ACH NETWORK

Whitepaper

AUTOMATIC CLEARING HIGH SPEED NETWORK

Contents

Abstract

We design and implement ACH Network, the first cryptocurrency based on a provably secure and scalable public blockchain design using both proof-of-work and proof-of-stake mechanisms. However, PoW has critical limitations that curtail its potential to empower a truly massive distributed economy and is justly criticized for its slowness, consumption of large amounts of energy, and congestion pricing in the form of high transaction fees. Different from the proof-of-work based Bitcoin, our construction uses two types of resources, computing power and coins (i.e., stake). The blockchain in our system is more robust than that in a pure proof-of-work based system; even if the adversary controls the majority of mining power, we can still have the chance to secure the system by relying on honest stake. In contrast, Bitcoin blockchain will be insecure if the adversary controls more than 50% of mining power. Our design follows a recent provably secure proof-of-work/proof-of-stake hybrid blockchain. To resolve these current limitations of PoW, we introduce a new strategy for difficulty adjustment in the hybrid blockchain and provide an analysis of it. We also show how to construct a light client for proof-of-stake cryptocurrencies and evaluate the proposal practically. We implement our new design. Our implementation uses a recent modular development framework for blockchains, called ACH . Our Proof of Activity (PoA) protocol offers good security against possibly practical future attacks on Bitcoin, and has a relatively low penalty in terms of network communication and storage space.

Introduction

The emergence of decentralized cryptocurrencies like Bitcoin has the potential to significantly reshape the future of financial transactions and distributed interactions in general, and eventually bring us a much more organized and documented digital world. In the Bitcoin system, a public distributed ledger, called blockchain, is maintained by a peer-to-peer network of nodes called Bitcoin miners via the proof-of-work (PoW) mechanism. Essentially, the proof-of-work mechanism enables an open blockchain, where miners are allowed to join and leave the system at any moment.

In this paper, we introduce ACH Network to analyse the security and performance implications of various consensus and network parameters of PoW blockchains. Based on our framework, we devise optimal adversarial strategies for double spending and selfish mining while taking into account real world constraints such as network propagation, different block sizes, block generation intervals, information propagation mechanism, and the impact of eclipse attacks. Our framework therefore allows us to capture existing PoW-based deployments as well as PoW blockchain variants that are instantiated with different parameters, and to objectively compare the tradeoffs between their performance and security provisions.

Blockchain Technology, having been around since 2008, has recently taken the world by storm. Industries are beginning to implement blockchain solutions for real world services. In our project, we build a Proof of Work based ACH network consensus protocol and evaluate how major applications can run on the underlying platform. We also explore how varying network conditions vary the outcome of consensus among nodes. Furthermore, to demonstrate some of its capabilities we created our own ACH Network.

Background

Nakamoto's blockchain We here briefly review Nakamoto's Bitcoin blockchain. Bitcoin blockchain is based on proof-of-work puzzles, which can be abstractly described via the following hash inequality: $H(hw,w,X) < T$ where $hw \in \{0,1\}$ κ is the hash of the previous proof-of-work block (κ is a security parameter), w is a suitable solution for this puzzle, X is the record component of the block, and T denotes the current proof-of-work target. Extending the chain. At any point of the protocol execution, each miner attempts to extend the blockchain. More concretely, upon receiving some record X, a miner chooses random $w \in \{0,1\}$ κ and checks whether w is a valid solution to the above hash inequality with respect to hw, hash value of the last block in the blockchain; if so, the miner reveals the solution to the system. In Nakamoto's design, multiple miners might and distinct solutions with the same preceding block, in which a blockchain fork will be introduced.

About Mining

Mining is the integral process wherein generation, transmission and validation of transactions of cryptocurrencies is done. It ensures stable, secure and safe propagation of the currency from the payer to payee. Unlike fiat currency, where a centralized authority controls and regulates the transactions, cryptocurrencies are decentralized and work on a peer-to-peer system. Banks that generate physical currency and monitor the transactions require huge infrastructure to function and operate. Cryptocurrencies overcome this need by implementing a mining system where people in the network, called 'miners' or 'nodes', monitor and validate transactions which generates currency. In cryptocurrency, a transaction is a transfer of coins from one wallet to another. When a transaction is made, the details of the transaction will be broadcast to every node in the network. The transactions made over a set period of time are collected to form a 'Block'. To incorporate transparency in the system, it is designed in such a way that all the transactions made from the inception of the currency are recorded and maintained in a general ledger called the 'Block chain' which, as the name suggests, is a list of blocks created from the beginning. Miners play a predominant role in mining. Miners process transactions by verifying the ownership of the currency from source to destination. Every transaction contains the hash of the previous transaction made by the owner through which authenticity of a present transaction is tested, thereby validating it. Miners also inhibit double spending of the currency through this validation process. The main purpose of mining is to generate and release coins into its coin economy. Whenever a transaction takes place and is validated, miners collect these transactions and include them into the block they are currently solving. Every block has to be solved before being broadcasted and put in the block chain. Solving of a block involves mathematical puzzles which are difficult to unlock and crack provided there will be some constraints on the output generated. Only on solving the mathematical puzzle is one allowed to add the block to the ledger and a reward of coins is given in return. Thus mining eventually boils down to a competition of mathematical puzzles to solve for the reward of coins. This mechanism prevents miners from easily procuring coins and thus maintains the fairness of the system.

Proof of Work (PoW)

PoW(Proof of Work) distributes digital currency according to the workload of miners. The higher the performance and the more the number of the mining machine, the greater the workload, the more digital currency will be distributed. 6 / 71 Bitcoin is a typical example of using the PoW scheme. Miner gets the right of packaging through mining that solved a mathematical problem. If successful, the miner receives bitcoin reward because of costing computing power. To control the currency rule, mining is set to a more complex model. Because the possibility of solving the problem by one miner depends on his calculating power, the difficulty of mining is determined by the sum of all the calculating power in the system. For the cryptocurrency of PoW, miners confirm transactions by competing to solve a mathematical problem. The first miner solved mathematical problem receives the reward. The complexity of the problem is designed to control the currency rule. This method solved the Byzantine general problem very well, but it was criticized by others as inefficient due to the waste of resources. At the same time, the only PoW consensus also faces security problems such as the 51% attack. With the development of the BTC and blockchain industry, the disadvantages of PoW are also exposed. For example, the currency owner cannot participate in any decision-making, and rights concentrated on miners. This runs counter to the idea of decentralization that decision-making right is concentrated on a few miners.

Delegated Proof of Stake (DPoS)

DPoS is a new consensus algorithm to guarantee the security of the digital currency network based on PoW and PoS. It can not only solve the problem of excessive energy consumption caused by PoW in the mining process but also avoid the problem of "trust balance" of PoS. Then, DPoS has become the representative of consensus 3.0. DPoS allows many users to participate in mining, which means that each currency owner can vote. And then generate some delegates of the same rights which understood as some nodes or pools. Their rights to each other are exactly equal. Currency owners can change these delegates at any time by voting to maintain the “long purity” of the chain system.

EDPoS+CPoW

CPoW (ContinuityProof of Work) and EDPoS (Extensible Delegated Proof of Stake) came into being to prevent the entire ecological operation stopping from the collapse of a single consensus node, and prevent the block network as a whole is not available from the collective stopping of DPoS nodes. BigBang Core's security consensus mechanism is EDPoS + CPoW. Block reward is the mining reward plus the total transaction fee of block transactions. Voting for an EDPoS node by token can increase the probability of the node packaging. Then Voters share the block reward by vote. The node needs to raise more than 2% of the total Token supply to become an EDPoS node.

Challenges with traditional mining

High Energy Costs

To maximize successful mining chances, you'd need to combine hundreds of ASICs together to solve one problem. Consequently, this would require extremely high power output, which will cost you exorbitantly high electric fees. A CBS News report revealed that Bitcoin mining consumes more energy than 150 countries. But here are possible ways in which this challenge can be solved.

1. Crypto miners can opt for less power-intensive protocols. One of them is the Proof of Stake (PoS) consensus that secures networks through the staking of crypto. Currently, Ethereum and Cardano are leading this shift. (Note: This does not solve the centralization problem, as higher stakes attract more interest. Only those who can afford to hold their crypto, and substantial amounts at that, benefit from the protocol.)

2. Running your mining activities on mining facilities and mining data centers that are powered by renewable hydroelectricity and solar energy. Mining companies like Hydrominers and Burency mitigate high energy costs by powering mining activities via hydroelectricity, and their mining plants are found around colder regions to reduce heat-dissipation costs.

Vulnerability to Cryptojacking

Beyond creating a democratic space, the essence of decentralization is to assure security, right? Well, hackers are getting more sophisticated at tapping your resources. In fact, in 2017, Auguard reported a 31 percent growth rate in in-browser cryptojacking. Meanwhile, power concentration is not only susceptible to malware attacks, but cyber thieves are now adopting a ransomware-like tactic to remotely mine cryptocurrencies from people's computers.

There is no conventional solution to tackle this problem per se, but an improvement to PoS adopted by DigiByte, which uses a hybrid of five protocols on its blockchain platform, is a strong means crypto miners can use to defend against this form of attack. Meanwhile, it is interesting to know that each protocol contributes only 20 percent to secure the platform in this case. So, if one system is under threat, 80 percent remains unaffected. In the same way, this hybrid model helps counter centralization. At any given point, a miner will only control 20 percent of the network, even if they were responsible for 100 percent of mining in a given protocol.

Centralization

ASICs have proven adept at solely mining a specific cryptocurrency. They are so powerful that once a coin-specific ASIC is released, it's sometimes challenging to mine without one. While this is a great development in the crypto industry, it is also perceived as a problem, because many crypto miners are influencing the way and manner in which ASICs are being created or designed. And since there are very few ASIC manufacturers, the mining space will eventually be centralized. However, there two possible ways to address this problem: Decentralizing the manufacturing process of ASIC miners, and putting into effect a new hash algorithm that would effectively wipe out all existing ASIC miners.

AUTOMATIC CLEARING HIGH SPEED NETWORK

ACH Overview

Automatic clearing High Speed (abbreviated as ACH) is a new cryptocurrency based on ACH method, which can effectively resist ASIC and avoid concentration of computing power. ACH also adopts CPoW mining mechanism innovatively, which limits the mining participation entry. Through this mechanism, it could effectively avoid the power monopoly, reduce the amount of digital currency flowing into the market and increase the income of miners. There is no longer competition between minors, but cooperation, which makes ACh more secure and trustworthy to stimulate the sustained growth in quotation.

ACH Network Solution

ACH is not only a new type of cryptocurrency, but also a reshuffle of the traditional mining industry. It subverts the concept of traditional mining and can effectively solve the following problems:

- Computing Power Monopoly - ACH using an improved ACH algorithm that can effectively resist the ASIC mining machine and prevent the power monopoly from the large miners which cause it is too difficult for retail investors to obtain profits.

- Malicious Smash - The CPoW mining mechanism adopted by ACH can reduce the number of market circulation, increase the miner's coin- holding period, prevent miners from digging with selling which invisibly lead to malicious smash.

- Over Increase of Computing Power - The CPoW mechanism can effectively control the number of mining machines to grow too fast. The number of ACHs circulating in the market is limited. To increase the number of mining machines, there must be enough ACHs to be pre- stored in the wallet, which can inhibit the quantity increase of mining machines to avoid the loss of miners' interests.

- Increase the Right of Miner - ACH mining must be held in ACH and pre-stored in the wallet to mine for higher interest, ACH is more like a miner's rights protection. Only holders can enjoy high returns, and not holding ACH will not be able to obtain high profits.

ACH Network Architecture

New developments in consensus designs like Proof-of-Stake (PoS) offer dramatic improvements to the traditional single-chain Bitcoin-style protocol in terms of throughput and confirmation latency. These advances have led networks such as Ethereum network to aspire to move away from PoW as soon as possible. While PoS offers the attractive advantages of deterministic confirmation and a significant boost in performance, PoS is nonetheless fundamentally bounded by the causally consistent execution speed of the application layer, which creates a hard upper bound on throughput. Though sharded PoS networks have been proposed that may further increase throughput, these changes move PoS towards a centralized system that begins to greatly resemble existing trustful financial networks.

The novel architecture of ACH Network is predicated upon two separate, yet related features that operate at distinct layers of the ACH Network stack. Cross-chain cryptocurrency transfers via on-chain SPV smart contracts and parallel-chain binding at the hashing level via peer-chain Merkle root inclusion. The former, which occurs in the application (smart contract) layer, leverages the latter to create valid Merkle proofs of currency transfer. In this section, we will first detail how to enable globally ”mass-conserving”17 cross-chain transfers of cryptocurrency via SPV. This implementation is necessary to avoid per-chain floating currencies that would require dedicated exchange markets to move value between individual chains. Next, we describe the protocol by which parallel chains are bound together to form a ACH network. The protocol itself does not impose an upper bound on network size, and is instead constrained theoretically by existing global IP infrastructure and bandwidth and practically by necessity- ACH Network configurations with throughput in excess of 100,000 transactions per second are not currently necessary.

ACH Mining Rules

The ACH mining mechanism requires the miners to pre-store a certain amount of ACH in the wallet to mine normally when mining, otherwise only 30% of the mining revenue can be obtained.

- If the miner does not deposit ACh in the wallet and runs the mining program directly, then only 30% of the mining revenue will be obtained, and the remaining 70% of the mining revenue will be automatically transferred to the ACH Foundation.

- The miner will receive a 100% return on the ACH specified in the specified address. When the miner does not want to mine, he can withdraw the mortgaged BFC at any time in real time.

- Depending on the computing power, the number of ACHs that need to be pre-stored is different. The higher the computing power, the higher the amount of mortgages required. Pre-stored standard according to 300 ACH per 1K computing power.

Model

To better understand how concentration in a blockchain affects double spending attacks we consider pools and miners in an industrial organization framework. We find that concentration in mining power is harmless for the networks resilience against double spending attacks. The findings stem from the fact that, the larger a pool is, the more it loses if the network value collapses. Hence, even if a large pool is more able to conduct mischief, it should be less willing to do so. Our model is stylized, yet its intuition carries over to other settings where large miners, pools or coalitions receive economic profits.

Model Setup

Consider a world in which time is infinite and discrete and is indexed by t, t = 0, 1, 2, . . . There are two types of agents – miners and pools – having a discount factor β ∈ (0, 1). Miners are homogeneous, risk averse and atomistic, whereas pools are risk neutral. In every period $t \geq 0$, miners choose their hashing power at a unit cost C, and hashing power allocation hm for each pool m ∈ {1, 2, ..., M} and ho for solo mining.

Mining Pools

Mining pools offer different fee and reward contracts; the simplest mechanisms being proportional payment and pay-per-share . In a proportional reward system , whenever a pool wins a mining competition a miner receives

$$(1 - f^m)R\frac{h_i}{H_m} \qquad (1)$$

where h_i is the miner's hash rate contributed to the pool m, R is block reward, H_m is the total hashing power in that pool and

$f^m$is a fee collected by pool m. In a pay-per-share reward mechanism a pool effectively rents miner's hashing power and pays a rent regardless of whether the pool wins block rewards or not, fully insuring participating miners. However, pay-per-share is uncommon and usually associated with significantly higher fees. In addition, diversification of miner's hashing power to different pools would effectively insure miners against idiosyncratic risk. Hence, in our model we choose to concentrate on proportional reward mechanisms.

Collusive Equilibria

We restrict each pool's strategy to the standard super game grim trigger strategy. Specifically, consider the following strategy for M incumbent pools to collude: 1. Collusion: In every period, pools agree upon a fee $f\ c$. Miners allocate their hashing power to pools.

2. Punishment phase: once one of the incumbent pools does not have any participants, punishment phase is triggered and the pools enter into a Bertrand competition. In absence of marginal costs, and because the pools are homogeneous, the pools will receive zero profits. In a collusive phase the pools discounted future profits are

$$\sum_{t=0}^{\infty} \beta^t \frac{H_m}{h} f_c R = \frac{f^c R}{1-\beta} \frac{H_m}{h} \qquad (2)$$

where H is network's total hashing power and β is the time discount factor.

Corollary 1, ***A collusive strategy is an equilibrium if***

$$\sum_{t=0}^{\infty} \beta^{t} \frac{H_m}{h} f_c R = \frac{f^c R}{1-\beta} \frac{H_m}{h} > f^c R \qquad \forall \frac{H_m}{h} \tag{3}$$

Corollary 1, states that the profit from lowering the fee, and hence capturing the whole market, should be less than the value of discounted future profits in collusion phase. From this naturally follows:

Proposition 1 If

$$\exists \frac{H_m}{h} \quad for\ which\ \frac{H_m}{h} < 1 - \beta \tag{4}$$

no collusion equilibrium exists.

Proposition 1 states that – given the discount factor – there should not exist extremely small pools for collusion equilibrium to exist. E.g. for annual β of 0.9, there should exist pools vesting less than 0.0002 percent of hashing power for collusion strategy not to be a Nash Equilibrium. For the remaining part of the analysis we will assume that such pools don't exist in the market, thus a collusion equilibrium can be sustained. Above, we have assumed that R is constant. In reality, because rewards are paid in a cryptocurrency, they are highly volatile. In our model this would yield the same result, because pools are assumed to be risk neutral. In addition, (some) crypto-currencies 8 Electronic copy available at:

https://ssrn.com/abstract=3506748 have expected declines in rewards (e.g. BTC reward is halved every 210,000 blocks, which occurs approximately every four years). It is a standard result that in these cases the benefit from deviating would be highest just prior to the expected decrease in reward [Rotemberg and Saloner, 1986]. For parsimony we have restricted our analysis from considering such cases.

Entry and Collusive Fee Setting

Every period t ≥ 0 there exists a possible entrant pool without miners. Therefore, an entrant would set a fee $f^e < f^c$ to obtain miners. Prior to an entry the entrant pays a positive entry fee ζ. An entry will trigger the price competition phase and, hence, each pool makes zero profits post entry. Therefore, a condition for a feasible entry is given by

$$f^e R - \zeta > 0 \qquad \text{where } f^e < f^c \qquad (5)$$

Corollary 2 It follows from feasible entry condition (Equation 5) that in order to deter entry colluding pools set a fee f^c

$$f^c \leq \frac{\zeta}{R} \qquad (6)$$

To keep the model parsimonious we have chosen a very simple barrier of entry as is manifested by Corollary 2.

However, one could equivalently assume that, once an entry occurs only an active fraction of miners observes it. Hence the active miners would face a trade-off between lower fees and smaller diversification benefits. In this case, to deter entry incumbent pools' fee setting strategy should make active miners indifferent between choosing an entrant pool or staying in incumbent pools. In addition, incumbent pools have likely established credibility for not siphoning rewards, having a reliable infrastructure etc. all attributes that an entrant might easily lack.

Miners

In every period t, a reward R is randomly assigned to a solo miner or a pool . The probability of winning the reward in every period t is $\frac{h_i}{H_m}$ for a solo miner and $\frac{H_m}{H}$for a pool, where H is network's total hash power and H_m is pool m's hashing power. Whenever a pool wins the mining competition it collects a fee f^m∈ (0, 1) and distributes the remaining reward to participants according to their contribution to the pool's total hashing power $\frac{h_i}{H_m}$. The miner j' s expected utility at t for t + 1 is hence given by the von-Neumann-Morgenstern Utility Function

$$U\left(H_J\right) = \frac{h_0}{H} u(R - C \sum_{i-0}^{m} H_i) + \sum_{i-0}^{m} \frac{H_m}{H} u((1 - f^m) R \frac{h_i}{H_m} - C \sum_{i-0}^{M} h_i \qquad (7)$$

where, $U($ $)$ is a continuous, monotonic and concave utility function and h0 is the allocation to solo mining and hm m ∈ [1, 2, 3, . . . , M] are the allocations to M different pools. Each pool sets a fee f m to maximize its profit.

Equilibrium Hashing Power and Allocation

Proposition 2 Given fees and total hashing power, all miners' symmetric allocations among pools offering the lowest fee are Subgame Perfect Equilibria. Proposition 2 was initially discussed by Cong et al [Cong et al., 2018]. Following intuition of Modigliani-Miller [Modigliani and Miller, 1958] the initial pool size does not matter whenever miner's are able to diversify by allocating their hashing power to multiple pools. Hence, any allocation **where all pools get a share and**? that is symmetric amongst the miners is a Nash Equilibrium. By a symmetric allocation we refer to an allocation in which each miner j allocates the same proportion of hashing power as all the other miners to each pool i.e.

$$\frac{h_{m,j}}{H_j} = \frac{h_{m,-j}}{H_{-j}} \; For\ each\ m\ \in (1,2,3, \dots \dots .. \mathrm{M}) and\ j$$

Corollary 3 Miners allocate their hashing power amongst pools

To acquire miners, pools set fees for which miners prefer pools over solo mining. If miners are atomistic, once a miner prefers mining in pool(s) over solo mining all miners will prefer pools over solo mining. Because pools, in our model, do not have costs and miners are risk averse, there exists a fee $f\ m\ >\ 0$ for which miners prefer pools and which pools are willing to offer.

Proposition 3

Miners' utility function simplifies to the Bernoulli utility function

$$U(H_i) = u\left((1 - f\ c\ )R\frac{\sum_1^M h_i}{H} - C\ \sum_1^M h_i\right) = 0 \tag{8}$$

Proof

It follows from the assumptions that miners are atomistic and mining is competitive, that miners gain zero utility in equilibrium. Therefore, by employing Proposition 2 and Corollary 3 we get Proposition 3.

By allocating according to Proposition 2 miners are able to perfectly diversify mining risk. Total costs are equivalent to a net reward payed to miners. Hence, profits for miners are zero. This simplifies our analysis and corresponds to what is observed in most crypto-currencies, namely that small scale mining is not profitable.

As proposed above, all miners symmetric allocations are Nash Equilibria. Miners, however, would need to coordinate to reach this allocation. Hence, to simplify our analysis we make the following assumption:

Assumption 1

Miners coordinate their allocation amongst pools offering lowest fees at t by employing aggregate allocation at $t - 1$ as a focal point in every period $t > 0$. Miners' allocation at $t = 0$ is exogenously given. In the absence of a definite coordination device, a focal point may function as such [Schelling, 1960][Mehta et al., 1994][Bacharach and Bernasconi, 1997]. We argue that if a set of pools is homogeneous and provides the same service for the same price, previous aggregate allocation is a natural focal point for miners to allocate hashing power. This is accentuated, when there exists a large number of miners causing coordination to be unfeasible. An allocation determined by a focal point is an allocation in the set of possible Nash Equilibria allocations given by Proposition 2. The assumption implies that, ceteris paribus, pool sizes are stable.

Proposition 4 In equilibrium total hashing power H is a function of f, R and C

$$H = \frac{(1-f^{C})R}{C} \tag{9}$$

Proposition 4 follows from Proposition 3 by summing over all miners and it states that in equilibrium, because miners are fully insured against idiosyncratic shocks and make zero profits, total cost of hashing power equals the net reward.

Smart contract

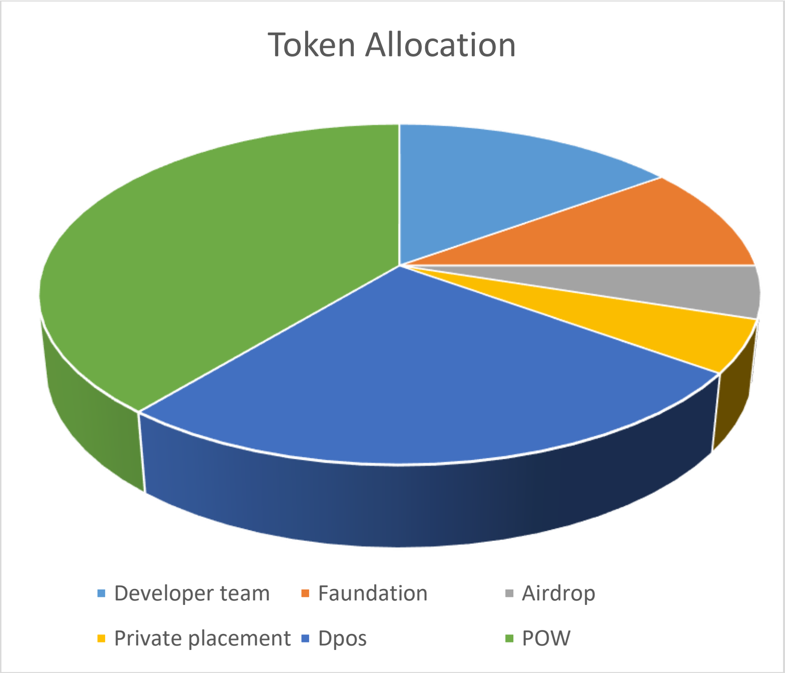
ACH Network mechanism is an essential part of the smart contract. A smart contract that syntactically requires an upgrade governance mechanism. In Pact, this mechanism can be autonomous (e.g. the mechanism in the Ethereum EVM where a hard fork is required to upgrade a given contract), centralized (e.g. a specific set of signature capabilities that is required to enact an upgrade), decentralized or a mixture of the aforementioned. the fundamental cryptocurrency itself is defined by a cryptocharter committed in the genesis block. Moving the definition of the coin to the Pact smart contract layer allows for its formal verification.

Token Distribution

As seen with token distribution of tokens will be dedicated to Development Team, Foundation, Airdrop, Drops and PoW. This percent of issued will be allocated for building business operations.

Business operations:

- Development Team = 15% Token
- Foundation = 10% Token
- Airdrop = 10% Token
- Privacy Placement = 5%Token
- Drops = 26% Tokens
- PoW= 39 % Tokens



Conclusion

In conclusion, ACH Network provides significant advances over existing approaches in scalable public blockchain. It provides unparalleled increases in PoW throughput while keeping the global hashrate, and thus energy required, constant. The confirmation latency of ACH Network is also significantly decreased from traditional PoW and is potentially even 18 lower than that of PoS systems. ACH Network achieves these advances while maintaining the core trustless, decentralized nature of PoW. This protocol enables greater practical decentralization and enables the creation of an ecosystem where enterprises, individual users, and large mining pools can co-exist peacefully by acting selfishly. ACH Network avoids liquidity and centralization problems associated with using staked channels for scaling while also staying in the existing global regulatory context. We present in ACH Network as a solution by which PoW can be scaled such that it support true decentralized economy.

ACH