# ALC Coin: A completely Decentralized Digital Cash

Subhas Mallik

alccoin.org

# Abstract

The basic fundamental of a crypto currency is its decentralized nature.

However, with the evolution of Bitcoin, many other kind of crypto currency has evolved. And we expect many more to come. This diversity estranged the pure decentralization leading to formation of central exchanges as third party. We propose a system of exchanging different crypto currencies without a third party, by implementing the Lightning Network, which allows

Atomic cross-chain trading. The atomic swap utilizes hash time-locked contract to link blockchains, so does the lightning network to link payments channel. This in-turn allows to effectively using multisig addresses which could eventually lead to a consumer and merchant friendly form of payment. On the other hand we also propose Equihash protocol for mining, which will eventually allow small miners to mine and keep the currency totally decentralized. The major focus of this project is on the financial exclusion of Eastern world by western monopoly on cryptocurrency and decentralized industry as a whole.

**Contents**

1. **Background**
2. **Scalability Problem**
3. **The Lightning Network**
4. **How it works**
5. **Achieving Pure Decentralisation**
6. **Consensus And Mining of Blocks**
7. **Conclusion**
8. **Acknowledgment**
9. **References**

# Background

* 1. In 2017, the ecosystem of crypto currency has filled with a wide number of different crypto currencies; each has its own need, and follows certain mechanism. We need a particular one for specific purposes, therefore the need of 3rd party crypto exchanges arise. These exchanges have made the market more of a centralized kind, since we lose our complete ownership of tokens when we keep them in such exchanges. Besides, a considerable population of the world is yet to experience crypto currency for the first time. The current development in technology and infrastructure has not sufficed to make end customer experience easy. The normal customer and merchant find it too fancy and sophisticated to be used in daily life. The transactions in Bitcoin or other crypto currency is irreversible, which makes it difficult to use in practical trades where chargebacks are often required. We are focused to bring a currency system which is more like cash (which is referred to 'ready money') in digital form, resulting in mass acceptance by merchants and end customers.
  2. On the other aspect of economics, there is a lack of an open decentralized organization like Ethereum in South East Asia. Through this project we want to build that gap. The Asians always had to follow west for the technology and now even for the financial aspect with cryptocurrency in the frame. To avoid the same scenario in decentralized industry, we propose a native blockchain for the Asian demography, with all the strengths of world’s most accepted Ethereum protocol. This open source project shall motivate developers in the Asian community to build various kind of useful smart contracts and tokens to be used by millions of people.
  3. We will use the Equihash protocol for consensus process. Ethereum uses Keccak-256 for consensus. The Equihash protocol is ASIC resistant, thus lets small miners to participate in consensus. In Ethereum new blocks are mined by the Ethash mechanism, but with Equihash mining occurs with each transaction which requires very small processing power.
  4. As Ethereum, Alchemist is also Turing complete thus developers can build smart agents on our blockchain. This possibility can have a huge impact on the society, businesses, fintech and many industries. In overall, it leads to the form of Alchemist Virtual Machine (AVM). Our network will be a world computer where all can access and use for their own work. Initially Solidity will be used as turing complete language for the AVM, but later we shall introduce a more advance high level language for developing dApps and individual tokens.

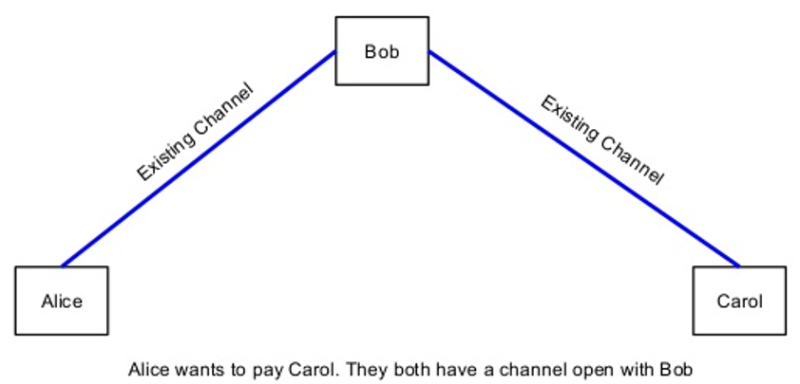


# Scalability Problem

A transaction on the blockchain gets completed when a new block is formed. Due to this design of blockchain, the block size becomes rate determining step for the speed of the transaction. Also the size of the blocks are limited (like 1 MB Block size in Bitcoin), which limits the no. of transactions to be recorded in a block to a very small number (7 transaction per second). Moreover, if we keep on increasing the block size for more transactions, then consequently the size of the blockchain increases enormously. Therefore we implement the concept of lightning network which runs off-chain and allows transactions to process over payment channels and without having to broadcast transactions onto the blockchain. The transaction needs to be broadcasted onto the blockchain only if a participant in payment channel acts as a jerk. In this way it’s possible to make billions of transactions in seconds, which is actually necessary for mass acceptance of a payment system.

# The Lightning Network

Lightning is a decentralized network using smart contract functionality in the blockchain to enable instant payments across a network of participants. A network of ALC payment channels cooperate in a trustless manner to complete transactions without hitting the blockchain. Lightning is a hashed time –locked contract which means the participants are bound to cooperate in a given interval of time otherwise the money gets refunded to the sender.



# How it works

The Lightning Network is dependent upon the underlying technology of the blockchain. By using real Bitcoin/blockchain transactions and using its native smart-contract scripting language, it is possible to create a secure network of participants which are able to transact at high volume and high speed.

**Bidirectional Payment Channels**. Two participants create a ledger entry on the blockchain which requires both participants to sign off on any spending of funds. Both parties create transactions which refund the ledger entry to their individual allocation, but do not broadcast them to the blockchain. They can update their individual allocations for the ledger entry by creating many transactions spending from the current ledger entry output. Only the most recent version is valid, which is enforced by blockchain-parsable smart-contract scripting. This entry can be closed out at any time by either party without any trust or custodianship by broadcasting the most recent version to the blockchain.

**Lightning Network**. By creating a network of these two-party ledger entries, it is possible to find a path across the network similar to routing packets on the internet. The nodes along the path are not trusted, as the payment is enforced using a script which enforces the atomicity (either the entire payment succeeds or fails) via decrementing time-locks.

**Blockchain as Arbiter**. As a result, it is possible to conduct transactions off-blockchain without limitations. Transactions can be made off-chain with confidence of on-blockchain enforceability. This is similar to how one makes many legal contracts with others, but one does not go to court every time a contract is made. By making the transactions and scripts parsable, the smart-contract can be enforced on-blockchain. Only in the event of non-cooperation is the court involved – but with the blockchain, the result is deterministic.

# Achieving Pure Decentralization

The problem of exchanging different digital currencies has created a kind of centralization with different 3rd party exchanges. With the implementation of lightning, atomic cross-chain trading is possible. This concept was first proposed by Tier Nolan as Atomic Swap of two currencies on different blockchains. With the atomic swap feature we make it possible to get rid of 3rd party exchanges. The algorithm of atomic swap given by Tier Nolan is here:

A picks a random number x

A creates TX1: "Pay w BTC to <B's public key> if (x for H(x) known and signed by B) or (signed by A & B)"

A creates TX2: "Pay w BTC from TX1 to <A's public key>, locked 48 hours in the future, signed by A"

A sends TX2 to B

B signs TX2 and returns to A

1) A submits TX1 to the network

B creates TX3: "Pay v alt-coins to <A-public-key> if (x for H(x) known and signed by A) or (signed by A & B)"

B creates TX4: "Pay v alt-coins from TX3 to <B's public key>, locked 24 hours in the future, signed by B"

B sends TX4 to A

A signs TX4 and sends back to B

2) B submits TX3 to the network

3) A spends TX3 giving x

4) B spends TX1 using x

This is atomic (with timeout). If the process is halted, it can be reversed no matter when it is stopped.

Before 1: Nothing public has been broadcast, so nothing happens

Between 1 & 2: A can use refund transaction after 72 hours to get his money back

Between 2 & 3: B can get refund after 24 hours. A has 24 more hours to get his refund

After 3: Transaction is completed by 2

- A must spend his new coin within 24 hours or B can claim the refund and keep his coins

- B must spend his new coin within 72 hours or A can claim the refund and keep his coins

For safety, both should complete the process with lots of time until the deadlines.

# Consensus and Mining of blocks

The generation of new blocks is done by PoW algorithm as used in Ethereum called Ethash. The reason of using a new algorithm for PoW was to attack the problem of mining centralization,  where a [small group](https://pbs.twimg.com/media/CVhkEhtUAAAl0LH.jpg) of hardware companies or mining operations acquire a disproportionately large amount of power to impact or manipulate the network (should they so choose). The economic forces within existing networks (such as Bitcoin and Litecoin) make centralization of mining efforts highly profitable, in part **due to the possibility for producing**[**ASICs**](https://en.wikipedia.org/wiki/Application-specific_integrated_circuit), specialized chips specifically designed to outperform standardised computer hardware by many orders of magnitude in hashing performance. Other factors that promote mining centralisation, such as handling of orphaned blocks, are tackled separately within the Ethereum protocol. **By specifically designing an "ASIC-resistant" PoW algorithm, the Ethereum team hopes to reduce economic incentives for mining centralisation** in Ethereum, [at least until a secure PoS algorithm can be designed and deployed](https://ethereum.stackexchange.com/questions/9/why-does-ethereum-plan-to-move-to-proof-of-stake). The mechanism will be updated to PoS as soon as Casper is released to the Ethereum blockchain.

We are using a much more efficient mechanism for block generation, Equihash. Equihash was first used by Zerocoin, then Zcash. It is well verified by Zcash community that mining Zcash is relatively easier than any other coin.

# Conclusion

We have proposed a new form of payment for masses and call it Digital Cash. We first stood with the design of Ethereum. Then addressing the current issue of scalability, we proposed a mechanism for off-chain transaction via the lightning network. This implementation increases the speed to billions of transactions per second. To get rid of 3rd party centralized exchanges, we suggested the concept of Atomic Swap through the lightning network, which effectively allows cross-chain trading. Finally, as we are committed to keep the new proposed system as eco-friendly, we focused on Equihash mechanism for mining of new blocks. We have introduced a public blockchain with a Turing complete language Solidity. Alchemist Virtual Machine (AVM) will allow masses to develop dApps, tokens and other products which could be highly impactful fir the society.Ultimately we have formed a structure which is self-sustainable and efficient enough for mass adoption by customers and merchants as form of payment in their daily life.

# Acknowledgement

We are gratitude towards the developers of Ethereum as they form the base of our model, to Satoshi Nakamoto for giving the world Bitcoin, The Lightning Network team who addressed the most awaited upgrade to the bitcoin framework, Tier Nolan for his work on Atomic swap, Zerocoin paper for Equihash mechanism, and the whole Blockchain and crypto community who are anticipating the future of Digital Currencies.

# References

1.] Nakamoto S. (2008): Bitcoin: A peer-to-peer electronic cash system. (<http://www.bitcoin.org/bitcoin.pdf>)

2.] Joseph Poon and Thaddeus Dryja for The Lightning white paper. (https://lightning.network/lightning-network-paper.pdf)

3.] Vitalik Buterin for the Ethereum White paper https://github.com/ethereum/wiki/wiki/White-Paper#code-execution

4.] Tier Nolan: Atomic cross-chain trading