PENCE COIN

Secure and Convenient Solution for Contract and Remittance

PenceCoin Team

PenceCoin: Secure and Convenient Solution for Contract and Remittance

PenceCoin Team

Abstract

The conventional money transaction system has many problems such as a long delay in confirmation, a high transaction fee, frustration of contract. While many cryptocurrencies are suggested as solutions for these problems, it is failing to achieve mass adoption because of the high high entry barriers for non-tech people. PenceCoin is the solution for those problems. Achieving security and stability with the blockchain technology, PenceCoin alleviates the counter party risk of financial contract by implementing smart contract. Furthermore, PenceCoin has two- layer privacy protection feature which secures financial safety. The first target market for PenceCoin is a payment system for the crossborder trading and it will be expanded to the daily life.

1 Introduction

1.1 Cryptocurrency for Financial Sovereignty

Money has been employed as the medium of exchange which enables people to trade with the unified measure of value. A transaction between different currencies is commonly implemented in recent days due to the noticeable increase of overseas trade market. Numerous kinds of financial systems are used for the transaction process.

However, conventional money transaction systems suffer from several limitations. When we send money to a contractor in different country, a typical choice limitations. When we send money to a contractor in different country, a typical choice the contractor receives the money. Moreover, we need to pay a high remittance fee to the bank while being exposed to the volatility of the exchange rate between different currencies as it takes time until the transaction is finished.

currencies as it takes time until the transaction is finished. where the financial infrastructure is insufficient. They have to pay a tremendous amount of the remittance fee comparing to their average income even if they also spend much money and time to go to the bank. Furthermore, it is hard to assure the reliability of the financial contract. Actually, we meet many untrustworthy people while making contract for doing works on behalf of us. While there have been various suggestions to solve these problems with cryptocurrency, it has a long way to go.

1.2 Bitcoin: A Peer-To-Peer Electronic Cash System

Satoshi Nakamoto suggested Bitcoin [1] as a peer-to-peer electronic cash system in pursuit of financial sovereignty, breaking away from traditional financial systems with cypherpunk movement. However, Bitcoin is failing to achieve the mass adoption in terms of real-world usages for several reasons.

In conventional systems, financial records have been kept confidentially by trusted third parties such as bank. Bitcoin was a try to break this societal chain by publicly open the ledger instead of by keeping the record personally. This enables to alleviate the counterparty risk in the currency transaction, and the privacy was to be achieved by keeping the key of the wallet secret.

However, it is known that the achievement of privacy in Bitcoin is failed in various aspects as mentioned by Open Bitcoin Privacy Project [2]. For example, Bitcoin.org [3] suggests people to use a new Bitcoin address when they receive a new payment because the transaction history of wallet is easily traceable. Although Bitcoin succeeded to alleviate the counterparty risk in the transaction with blockchain system, this non-privateness became an obstacle of the mass adoption along with the technological entry barrier.

Furthermore, a high transaction fee and slow block confirmation time are pointed out as main limitations of Bitcoin in particular for the acceptance of Bitcoin in the situation such as in front of the counter in a retail store. The retail transactions typically handle a small amount of money, therefore, the high transaction fee can be an excessive burden on the users. The delay of the transaction confirmation also inconveniences the users who are familiar to the instant transactions of conventional payment systems such as a credit card.

These problems should be appropriately handled in some way to bring out the mass adoption of the cryptocurrency-based transaction. There have been several approaches to tackle the problems. However, none of them succeed sufficiently, and the cryptocurrency-based transaction is still disregarded by the users.

1.3 Smart Contract

The concept of smart contract is developed by Nick Szabo in his first publication "Smart Contracts: Building Blocks for Digital Free Markets" [4] in 1996. He described smart contract as follows: “New institutions, and new ways to formalize the relationships that make up these institutions, are now made possible by the digital revolution. I call these new contracts "smart", because they are far more functional than their inanimate paper-based ancestors. No use of artificial intelligence is implied. A smart contract is a set of promises, specified in digital form, including protocols within which the parties perform on these promises.”
Although smart contract is suggested in 1996, it is implemented in earnest and publicly employed in 2015 with Ethereum [5], which introduced the concept of “programmable money” to the world and became one of the most successful and active public blockchain projects. While the counterparty risk in the network side is alleviated with the system suggested with Bitcoin, Ethereum suggested a system that can relieve the risk in the financial side with smart contract.

However, smart contract is an innovative solution though, we are witnessing another barrier for the mass adoption. Smart contract can be implemented by programming with Solidity, a programming language developed for the purpose for Ethereum. It means, making a smart contract is a kind of programming. Therefore users without any technological knowledge about programming cannot make smart contract on their own. Moreover, the programming languages developed for smart contract implementation have technical flaws. A programming language called Serpent was developed in the early period before Solidity became popular, but Serpent was discarded as its critical vulnerability was disclosed. After Serpent was retired, Solidity became lingua franca for the smart contract development in Ethereum platform. However, Solidity is also getting criticized for its degraded usability these days.

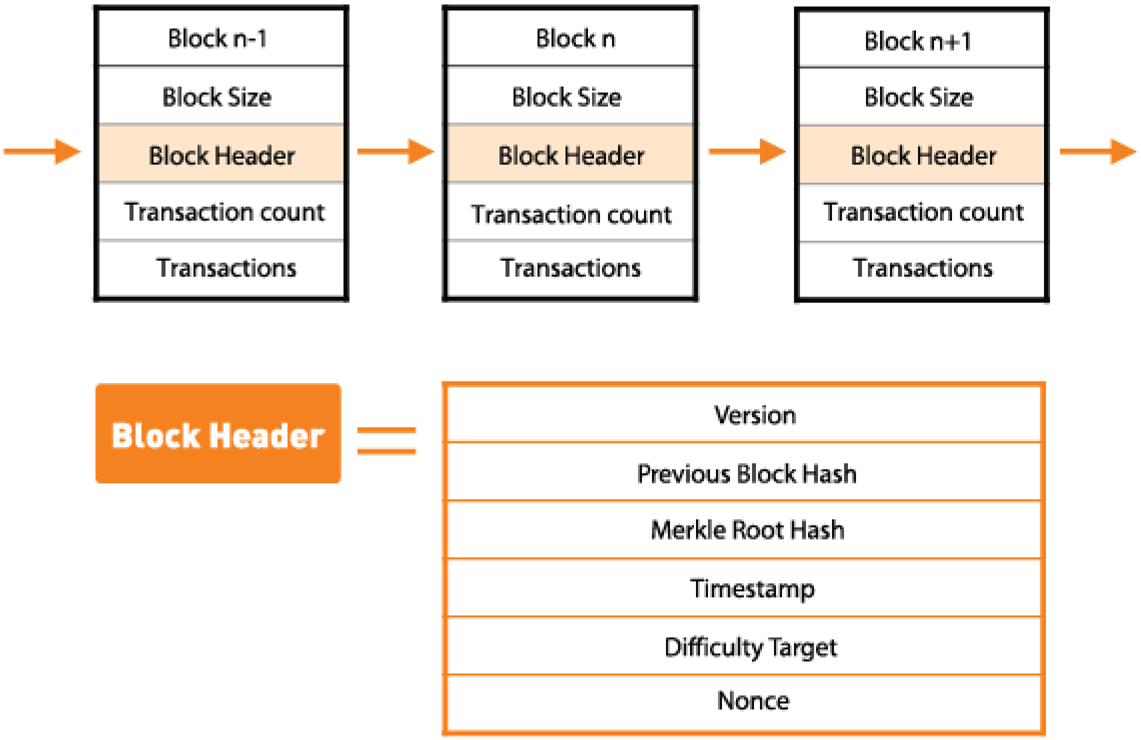
Leaving the technical issues of programming languages aside, an easy–to–use software platform to make smart contract and interact with the smart contract even the user does not have any technological background lacks.

1.4 PenceCoin

PenceCoin is a cryptocurrency for the contract and remittance. PenceCoin is optimized for financial transactions, from peer–to–peer money transfers to overseas remittances and trade settlements between companies. PenceCoin implements smart financial transaction. For the better usability and accessibility of the smart contract, a mobile wallet will be provided that simplifies the processes of making and transacting with smart contract conveniently. Furthermore, PenceCoin provides secure transactions based on the improved privacy feature.

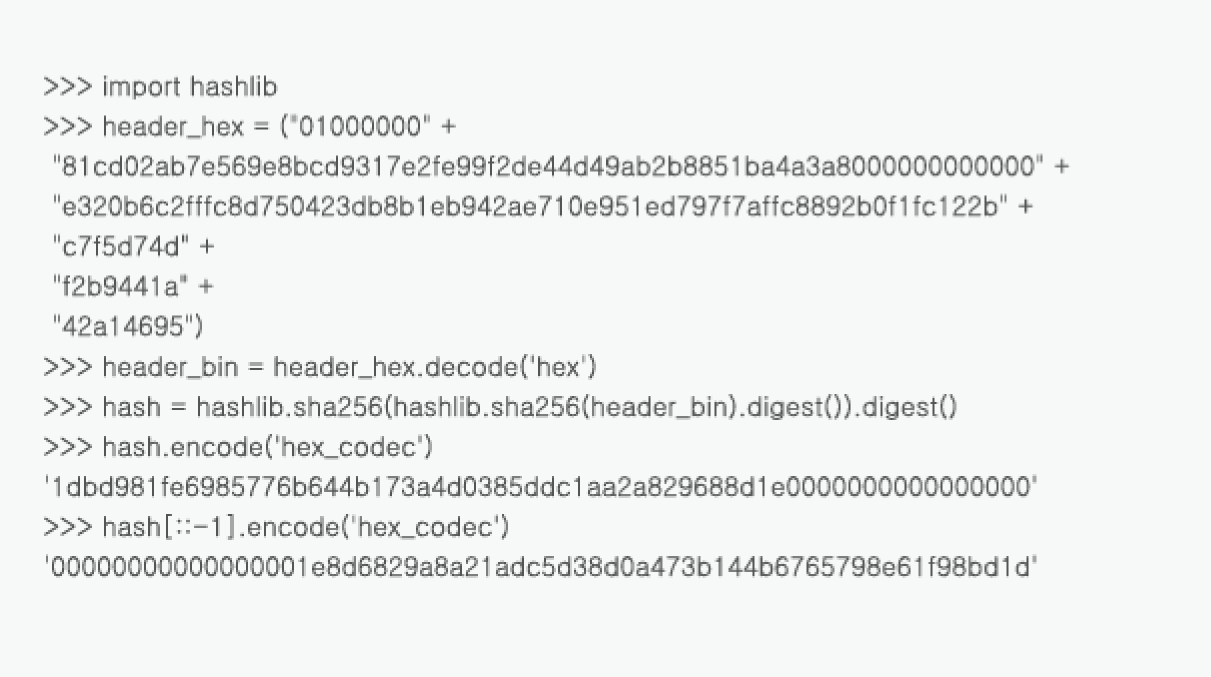
2 Technology

2.1 Proof of Work



Every transaction has a hash associated with it. In a block, all of the transaction hashes in the block are themselves hashed, and the result is the Merkle root. In other words, the Merkle root is the hash of all the hashes of all the transactions in the block. The Merkle root is included in the block header. With this scheme, it is possible to securely verify that a transaction has been accepted by the network by downloading just the tiny block headers and Merkle tree= downloading the entire block chain is unnecessary. This has the advantage that only a list of root, log2(n) hash partners and the index of the transaction are sufficient to reconstruct a Merkle branch, allowing Simplified Payment Verification with much less data than the complete block.

Example code below:



```
>>> import hashlib
>>> header_hex = ("01000000" +
 "81cd02ab7e569e8bcd9317e2fe99f2de44d49ab2b8851ba4a3a8000000000000" +
 "e320b6c2fffc8d750423db8b1eb942ae710e951ed797f7affc8892b0f1fc122b" +
 "c7f5d74d" +
 "f2b9441a" +
 "42a14695")
>>> header_bin = header_hex.decode('hex')
>>> hash = hashlib.sha256(hashlib.sha256(header_bin).digest()).digest()
>>> hash.encode('hex_codec')
'1dbd981fe6985776b644b173a4d0385ddc1aa2a829688d1e0000000000000000'
>>> hash[::-1].encode('hex_codec')
'00000000000000001e8d6829a8a21adc5d38d0a473b144b6765798e61f98bd1d'
```

PenceCoin employs proof-of-work system to attain the security of the network, which is suggested by Satoshi Nakamoto for Bitcoin. The proof-of-work includes a search process for a search process for a hashed value which is lower than or same with a target value which is set by a protocol. The difficulty of proof-of-work can be simply represented with the quantity of leading zero bits of the target value. The confirmation of the work, whether the result is proper or not, can be done by executing the hash value again. Network participants do proof-of-work by increasing a nonce, which is a number concatenated to the hash value of the previous block, in the block until the worker finds a value that satisfying the condition with target value when it is hashed.

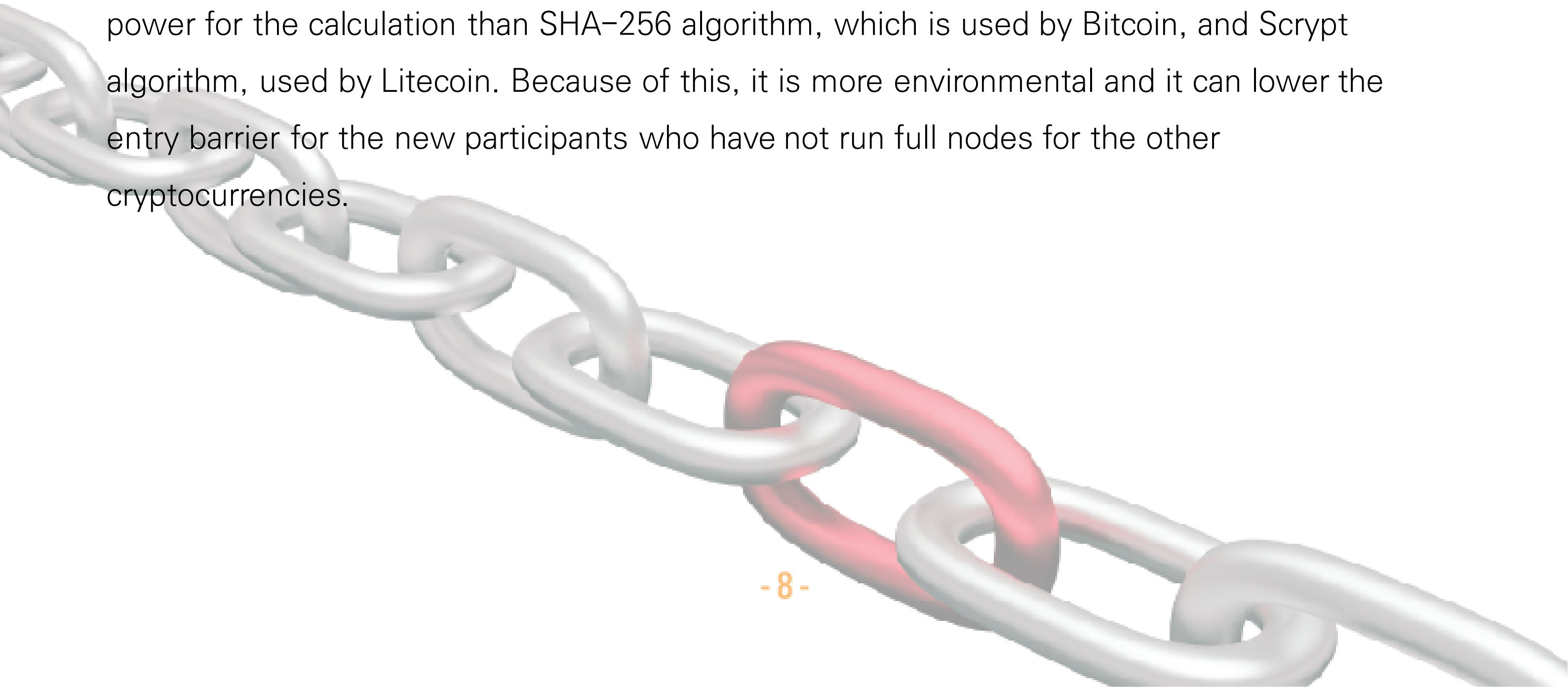
Contents of a block cannot be changed without finding the value again, and it needs a tremendous amount of work of machines. If a malicious actor tries to modify a block, the whole process needed to build the blockchain after the target block must be done again from the block to the present block because a former block is linked with a later block by including the data of the former block, such as the hash value and transactions.

Moreover, the proof-of-work can be used for consensus settlement. Like voting system based on IP address, one vote for one IP address, consensus settlement system can be implemented as one vote for one machine with proof-of-work. If the majority agrees with one opinion, they could vote by doing the proof-of-work for one chain.

Therefore, the opinion of the majority could be captured with longest chain. If the majority of the network participants are honest, the honest chain would be the longest chain as it generates blocks faster so it would outpace the other competing chain. When an attacker attempts to modify the record of blockchain, the chain that the attacker supports should be the longest chain as the network participants believes the longest chain is the honest chain. The attacker needs more than a half of the network computings chain should generate blocks faster than the other chains, and it is hardly achievable as the network grows.

As the network grows and gets more network participants, the block creation time gets shortened as more machines do proof-of-work. In order to keep the value of incentives, the difficulty of the proof-of-work should be adjusted, and it is adjusted by moving average method targeting one block per minute. In other words, the difficulty increases when the block is generated too fast and vice versa.

X11 hashing algorithm, an algorithm chaining which uses 11 rounds of different hash algorithm, is used for PenceCoin for the proof-of-work process. X11 is more energy-efficient for mining with CPU and GPU as proof-of-work process with X11 algorithm requires lower processing power for the calculation than SHA-256 algorithm, which is used by Bitcoin, and Scrypt algorithm, used by Litecoin. Because of this, it is more environmental and it can lower the entry barrier for the new participants who have not run full nodes for the other cryptocurrencies.



2.2 Masternode

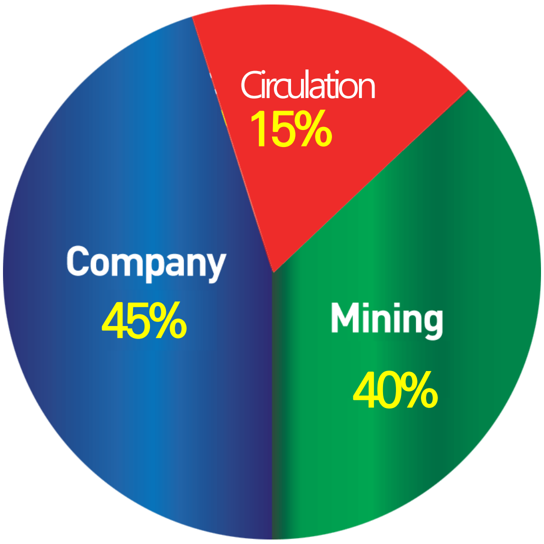
Full nodes are key elements because not only they constitute the network but also they process the whole steps of transactions in blockchain network. They receive interactions of users and propagate it into the network, and they verify and record the transactions. However, relying on the network participants with goodwill is mathematically unstable according to game theory. Network participants who run the full node should be incentivized as each network participant spends their resources for the network.

In Bitcoin, nodes are rewarded in the process called mining, getting reward of finding new block appropriate for the blockchain as the next block in the proof-of-work process. But proof-of-work is not a good solution for incentivizing the participants to join the network for the network which is in its early stage because it costs a lot of electricity and time. Moreover, it is not plausible to expect for users to run their own node to mine the token when the value of token is not feasible.

While PenceCoin uses proof-of-work mechanism for the validation, PenceCoin employs masternode network as a second layer network. Masternode are full nodes, and they should provide reliable network stability and high availability for the services:
smart contract, private transaction, and proprietary credit card transaction. Full nodes are rewarded with seperated reward program. The token could achieve feasible level of value with implementation of masternodes as it can decrease the circulating supply. Because of this structure with the appropriate rewards and the implicit increases of token value, masternode system incentivizes people to run the full node.

Masternodes must provide a specific level of service, and they have to put up a collateral, 100,000 PenceCoin, in order to participate in the network as masternode. The collateral is different with the stake in proof-of-stake system as it would not be slashed while the masternode is running properly. As the masternode should operate stably, it can provide stable service.

Masternodes get a reward as a form of a dividend when the masternodes provide a service to clients who requested. The reward of masternodes is proportional to the block reward, at first about a half of it, and it can be adjusted according to the network status with soft forks. As users have to purchase PenceCoin in order to run the masternode, users can approach this system as an investment as they earn interests of their purchase of PenceCoin. There are limitations for the number of masternode in two kinds of sense. The number of masternode is limited as there is a limitation for the total supply of PenceCoin, 2 billion. Accordingly, only 20,000 masternodes can be running on the network. As the number of the masternodes increase, it becomes hard to run a new masternode because the circulating supply on exchanges of PenceCoin would be lowered. Therefore the implicit limit is created because the cost to acquire the amount of PenceCoin needed to run masternode increases.



This system works as a protector from a malicious actor of the masternode This system works as a protector from a malicious actor of the masternode masternode network in order to control the master node network. However, the cost for acquiring masternodes more than a half of the network will be infeasible when the malicious actor wants to attack the network to get enough reward for the attack as the network become matured.

Furthermore, it is needed to form a quorum in order to serve a service of the masternode network. In the quorum system, each masternode checks the status of the other masternodes to confirm the node is active and working properly. 5 Masternodes are pseudo-randomly chosen in the masternode network, and they check the status of each other. The selected masternodes propagates the status of the nodes through the network. There might be unchecked masternodes for a long time as the choice system is random. unchecked. Therefore, there is one-hour limit for the unchecked nodes to be checked. It means the network keeps the timestamp of the status check of each node, and the network picks nodes to be checked when the nodes are unchecked more than one hour. A node which is failed to be checked its status is excluded from the masternode network for a day to guarantee the stable service availability.

The masternode network propagates announce message and ping signal through the network to announce new masternode when new masternode is connected to the masternode network. After the two messages are received by each node, the new node is recognized as an active node on the masternode network. New masternode can be set up by sending a fixed amount of PenceCoin to an activation address in a wallet which activates the masternode feature and sends the messages into the network. In the process, a new private key is generated for signing the messages for the services running on the masternode network. The wallet storing the collateral is locked with the new key. The client is disconnected.

2.3 Smart contract

By binding script for program in the transaction, it is able to run the script on the network and keep it as a record in the blockchain. Simple scripts can be embedded in each transaction in Bitcoin protocol. For example, multisig, requiring two private keys out of a given three keys to validate, can be implemented with the script within the Bitcoin protocol.

Ethereum expanded the range of functions of the script with built-in Turingcomplete programming language. Versatile use cases are developed on Ethereum network. Not only smart contracts with the built-in programming language, but also decentralized applications which can create its own rules for the ownership and transaction format are being implemented these days.

However, several shortfalls in the system exist as it has high degree of freedom in the development. The major problem is the security of the contract depends on the capability of the contract developer. This gives the responsibility of the contract to a developer who just works for a company, and it is a high risk for the companies making contracts on the smart contract platform. This is one of the reasons the smart contract is failing to achieve mass adoption for the business field.

Furthermore, smart contracts cannot be modified once the contracts are recorded on the blockchain. Therefore, users just should believe the behavior of the contract after it is published. Even if there is a bug in the code of contract, it cannot be patched. Although there are a few ways of workaround, it is a fundamental problem.

Moreover, this system is not appropriate from the environmental perspective because every full node on the network should run the same smart contract codes to verify it. Although this is related to the mining system and retaining security, it is wasteful for every machine on the network to run the same code at the same time. is striving to achieve enough scalability.

As the main goal of PenceCoin is security and convenience, PenceCoin uses Turing-incomplete smart contract language. For the simple and easy-to-use remittance and contract services, PenceCoin provides mobile and desktop wallets with concise UI. The wallets will have the simplified form necessary to transfer money or make contract, and the smart contract code will be implemented based on the input automatically. Users are not needed to worry about the bug or failure of the process as the system implements fully audited code automatically with a few variables which receives input.

Masternode network is in charge of the process of the smart contracts. The most recently checked three masternodes are chosen and the masternodes process the smart contract. The smart contracts can be processed precisely and securely with this structure, as the stability and security of the masternodes are guaranteed with the status checking system.

2.4 Privacy

The privacy feature of Bitcoin is limited as mentioned above. In order to complement this, an anonymization method called CoinJoin [6] is suggested by Gregory Maxwell. CoinJoin is making a joint payment transaction with who agreed to make a payment together. This mixing method increases privacy to a certain level though, it is found out that the mixed payment can be de-anonymized. A common implementation of CoinJoin for Bitcoin transaction is simply merging a number of transactions together.
However, the sender can be identified easily by adding up the output values until the sum is equal to a value of the input. Although the difficulty of de-anonymization grows

exponentially as the number of mixed payment increases, it can be anonymized with a feasible amount of resources with brute-force calculation. Another strategy for CoinJoin is using an entity that knows the identity of the user. However, anonymization is already failed at the point of using the platform that knows the identity of the user.

To achieve more improved privacy, PenceCoin implements improved version of CoinJoin. A transaction can be formed by multiple payments from multiple users by merging it. At least three users are required to execute a private transaction. The key to achieve the privacy is using fixed denominations of 0.1 PenceCoin, 1 PenceCoin, 10 PenceCoin, 100 PenceCoin, 1,000 PenceCoin. When a private transaction is formed, users who requested the same amount of PenceCoin for the transaction are grouped. A fixed amount of fee for the private transaction is charged equally to the grouped users in kepts as the information of sender, the original address, is order to avoid the situation the output amount is different for each user as they pay different fee.

The grouping process is done by masternode network. A user can request to the masternode network for making a group at a fixed interval to execute private transaction with a sum of denominated amount, without sending any identifiable information. After the masternode network receives the message, they gather users who want to send each denominated amount. When the enough number of users are gathered, the masternode network sends a signal to users asking to prepare a certain denominated amount, and it is called a “round”. This “round” is repeated until the largest amount of transaction among users asked is fulfilled. Users send the amount of the round to a randomly generated wallet address of themselves each round. After all the rounds are finished, masternode network sends a signal that the rounds are finished. Then masternode network prepares two lists for the inputs and outputs of the joint transaction, and users sends the inputs, the randomly generated addresses, and outputs to the lists. The transaction occurs from the randomly generated addresses of a sender directly to the receiver when the list is written and signed completely. As the wallet client of the user knows the generated address, wallet can show the history of transaction. Receiver as well can see the transaction on the blockchain, its output address and the amount sent. The privacy can be kepts as the information of sender, the original address, is not delivered to the masternode network.

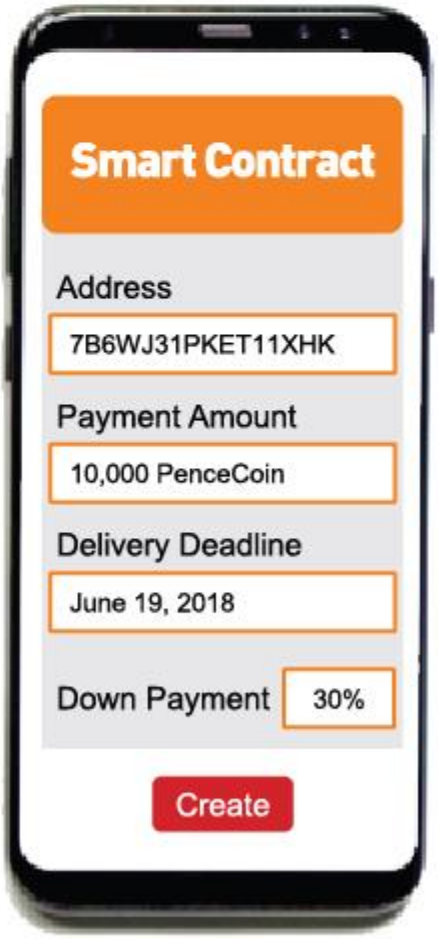
PenceCoin uses Schnorr signatures at the signing phase. With Schnorr signatures, higher privacy level is achieved. The private transaction feature of PenceCoin merges a number of payments into one transaction. The masternode network applies Schnorr signature with aggregated signatures of each payment when the payments are combined. Therefore, this transaction looks as if it is a single big transaction with only one signature. Hence, the private transaction achieves high privacy, and also high efficiency for the size of the block and resources needed for computation.

Furthermore, Schnorr signatures are used for smart contracts as well. With the idea of the scriptless scripts [7], PenceCoin runs smart contracts off-chain by using Schnorr signatures. Many details of the contract including the information of the participants and the amount of capital are exposed to the whole network with conventional on-chain smart contracts. It is not desirable for the purpose of smart contracts, especially for business-to-business contract. However, with scriptless script system, the network does not know the details of the contract and knows only the agreement among the participants of the contract, whether the participants verified that the result of the contract is valid according the terms of the contract. It means that the scriptless script gives benefits to the network, as they can save the resources for the computation, and also to the users, as they can make smart contract with lower fee. Because of these benefits, PenceCoin is considered to attract more users as a financial platform for making contract.

2.5 Wallet

The mobile wallet of PenceCoin will be provided for iOS/Android. The wallet will have pretty simple UI to give intuitive usability with good user experience. The main feature of the wallet is a form that can create smart contract easily. The smart contract form has a few text boxes for key components of a contract. It has text boxes for the address of the counterparty, key dates like the deadline for delivery of promised product or service, an amount of the whole payment, a ratio of down payment and so on. Though many other features and details like a text box that can store the terms of agreement can be added, it would be optional and the basic form will be quite simple.

In addition, the network of PenceCoin has privacy transaction feature though, mobile wallet also has a feature to improve privacy. It is known that one of the most frequently used hacking techniques is just watching the password when a user types it, and it is same for the cryptocurrency. When the mobile wallet has a fixed address, the address will be shown to the other people everytime the user uses mobile wallet. It means the address can be address, so a hacker can target the user easily by checking the financial transaction history of the address. To avoid this kind of situation, PenceCoin mobile wallet randomly generates a temporary barcode and users can make transactions with the barcode. As the barcode is valid only for a short period until the transaction is completed, the risk of being hacked can be significantly lowered.



Smart Contract

Address
7B6WJ31PKET11XHK

Payment Amount
10,000 PenceCoin

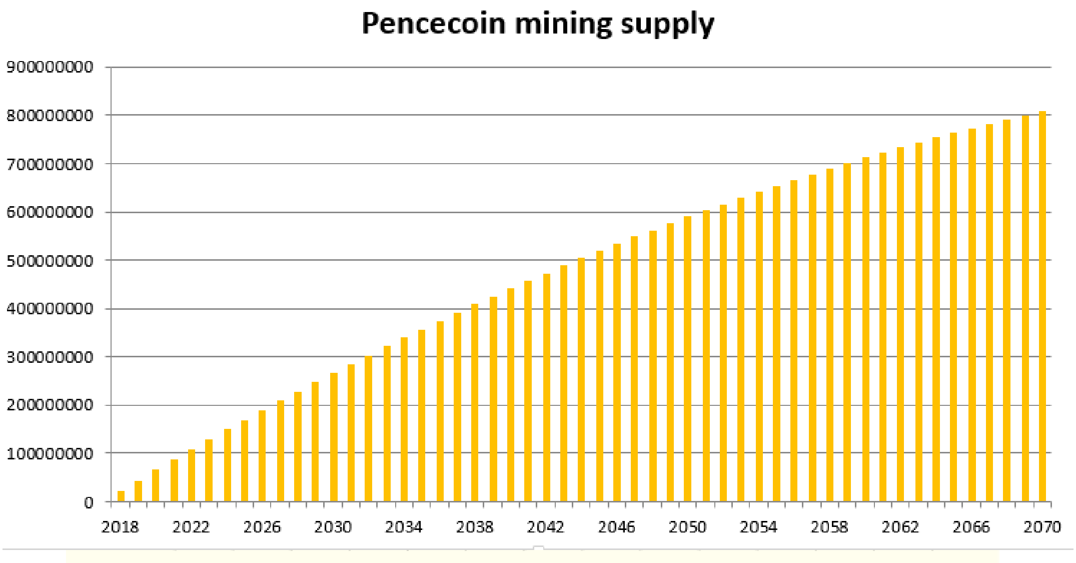
Delivery Deadline
June 19, 2018

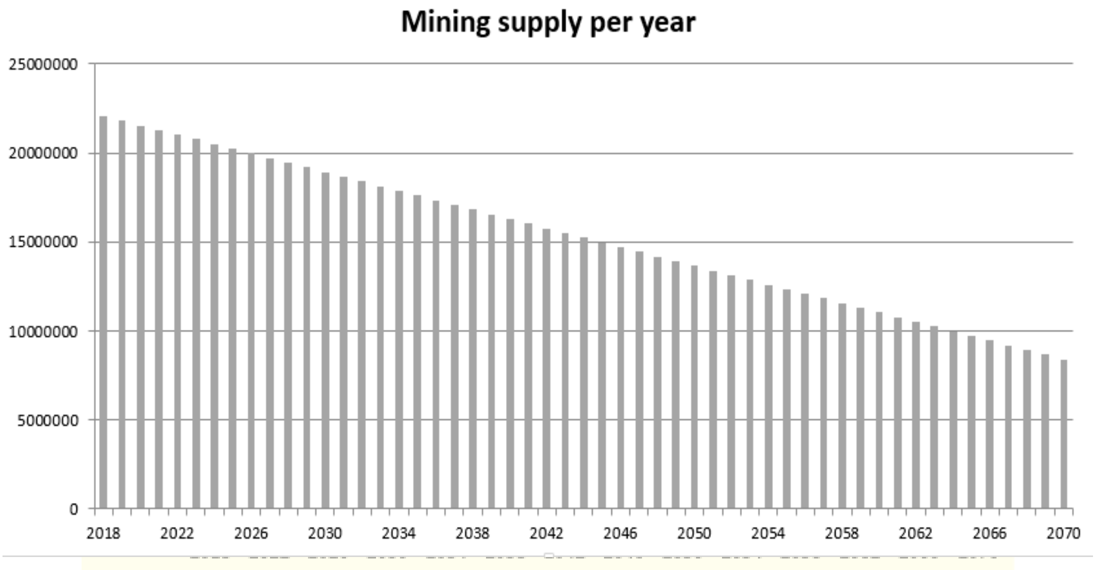
Down Payment 30%

3. Future roadmap

3.1 Mining

The mining supply, including the rewards for masternodes, of PenceCoin will be reduced by 1.2% per year, in order to restrict the inflation of PenceCoin. The total mining reward for the first year is about 22 million PenceCoin. PenceCoin will be produced for about next 52 years, and it will reach 800 million, the maximum supply for mining, in 2070.





3.2 Use cases

PenceCoin team will focus on making the real-world use cases. The introduction of PenceCoin will be started with the business-to-business cross-border trade fields by securing the clients such as large-scale franchises, and the business target is their supply contracts. Once PenceCoin is introduced for their contracts, the psychological barriers of the business entities about PenceCoin will be lowered. Along with this first-mover advantage, the target market will be gradually expanded to retail stores connected to the aforementioned business entities. With this strategic approach, seamless user experience will be provided from their business to the daily life. As the essence of the financial transaction is same regardless of the size of the transaction, the platform that is easy to use for the large-scale contract will be equally easy to use for simple daily financial transactions such as personal wire transfer.

PenceCoin will establish the payment network for both online and offline with partnerships, and the proprietary protocol and module will be provided for the partners in order to become the true daily payment method. With the collaboration with APS card, PenceCoin can be used for the offline payment. Digital authentication tool is needed in order to be used as the offline payment method, PenceCoin found a credit card can be used for the authentication. As mentioned earlier, offline payment with a cryptocurrency was not plausible because of the high transaction fees and long waiting time. However, PenceCoin system processes the proprietary credit card transaction for APS card with the masternode network, therefore PenceCoin can be used at retail stores without any modification for their payment transaction system. The proprietary credit card transaction will be processed instantly, almost same with the credit card payment, with the masternode network, and the information for the transaction will be securely processed. The details for the credit card transaction will be announced by APS and this collaboration will have significant impact for the cryptocurrency ecosystem.

The optimization for the confirmation time of ordinary transaction will also be progressed. The ordinary block time of PenceCoin, one minute, can be too long for the daily personal transaction. PenceCoin network will use artificial intelligence system to ease that kind of inconvenience predicting the probability that the transaction can be problematic. This feature will beneficial to a small amount of payment, and it will be available if the user agrees to use.

Furthermore, a development of a social platform connecting the people all over the world is considered. PenceCoin will be the native token for the platform being used as the payment method within the service. Moreover, the reward program that provides a reward (i.e. PenceCoin) according to the engagement, such as time spent on the platform, total sent messages, the number of connected people, is being planned.

We make countless number of contracts and payments.
With PenceCoin, it will be easier and safer.

References

① Satoshi Nakamoto. Bitcoin: A Peer-to-peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf, Oct 2008.

② bitcoin.org/bitcoin.pdf, Oct 2008.

③ Bitcoin.org. Protect your privacy. https://bitcoin.org/en/protect-your-privacy

④ Nick Szabo. Smart Contracts: Building Blocks for Digital Markets. http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html, 1996.

⑤ Vitalik Buterin. A Next-Generation Smart Contract and Decentralized Application Platform. https://github.com/ethereum/wiki/wiki/White-Paper, 2015.

⑥ Gregory Maxwell. CoinJoin: Bitcoin privaty for the real world. https://bitcointalk.org/index.php?topic=279249, 2013.

⑦ Andrew Poelstra. Mimblewimble and scriptless scripts. https://diyhpl.us/wiki/transcripts/mit-bitcoin-expo-2017/mimblewimble-and-scriptless-scripts/, 2017.