limited number of transactions. As usage of the Bitcoin system increases, individual blocks cannot contain all transactions generated in the last ten minutes. This causes many transactions to be delayed by several blocks, which increases the processing time of transactions. In addition, the Bitcoin network and its blocks are increasingly used to validate transactions not involving Bitcoin; since many applications "piggyback" their transactions on the Bitcoin network, the small size of blocks represents a serious problem.

This problem cannot be solved by simply increasing the size of the blocks. Cryptographic operations to validate blocks (i.e., mining), are performed by hardware chips and hardware boards that specify the size of the block in their hardware logic, so the size of blocks cannot be easily increased. In addition, such a solution would not be backward-compatible with the blockchain created during the lifetime of the Bitcoin system.

Problem C-2: Transaction Validation Time – In the current Bitcoin system, the difficulty level for miners is adjusted to be one hash produced, on average, every ten minutes. This means that the number of leading zeroes in the acceptable hash is specified in such a way that the distributed network of miners performing cryptographic validation of the blocks can create a valid hash of each block in about ten minutes. This means that there is a significant delay in the procedure to validate individual blocks. Furthermore, due to potential forks in the blockchain and the need for their synchronization, final validation of transactions requires about six blocks (about one hour). Thus, Bitcoin transactions are not instantaneous.

This problem could be solved by simply lowering the target value so that hashes of blocks are created, on average, in less than ten minutes. However, this approach would have a direct negative effect on the overall security of the Bitcoin system; if miners could produce the hash in a shorter period of time, so could hackers, and the system would become vulnerable to illegal modification of transactions and their insertion in the blocks.

Problem C-3: Potential Hashing Problem – Miners perform repetitive trials to produce valid hashes by creating random values, inserting them in the completed block, and then trying to create an acceptable hash of such block. This system is based on the assumption that such a hash exists. However, if an acceptable hash cannot be created with any random value for a given block, then the block could not be validated and the entire Bitcoin system would be stalled.

This problem could be solved by slightly modifying the problematic block so that the new block with a random value would still produce an acceptable hash. However, modification of the current block would require the same intervention throughout the entire Bitcoin system (consensus). Such a protocol does not exist in the current version of the Bitcoin system and its introduction would require re-engineering and re-deployment of the entire Bitcoin system (i.e., all Bitcoin network and mining nodes).

Problem C-4: Dependence on Trusted Third Parties – The current version of the Bitcoin system depends on third parties (i.e., miners). If the miners were to stop mining, the entire system would be blocked. Members of the Bitcoin system are forced to trust miners to perform their operations correctly and in a timely manner. However, as has been reported in the literature, there are many opportunities for miners to cheat the system through, for example, selfish mining and delays in releasing validated blocks. Furthermore, since the priority of transactions to be included in blocks depends on their fee, with the increased overload of blocks in order to raise processing priority transaction fees are significantly increasing and becoming very expensive.

Problem C-5: Distribution of Bitcoin Addresses – Bitcoin addresses are random strings and therefore their values cannot be effectively validated by their recipients. The only way to validate them would be to open the cryptographic envelopes created by these public keys. But that requires users' private keys and therefore this approach is practically impossible. Thus, the distribution of Bitcoin addresses is unreliable and can cause serious problems. If the recipient's Bitcoin address were incorrect due to, for example, accidental modification during the transfer to the sender to make payment, the sender would send the payment to an invalid address. This address is a "black hole" as those bitcoins would be permanently lost as they are not recoverable.

This problem can be solved by extending distribution of Bitcoin addresses between parties with some form of integrity / correctness verification mechanism applied to these addresses. The approach would be to distribute Bitcoin addresses as cryptographically self-signed objects, so that the public key contained in such objects would be used to validate the signature of the object. This solution is not impossible and would not have any serious effect on the operations of the current Bitcoin system as it is outside the scope and functionality of the standard Bitcoin protocol.

Problem C-6: Anonymity of Users – It has already been mentioned that Bitcoin's claim that users and their addresses are anonymous is not completely true. Methods of receiving bitcoins (through mining or by purchase at exchanges) require users to be registered, revealing their identity. Even if they receive bitcoins from a partner without mining or purchasing, users' identities can be revealed by analyzing various properties of the protocol and tracing previous transactions.

Minor modification of current Bitcoin operational procedures and concepts cannot adequately solve this problem, as users can be traced even if they use only standard Bitcoin payment transactions. Thus, to ensure the full anonymity of users, an innovative solution is needed.

Problem C-7: Loss of Bitcoins – Bitcoins are stored in so-called Bitcoin wallets on users' workstations, smartphones, or servers. In case of a crash, hardware malfunction, or loss of devices, the stored bitcoins are irreversibly lost. It has been reported that about 5% of produced bitcoins are currently out of circulation and are assumed to be lost.

This problem can be solved by adequately archiving and recovering bitcoins, but most current suggestions (e.g., offline "cold storage") are often inconvenient for normal use and updating of such archives.

Problem C-8: Illegal Transactions – Bitcoins can be used for any type of transaction, even those that are illegal, such as money laundering or payment of ransoms. Bitcoin transactions cannot be controlled because the system is not regulated. There is no simple solution for this problem with the standard Bitcoin system. An innovative solution is needed in order to guarantee that Bitcoin supports only legal transactions.

Problem C-9: Packaging of Transactions into Blocks – In principle, packaging transactions into blocks is convenient if the transactions are uniform (i.e., of the same type and belong to the same application). This is the case for Bitcoin, as all transactions are payments, but not for other applications and transactions. For example, in medical applications, transactions may include personal, medical, pharmaceutical, or financial data and thus a uniform approach cannot be used for their protection and validation.

Potential solutions to this problem are to process transactions individually or to package similar transactions in separate blocks. However, neither of these solutions is feasible without substantial reconstruction of the current Bitcoin system.

Problem C-10: Limited Amount of Bitcoins – It is well known that Bitcoin system generates a limited amount of Bitcoins (in total, 21,000,000 bitcoins). This approach is inconvenient for the large "Bitcoin economy."

This problem cannot be solved with the current Bitcoin system; additional bitcoins cannot be generated outside of the current fixed schedule, and existing bitcoins cannot be "split" in order to increase the total number.

2.3. Operational Problems of the Bitcoin System

The operational problems associated with the Bitcoin system are not crucial for its operation, but they are inconvenient and present obstacles for normal operation and use of bitcoins. Therefore, correcting or eliminating those problems is not crucial but is desirable.

Problem O-1: Bootstrapping New Wallets – Due to the very large and continuously increasing size of the blockchain, bootstrapping Bitcoin wallets takes quite a long time. Some vendors apply optimizations or partial downloads, but bootstrapping (activating) a new personal wallet may still take several days. This problem is significant since most of the transactions contained in the blockchain are redundant and will never be used to validate any transaction.

This problem might be solved by limiting the size of the downloaded Bitcoin blockchain. However, such an intervention would require modification of not only the bootstrapping procedure but also the transaction validation protocol. Thus, there is no straightforward solution for this inconvenience.

Problem O-2: Control of the System by Bitcoin Network Nodes – Users must completely trust that the Bitcoin network nodes will operate in a manner correct and compliant with protocol specifications. This assumption is reasonable since the network nodes are using publicly available software. However, only developers have the ability to modify that functionality and users do not have much of an influence on their decisions. One such change in operational policy was the introduction of a 0.0001 bitcoin "network fee." This modification, although not financially significant at present, is problematic as (a) network nodes are operated by members of the community, who thus bear the costs of node operations and (b) it is not clear who collects the network fee since no operational authority is responsible for running the Bitcoin network.

Problem O-3: Selfish Mining – Selfish mining is a phenomenon in which miners mutually collaborate to their benefit. Since miners are necessary in the current Bitcoin system, there is no simple solution to this problem.

Problem O-4: Vulnerable Short Chains ("51% Attack") – It is well known that if a group of miners has 51% of the mining computing power, they could "overrun" the other miners and illegally modify the blockchain. Since miners are necessary in the current Bitcoin system, there is no direct solution to this problem.

2.4. Problems Regarding the Security of Bitcoin System Components

In principle, all the components of the current Bitcoin system, including wallets and exchanges, are vulnerable to hacking. During the last several years it has been shown that these threats are real and very probable. Hacking is most often performed by breaking protections and stealing users' or exchanges' private keys. There are several ways to protect private keys, the most popular of which is to keep them offline in secure storage. However, this solution is not convenient as private keys are used for outgoing payment transactions, and without these keys the parties that own them cannot perform outgoing transactions.

All potential methods of protecting private keys are outside of scope of the current Bitcoin protocol and therefore must be introduced as extensions. With the proposed system, Bitcoin transactions are performed with special, virtual accounts, and not with their standard accounts. This approach means that the private keys of users' wallets and exchanges are not needed and can be stored safely in offline storage.

2.5. Current (Potential) Solutions

Solutions to most of the current problems are mainly evolving in two directions. One involves splitting the bitcoin currency and its blockchain into two separate autonomous systems. One system is the existing Bitcoin system, while the other, called *Bitcoin cash*, would operate with new principles and solutions that would solve some of the current problems associated with bitcoins. The new system is called *SegWit2x*, and it could eliminate problems regarding block size and delays in transaction validation.

SegWit2X is hard fork of the Bitcoin system blockchain with the purpose to double Bitcoin's block size, allowing for up to 8 megabytes of block space. However, this solution has many new problems and does not represent an ideal solution for all the problems associated with the current Bitcoin system, which are described above. The other approach that addresses the problems associated with centralized exchanges, suggests using a distributed structure for exchange servers in order to eliminate the vulnerabilities of single servers, which are often targets of successful attacks.

Current *centralized Bitcoin* exchanges are operated and administered by single servers, which are a single point of failure. Users deposit Bitcoins directly with the exchange, which is responsible for matching purchasing and selling transactions, usually in real time. The disadvantage of centralized exchanges is that they *require users to trust the exchange with their money*. A fraudulent or compromised exchange can result in theft of users' bitcoins. There are also other drawbacks to centralized exchanges, such as users' vulnerability to fraud by the exchange administrators.

Decentralized exchanges were created specifically to address the vulnerabilities of centralized exchanges. In a decentralized exchange users retain a degree of control over their own funds. They do not send money directly to an exchange controlled by a single entity; instead, trading orders, and thus release of user funds, are authorized directly by users via digital signatures. Therefore, in principle, bitcoins cannot be stolen.

"In principle" is the tricky phrase here. It is well known that the ability to authorize transactions does not equate to real control. Enabling users to control their own bitcoins with some additional interventions seems like a good thing, but it also replaces the real-time transactions performed by centralized exchanges with slow, on-chain trading, which exposes users to new monetary risks. This community empowerment-based design approach also permits token holders to modify their purchase/sale contracts. Unfortunately, this creates the systemic risk that users' bitcoins could be exposed to theft.

New concept of decentralized exchanges does not solve previously stated Bitcoin system problems as they still have some design flaws. In order to support real-time trades, decentralized exchanges adopt essentially the same approach as public ("broadcast") announcements of purchase requests or sale offers. In the current system based on centralized exchanges users who want to buy bitcoins send offers or requests to off-chain matching services, which post them in off-chain order books. This posting takes place in real time and thus are much faster than if purchase request and sale offers were posted on a decentralized blockchain. Any user can publish any buy request or sell offer on the order book. In order to validate their authenticity, requests and offers are digitally signed by their creators. Current decentralized solutions try to minimize the amount of trust that users must place in the off-chain matching service by not giving it the power to automatically match buy requests and sell offers. Instead, any other user can trade against a posted buy request or sell offer by adding a counter-request/offer and digitally signing and sending the complete transaction (i.e. pair of requests/offers) directly to the Bitcoin blockchain. If such distributed exchanges use smart contracts, the contracts are used to execute the transaction and transfer assets between the buyer and seller.

The general design described above has several important vulnerabilities:

Vulnerability against man-in-the-middle adversaries: The lack of automatic matching of buy requests and sell offers enables illegal manipulation by an adversary acting as a man-in-the-middle between two parties. In such a fraudulent scheme, stale orders are filled, preventing users from quickly cancelling their bitcoin purchase orders in response to market fluctuations. For example, the adversary selling bitcoins can execute a standing pair of orders (sell 1 token at 1 bitcoin and buy 1 token at 2 bitcoins) to make an immediate profit of 1 bitcoin. Since the only way for users to invalidate their signed orders (which they published on an off-chain service) is by sending an on-chain cancellation transaction that is explicitly processed by the exchange contract, the adversary may pay miners a high processing fee and win the race against the cancellation transaction. Therefore, users who wish to increase the probability of a successful cancellation may need to attach an excessively high fee depending on the value of the trade, which makes the exchange platform unattractive to honest users. In addition, users must react to cancellations in real time, but it is very difficult for ordinary users to recognize ongoing fraudulent transactions.

Vulnerability to fraud by miners: Order cancellations are a common feature of decentralized exchanges (after all, an exchange without the possibility of cancellation may not be useful in a volatile market) and their on-chain nature renders these cancellations particularly vulnerable to the threat of so-called miner front-running, in which the miner of the next block will always have the option to execute cancelled orders with themselves as the counterparty, potentially profiting from such an order. To add injury to insult, the miner collects the transaction fee costs from failed cancellations. This issue is recognized as a limitation of on-chain cancellations in the community.

Exposure to exchange abuses: Since the off-chain matching service doesn't perform automatic matching of requests and orders, it is supposed to publish all users' orders as quickly as possible resulting, in principle, in a fully transparent exchange. However, in cases of abuse, the exchange can *suppress* orders by mounting a denial-of-service attack against users in order to corner a market or censoring particular users' transactions. Worse yet, it can *front-run* orders and engage in the same kind of in-market "sandwich" arbitrage described above for miners, especially when high-value trades are requested. The problem is that signed orders first flow to the off-chain server, which can match the trade data with the pseudonymous users that it controls. Thus, both suppression and front-running by an exchange are extremely hard to detect.

In conclusion, this analysis of decentralized exchanges has shown that they are much more complex than standard single-server exchanges and require additional trust in multiple third parties. Careful analysis of the current solutions has shown that they have solved the problem of a single point of attack but introduced many principles, rules, and additional operations that are contrary to the nature and spirit of the current Bitcoin system, which is supposed to be a fully distributed, community-based, and peer-to-peer transaction system.

3. SUMMARY OF THE INNOVATIVE APPROACH AND SOLUTIONS

3.1. Innovative Ideas and Solutions

The solution to all the problems associated with the Bitcoin system described in previous sections is based on four innovative ideas:

(1) Use of virtual Bitcoin accounts instead of standard Bitcoin accounts;
(2) Use of multi-party signatures to certify and validate individual transactions;
(3) Use of community auctions to buy and sell bitcoins; and
(4) Sponsored encapsulation of native and virtual Bitcoin accounts, users' identities, and financial profiles.

Virtual Accounts: The new *virtual Bitcoin account* system functions in parallel to and it is autonomous from the current standard Bitcoin system and Bitcoin accounts. In the current standard Bitcoin system every user has his/her own Bitcoin address, which contains a certain number of bitcoins that represent the balance of the Bitcoin account. In this paper, these accounts are called *native Bitcoin addresses* and denoted as *nBA*. Therefore, in the current standard Bitcoin system payment transactions are performed as transfers of a certain amount of Bitcoins from the paying *nBA* to the receiving *nBA*. Users initially load these *nBAs* either by mining or by purchasing bitcoins on third-party exchanges. This situation and transaction in the native Bitcoin system is shown in Figure 1.

In the new system, described in this paper, each user is assigned an additional so-called *virtual Bitcoin account*, denoted as *vBA*. These accounts are just random numbers without any cryptographic interpretation. In the original Bitcoin system account numbers are also used as cryptographic keys for encryption of transactions. In the new system transactions are encrypted by cryptographic keys that are independent of account addresses. For that reason, virtual account numbers to not need any special form or interpretation – they can be standard random numbers. In addition to creating a *vBA* for each member of the Bitcoin system, the business entity that runs the new system creates its own native Bitcoin account, called an *escrow Bitcoin account* and denoted as *escBA*. The situation after initial setup of the system is shown in Figure 2. Each user has his/her virtual Bitcoin account, the balance of these accounts after they are created is *zero* and the balance of the escrow Bitcoin account, after its creation, is also *zero*.

In order to use his/her *vBA*, each user initially transfers all or certain number of bitcoins from his/her *nBA* to the *escBA.* In return, the system credits the user's *vBA* with the same number of virtual bitcoins as the amount transferred to the *escBA*. In essence, users "deposit" their bitcoins into the *escBA* and receive the same number of virtual Bitcoins in their *vBAs*. The situation after User 1 transferred 10 Bitcoins from his real to his virtual bitcoin account, is shown in Figure 3. User 2 transferred 5 Bitcoins. Both transfers are performed in real Bitcoin system, from Bitcoin accounts of users to the escBA. As the consequence of these transfers, the system credits users' vBAs with the equivalent number of virtual bitcoins.

Once bitcoins are deposited in the *escBA*, all payment transactions between users are performed as transfers between virtual Bitcoin accounts. However, these transactions are simply bookkeeping actions using the *vBAs* of users involved in the transaction; real bitcoins are not moved from the *escBA* and therefore no transaction is performed in the Bitcoin system. The situation when User 1 pays 3 bitcoins to User 2 is shown in Figure 4. *vBA* of User 1 is debited and *vBA* of User 2 is credited with 3 bitcoins. Effectively, Bitcoins are not moved at all.

If users want to "cash out" their bitcoins from their *vBAs*, a native Bitcoin transaction is triggered to transfer the cashed-out bitcoins from the *escBA* to the user's *nBA*. However, in practice, there is no reason for such an action as users may use their virtual bitcoins for payments and if they want to cash out their bitcoins into real currency, they can do so directly using the bitcoins that are deposited in the *escBA*. These two options are shown in Figure 5 and in Figure 6. When User 1 wants to pay, example, 2 bitcoins to User 3, who is not in the new Bitcoin system, he/she can do that in two ways. He/she can first transfer 2 bitcoins from the *escBA* back to his/her *nBA* and then perform bitcoins transaction in the standard system to transfer bitcoins from his/her nBA to the nBA of User 3. This situation is shown in Figure 5. Alternatively, User 1 can transfer 2 bitcoins directly from the *escBA* to the *nBA* of the recipient. This transfer is shown in Figure 6. The advantage of the second option is that the transfer is performed as only one transaction in the native Bitcoin system, compared to the two transactions with the first options.

Multi-Party Signatures: The standard Bitcoin system, like any other system using a blockchain, must guarantee that transactions cannot be later modified and/or that transactions cannot be inserted into the blockchain to ensure the data integrity of transactions and their time sequence. In the current standard Bitcoin system this is achieved with the hashing mechanism and with cryptographic chaining of blocks performed by miners. This specific solution introduces many problems regarding block size, time delays, selfish miners, and use of trusted third parties, as described above.

However, the integrity of individual transactions and immutability of the blockchain can be guaranteed by other protocols that do not require blocks, do not introduce time delays, and do not need or involve third parties. The innovative solution introduced in this paper is based on (a) a multi-party signature protocol and (b) a reliable time-stamping protocol.

The purpose of hashing blocks in the current standard Bitcoin system is to prevent their post-factum (accidental or intentional) modification and in that way guarantee the original content of blocks. Hashing cannot be performed by the originators (senders) of transactions; if it could, hashes could be modified later by the person who initially created them. At first, this seems to call for a third party to create the hashes. The Bitcoin system uses miners—people who perform hashing computations with blocks—for this purpose. However, this solution is not optimal as it makes the system dependent on third parties.

A much better solution is to use blockchain nodes to create hashes. These nodes receive transactions, so they can ensure their content by hashing them and then digitally signing these hashes. In the system described in this paper, the originators (senders) also create hashes of each transaction and digitally sign these hashes before submitting them to the blockchain network.

This function—digital signing of individual transactions—is not present in the processing logic (scripts) of the current standard Bitcoin network nodes, which only validate the balance of the sending account. In this paper the functionality and capabilities of ledger network nodes are extended to include hashing and creation of digital signatures. With this approach transactions are signed by two parties (their sender and the ledger network node), so their correctness can be validated by all other users in the system and transactions cannot be illegally modified by their originators after their creation.

The nodes of the current Bitcoin network cannot perform these cryptographic operations with individual transactions. Therefore, in order to introduce these new operations, the architecture of the current standard Bitcoin system must be modified to include additional functionality just described. But, such approach is not feasible, as it would include re-engineering of the entire Bitcoin network and it would not be backward compatible with the current Bitcoin system. Therefore, the new system described in this paper uses its own secure blockchain ledger, the nodes of which (a) manage and maintain various their own cryptographic credentials and (b) perform various cryptographic operations, such as hashing and digital signing of transactions.

In addition to ensuring the data integrity of individual transactions, a correct blockchain system must also prevent the possibility of inserting transactions into the middle of the transaction sequence (i.e., chains). To do so, the current standard Bitcoin system uses a chaining technique where the hash of the previous block is included in the current block before hashing it. However, correct transaction sequence in a ledger can be guaranteed if transactions are entered into the blockchain with a *guaranteed* and *reliable* record of the *time of their creation*. This service (reliable Internet time) is available in the Internet network, so it can be used instead of cryptographic chaining.

Since transactions with virtual Bitcoins and *vBAs* are not performed in the current Bitcoin network, the new secure ledger must be designed with security functions as described in this paper. Since transactions are inserted in the secure ledger at one point of the new secure ledger (and not by multiple miners, as in the Bitcoin system), the new secure ledger does not need synchronization and consensus protocol. Thus, the nodes in the secure ledger add new transactions to the transaction sequence by first inserting into transaction objects the correct and reliable time and then hashing and digitally signing these transactions.

Use of Community Auctions for Buying and Selling Bitcoins: The new system solves the problem of third-party exchanges as vulnerable points in the current Bitcoin system. Some alternative solutions described above still use exchanges, but they are distributed and therefore do not represent a single point of failure. However, they are still third parties and have their own serious weaknesses and problems.

In this paper a new solution is introduced that completely eliminates exchanges (centralized or distributed) and, in doing so, not only eliminates all problems associated with exchanges, but also aligns with the spirit of the Bitcoin system as a peer-to-peer transaction system.

The innovative idea is very simple: the buying and selling of bitcoins is organized as a global Bitcoin *community auction*. Instead of transferring bitcoins to (centralized) exchanges or placing orders to off-site nodes, those who want to buy or sell bitcoins simply announce that on the standard Bitcoin network. These announcements are "piggybacked" to other bitcoin transactions and therefore inserted into the Bitcoin blocks, reaching all members of the Bitcoin community.

The procedure for running auctions is very simple, with four possible scenarios:

Selling Bitcoins:

1. When a user wants to sell bitcoins, he/she first checks for any requests to buy bitcoins already posted on the Bitcoin blockchain. If there are no pending requests, the user posts his/her offer to sell bitcoins. These sale offers will then be listed to users requesting to buy bitcoins.
2. If there are requests to buy, the user selects one request and creates an offer to sell bitcoins. When the buyer selects the best offer, bitcoins are transferred from the seller and payment is transferred from the buyer as direct, peer-to-peer transactions.

Buying Bitcoins:

3. When a user wants to buy bitcoins, he/she first checks if there are any offers to sell bitcoins already posted on the Bitcoin blockchain. If there are no posted offers, the user posts his/her request to buy bitcoins. These requests will then be listed and users who want to sell bitcoins can see them.
4. If there are offers to sell bitcoins, the user selects one offer and creates his/her offer to buy bitcoins. When the best offer is selected by the seller, bitcoins are transferred from the seller and payment is transferred from the buyer as direct, peer-to-peer transactions.

If two users involved in the transaction have already transferred their bitcoins to their *vBAs*, the transaction is performed as simple book-keeping transaction in the new system, without even moving bitcoins from the *escBA*. procedure for running auctions is very simple, with four possible scenarios:

Sponsored Encapsulation of Native and Virtual Bitcoin Accounts, Users' Identities, and Financial Profiles: Problem C-5 described the issue that may occur when passing Bitcoin addresses between users. In the system described in this paper, standard Bitcoin addresses are used to exchange bitcoins between users' *nBAs* and the *escBA*. Therefore, the problem of incorrect Bitcoin addresses can be manifested as incorrect transfer of users' *nBAs* to the Escrow Agency.

A way to detect incorrect transfers is to use a data integrity mechanism for *nBA*s. The most convenient is based on a hash of the *nBA* protected by the digital signature of the sender. In this way, the addresses are self-signed objects and can be validated using the value (public key) contained in the cryptographically protected *nBA* object.

This approach can also be used with *vBAs* when exchanged between users. However, digitally signed *nBAs* are self-validating, while *vBAs* are not. This means that cryptographically encapsulated *vBA*s must also include the certificate of the *vBA's* owner. To ensure the uniformity of the system, the same procedure may also be used for validation of *nBAs* too.

Managing, distributing, and validating users' certificates is another function of the secure ledger used by the system described in this paper. As is well known, an integral component of each certificate is the identity of the certificate's owner, so the secure ledger manages also users' identities.

In order to prevent illegal transactions with bitcoins, the user's identity must be included in the cryptographically signed *nBA* object so users trying to perform illegal transactions can be identified. However, this would eliminate the transaction's anonymity against other users.

In order to prevent illegal transactions but still ensure the privacy and anonymity of all users, users' identities included in the self-signed *nBA* objects should be cryptographically encapsulated for the Escrow Agency. This is achieved by cryptographically enveloping the user's identity with the public key of the Escrow Agency. Since the public key is already available to the user as the receiving *nBA* address when transferring bitcoins to the *escBA* or within the publicly available certificate of the Escrow Agency, it can be used for cryptographic enveloping of users' identities. This cryptographic protocol enables Escrow Agency to control the validity of transactions by recovering the clear form of the user's identity, if needed.

3.2. Analysis of Problems and Proposed Solutions

In this section, the problems listed in section 2.2 are reviewed and the ways in which the proposed system eliminates all these problems are presented.

Problem C-1: Block Size – The proposed system does not use blocks, so block size is irrelevant.

Problem C-2: Transaction Validation Time – In the proposed system, transactions are validated individually and instantaneously, so transaction validation time (i.e., delay) has been reduced to a minimum.

Problem C-3: Potential Hashing Problem – Hashing of transactions has no target value, so any hash is acceptable and there is no hashing problem.

Problem C-4: Dependency on Trusted Third Parties – The proposed system does not involve third parties.

Problem C-5: Distribution of Bitcoin Addresses – Bitcoin addresses are not used, so problems regarding their distribution are irrelevant.

Problem C-6: Anonymity of Users – In the proposed system, users and their transactions are completely anonymous; their *vBAs* are purely random numbers and therefore cannot be traced to their real identities.

Problem C-7: Loss of Bitcoins – In the proposed system, bitcoins cannot be lost. The number of bitcoins in an account is recorded during the "cash-in" process and remains accurate regardless of what happens with the bitcoins stored in *nBAs.*

Problem C-8: Illegal Transactions – Illegal transactions cannot be performed since use of *vBAs* for illegal transactions can be effectively blocked.

Problem C-9: Packaging of Transactions into Blocks – In the proposed system, blocks are not used and individual transactions are cryptographically confirmed, so this problem is irrelevant.

Problem C-10: Limited Number of Bitcoins – This problem may be solved by splitting virtual bitcoins so that two, four, or more of them correspond to one real bitcoin.

Problem O-1: Bootstrapping New Wallets – The process of bootstrapping new wallet is simple and instantaneous since it is not necessary to download the full Bitcoin chain.

Problem O-2: Control of the System by Bitcoin Network Nodes – In the proposed system the Bitcoin network is not used for payment transactions, so the functions of Bitcoin network nodes are irrelevant.

Problem O-3: Selfish Mining – In the proposed system miners are not used, so problems related to miners are irrelevant.

Problem O-4: Vulnerable Short Chains (“51% Attack”) – In the proposed system individual transactions are confirmed by multi–party signatures, so it is not possible to illegally modify them.

3.3. Trust in the Escrow Agency

The described protocols and procedures for managing and using *vBAs* in the new system seems to indicate that the Escrow Agency is acting as a trusted third party. If true, that would be contrary to the claim that the new system does not use and does not depend on any third party. It is important to note that virtual bitcoins are transferred to the user’s *vBA* after the *escBA* receives real bitcoins from the user’s *nBA*. It is well-known that such a transfer is irreversible, so the Escrow Agency has the ability to cheat users by not assigning an equivalent number of virtual bitcoins to the user’s *vBA* after receiving bitcoins transferred from user’s *nBA*.

This potential problem is classical example of collaboration of mutually suspicious parties. The user is willing to transfer real bitcoins from his/her *nBA* to the *escBA* only after an equivalent number of virtual bitcoins has already been assigned to his/her *vBA*, and the Escrow Agency is willing to assign these virtual bitcoins only after the real bitcoins have been transferred to the *escBA*. The “deadlock” can be resolved by introducing a special form of smart contract managed by the secure ledger. A smart contract is a simple document, in this case featuring just two indicators, each of which indicates one of the transfers described above. When the Escrow Agency assigns *vBTC* to user’s *vBA*, this action will turn the “*credit to user’s vBA*” indicator *on.* However, but the user’s *vBA* will not be updated until the user transfers real bitcoins from his/her *nBA* to the *escBA* to the Bitcoin network. This operation will trigger effective transfer to the user’s *vBA,* since “*credit to user’s vBA*” indicator is *on.*

5. DETAILED DESCRIPTION OF THE PROPOSED SOLUTIONS

The prerequisite for the new system is availability of the secure ledger with security features and functions described above. This aspect is outside of the scope of this paper, so availability of such secure ledger is assumed. Operations of the virtual Bitcoin system involves five steps:

5.1. Establishment of an Instance of the Virtual Bitcoin System

A business entity that wants to act as an Escrow Agency of an instance of the virtual Bitcoin system installs all the appropriate software and generates its own standard Bitcoin address (i.e., an *escBA*). After these two actions have been performed, an instance of the system is ready to begin its operation.

5.2. Registration of Users

Users access the instance of the system by first creating their identities and certificates, using secure ledger, and then registering their *vBAs*, which are just random numbers. In order to use the system, users must already have *nBAs*, so during the registration procedure, users “link” their *nBAs* and *vBAs*.

5.3. Loading Virtual Bitcoin Accounts (“Cash-In”)

In this procedure users convert the real Bitcoins stored in their *nBAs* to an equivalent amount of *vBTCs*. The procedure involves two steps: (1) the user’s real Bitcoins are transferred from his/her *nBA* to the *escBA* using the standard transaction performed by the Bitcoin system, and (2) the user’s *vBA* is credited with the same amount of *vBTCs*.

5.4. Payments Using Virtual Bitcoins

This procedure is simple update of the two *vBAs*; the payment is debited from the sender’s *vBA* and the same amount is credited to the receiver’s *vBA*. No Bitcoin system transaction is performed.

5.5. Unloading Virtual Bitcoin Accounts (“Cash-Out”)

In this procedure users convert the virtual bitcoins stored in their *vBAs* to an equivalent number of real bitcoins. The procedure is the reverse of the cash-in procedure and also involves two steps: (1) real bitcoins are transferred from the *escBA* to the user's *nBA* and (2) the number of virtual bitcoins transferred to the *nBA* is debited from the user's *vBA*.

6. CONCLUSIONS AND CONTRIBUTIONS

The contributions of this paper are:

1. A system using *virtual accounts* for Bitcoins and for any other crypto currency and using *virtual currencies*, which represent equivalents of their real crypto currencies, is described.

    1.1 An instance of the system is established by creating an address (account) for real Bitcoins or for any other crypto currency owned by the Escrow Agency which is managing other accounts and handling transactions in the system.

    1.2 Users are registered in the system by creating their identities and certificates and then by creating their virtual addresses (accounts) for Bitcoins or for any other crypto currency and linking these addresses (accounts) to their real addresses for Bitcoin or for any other crypto currency.

    1.3 Virtual Bitcoin addresses (accounts) are credited by transferring real Bitcoins from users' real Bitcoin addresses (accounts) to the real Bitcoin address (account) of the Escrow Agency and by increasing the balance of the user's virtual Bitcoin address (account) by an equivalent number of virtual Bitcoins ("cash-in").

    1.4 Payment transactions between virtual Bitcoin addresses (accounts) are performed as simple bookkeeping operations using virtual Bitcoin addresses (accounts); the virtual Bitcoin account of the sender is debited, and virtual Bitcoin account of the receiver is credited by the payment amount.

    1.5 Virtual Bitcoin addresses (accounts) are debited by transferring real Bitcoins from the real Bitcoin address (account) owned by the Escrow Agency to the users' real Bitcoin addresses (account) and by decreasing the balance of the user's virtual Bitcoin address (account) by the equivalent number of virtual Bitcoins ("cash-out").

2. A method for ensuring the correctness of the original content of individual transactions and their correct time sequence based on *multi-party digital signatures* and *reliable Internet time* is described.

    2.1 The originator of the transaction creates the hash of the transaction and its digital signature.

    2.2 The server of the secure ledger with which the originator of the transaction is associated adds its digital signature to the transaction.

    2.3 The server of the secure ledger with which the recipient of the transaction is associated adds its digital signature to the transaction.

    2.4 The server of the secure ledger with which the originator of the transaction is associated creates the time at which the transaction was created based on reliable Internet time.

3. A method of selling and buying real and virtual bitcoins and other crypto currencies based on *community auction protocol* is described.

    3.1 If there are no offers to sell on the global Bitcoin blockchain, the buyer posts a request to buy bitcoins. If offers are posted, the buyer selects an offer and posts an offer to buy.

3.2 If there are no requests to buy on the global Bitcoin blockchain, the seller posts an offer to sell bitcoins. If requests are posted, the seller selects a request and posts an offer to sell.

4. A method of preventing incorrect and illegal transactions with virtual bitcoins and other crypto currencies based on *sponsored* handling of virtual and native Bitcoin addresses, user identities, and user certificates is described.

4.1 The virtual Bitcoin account of the sender, the virtual Bitcoin account of the receiver, and the amount to pay are cryptographically enveloped for the Escrow Agency.

4.2 The identities of the sending and receiving users are included in the payment transaction, cryptographically enveloped for the Escrow Agency.

4.3 The certificates of all signing parties are also included in the payment transaction.