UniChain

The Technical White Paper

Powered By UniLab

June 27, 2019 [version 1.0]

Abstract

Unichain is a highly scalable blockchain platform that takes advantage of cutting-edge technologies which have the capacity of handling millions of transactions per second without compromising decentralization and security.

UniChain is first and foremost designed to serve the *Uniworld.io* ecosystem [1]. It is a public Blockchain featuring so-called multi-side-chains so everyone can connect and use and build upon this platform for a plethora of purposes. The development tool kits to work with UniChain ecosystems are provided by us as well.

I. Introduction

Blockchain technology is getting more and more sophisticated. It's not just a payment method aka. crypto-currency, but can also be applied to many traditional applications such as loyalty programs, identification of users, for supply chains, in health care, insurance and of course banking [2].

The first and most famous application of Blockchain is Bitcoin which is described as a peer-to-peer electronic cash system. It can process roughly 3 -7 transactions per second (TPS) [3]. Ethereum introduced Smart Contracts and is described as Blockchain 2.0. The maximum number of transactions that Ethereum can handle is 15 TPS [3].

Some of the recent blockchain platforms promise to increase the speed of TPS to hundreds or thousands of TPS by changing the consensus algorithm. For example: Proof of Stake (PoS) or Proof of Authority (PoA), or by applying sharding (multi-chain technologies).

It's clear that those blockchains mentioned above aren't sufficiently functional in practice. The more people join the network, the more transactions and the more time to wait for transactions to get confirmed passes.

Scalability is one of the biggest issues for big Blockchain platforms beside decentralization and security. In the following sections, we propose a new Blockchain platform that combines the advantages of many current Blockchain technologies including side-chain architecture, a DPoS-HotStuff consensus algorithm, the bridge protocol and also an incentive model. We call it the UniChain.

II. Side-chain Architecture

UniChain is a Blockchain platform that supports multi-chain, with the root and central chain being UniChain. This core chain plays an important role to validate all side-chain's states and also links them together.

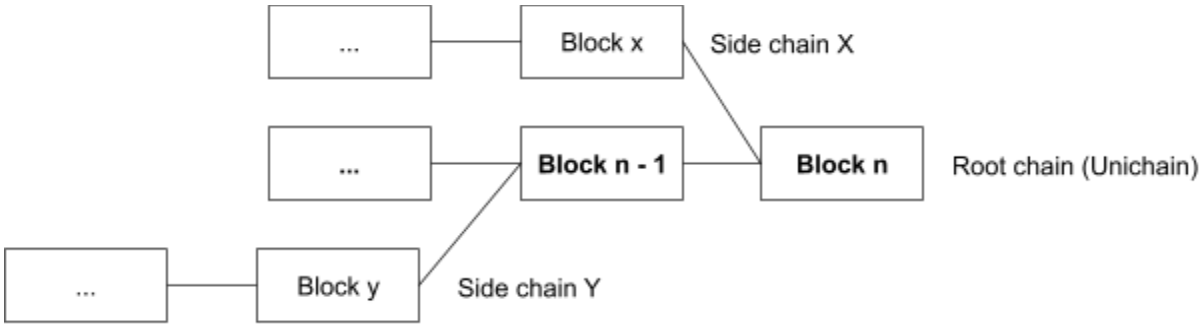

Figure 1. Side-chain architecture

Each side-chain has its own block- and transaction validators. Side-chains are independent from each other, and have a separate ledger. Operations on chain X cannot

take effect on chain Y and vice versa. Because of this independence, we can 'scale-out' the platform as much as we want.

With side-chains able to handle around ten thousand transactions per second, we will reach millions worth if the platform has 100 side-chains.

Communication Between Chains

Side-chains communicate with the root-chain and other chains via smart contracts. UniChain provides the smart contract system for this communication called the *UniBridge protocol*. Funds on side-chains are also held on the root-chain. This allows for fraud proof deposits and withdrawals of funds on side-chains via state transition.

Side-chains do not disclose all information on the root-chain. Instead, blockheader hashes and a bit of states are submitted and if there is proof of fraud on the root-chain, then the block is rolled back and the block creator is penalized by the smart contract system governed by the root-chain.

The UniBridge protocol also helps UniChain to communicate with other Blockchain platforms. I.e. information, token in exchange to Ethereum, Bitcoin, or EOS and so forth.

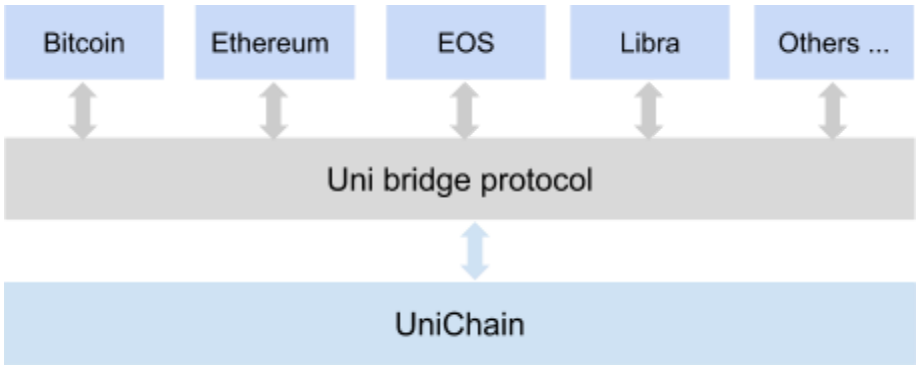

Figure 2. UniBridge protocol

In case of the exchange of tokens to other Blockchain platforms, the UniBridge protocol works as a decentralized exchange.

III. DPoS-HotStuff Consensus Algorithm

Consensus is the heart of any Blockchain platform. The popular consensus algorithm in Bitcoin and Ethereum is Proof of Work (PoW) which consumes huge amounts of electric energy to secure a ledger.

This type of consensus algorithm makes the Blockchain fully transparent, public and decentralized but cannot scale to adapt to the big volume of transactions. In this paper, We apply Delegated Proof of Stake (DPoS) to our platform. DPoS is not a new consensus algorithm. It has been applied in Bitshare, EOS, and others. However, we combine the DPoS with HotStuff [4] and side-chain architecture to make our system scalable and reach Block finality after one second.

DPoS Algorithm

DPoS is a consensus algorithm developed to secure a Blockchain by ensuring representation of transactions within it. DPoS is designed as an implementation of technology-based democracy. Using voting and election processes to protect Blockchains from centralization and malicious usage.

Before you can fully understand how UniChain DPoS works, we need to clarify some of the terminologies:

- Account: A unique identity on UniChain. Each account has it’s very own key pair. The addresses are an account representation on Blockchain.
- UniWorld Cash (UNW): This is the native token of UniChain.
- Stakeholder: Any account with a token balance > 0

- Node: Refers to regular nodes and is a software that anyone can download to run a node and maintain the ledger, validate- and update transactions.
- Witness node: A 'full' node that represents an account with a minimum of 100,000.00 UniWorld Cash and receives enough approving votes from the community. Transactions and blocks are only validated by witness nodes.

In UniChain, there are 55 witness nodes by default. That number may be increased. To become a witness node, Stakeholders must deposit at least 100,000.00 UniWorld Cash to their accounts and then broadcast transactions to register as a witness node candidate. Other stakeholders will vote to decide the witness. The power of votes is based on the amount of tokens stakeholders have. The top 55 candidates with the 'largest' votes will become the witness nodes. The voting process is repeated every 1670 blocks called the epoch. In each epoch witness nodes have the capacity to produce a total of 32 blocks.

How Witness Nodes Produce Block In UniChain

After the election process, 55 elected witness nodes are now ready for producing blocks. The traditional DPoS algorithm 'round-robin' produces blocks. I.e. block *n* is produced by witness *n*

$$Witness \in \{1, 2, 3, n-1, n\}$$
$$Block \in \{1, 2, 3, n-1, n\}$$

The process is predicted and may be broken up by a dishonest witness node. To protect the block producing predictions from being turned, we propose a random witness producing blocks while ensuring that every witness produces an equal number of blocks (32 blocks for each epoch).

Random Witness Chosen Algorithm

$$Witness \in \{1, 2, 3, n-1, n\} \; n = 55$$

$$magicNumber = hexToIn(last\ 10\ Digits(previousBlockHash))$$
$$index = magicNumber\ mod\ 55$$
$$Witness = Witnesses[index]$$

Because the previous block's hash is only known at the processing calculation time, the magicNumber is the unknown number and therefore the next selected witness remains a secret. By using formulations as shown above, one witness may be chosen according to n-time to produce a block and it may exceed the capacity of 32 times correspondingly. To solve this problem, when any witness reaches the maximum number of producing blocks, It is removed from the random selection pool and gives another witness a chance.

HotStuff

HotStuff is a leader-based Byzantine fault-tolerant (BFT) replication protocol for the partially synchronous model. It is used in the Libra project and reduces the communication complexity - linear in the number of replicas. HotStuff changes BFT communication from mesh to star network, which relies on the leader.

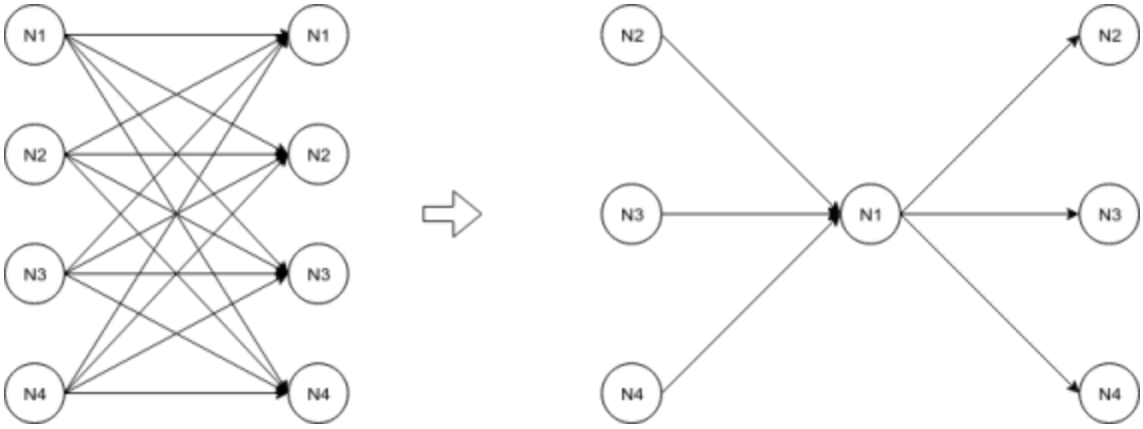

Figure 3. BFT's mesh vs. HotStuff's Star network

The traditionally practical BFT uses two rounds of message exchanges. The first phase guarantees proposal uniqueness through the formation of a quorum certificate (QC) consisting of (n − f) votes. The second phase guarantees

that the next leader can convince replicas to vote for a safe proposal.

The algorithm for a new leader to collect information and propose it to replicas is called the view-change. The view-change two-phase based in traditional BFT and not simple or bug-prone [5]. Any proposal in BFT has a communication footprint of $O(n^3)$ authenticators. The total number of authenticators transmitted - if $O(n)$ view-changes occur before a single consensus decision is reached - is $O(n^4)$.

HotStuff is three-phased,- allowing for a new leader to simply pick the highest QC it knows of. It introduces a second phase that allows replicas to "change their mind" after voting in the phase, without requiring proof of a leader. This alleviates the above complexity, and at the same time considerably simplifies the leader replacement protocol procedure.

	Authenticator complexity		
Protocol	*Correct leader*	*view-change*	*f leader failures*
DLS	$O(n^4)$	$O(n^4)$	$O(n^4)$
PBFT	$O(n^2)$	$O(n^3)$	$O(fn^4)$
SBFT	$O(n)$	$O(n^2)$	$O(fn^2)$
Tendermint/Casper	$O(n^2)$	$O(n^2)$	$O(fn^2)$
HotStuff	$O(n)$	$O(n)$	$O(fn)$

In HotStuff:

- Pre-commit phase: Leader receives the *prepare-vote* for current proposal. It combines to *prepareQC* and then broadcast the *pre-commit* to all nodes in the network
- *Commit phase*: Leader receives *pre-commit* votes from *(n-f)* nodes, then combines it into *precommitQC* message and finally broadcasts to all nodes in the network. When replicas receive the message, It locks the state transition request so that q`1 of the consensus decision can be reached.

- *Decision phase*: When the leader receives enough commit-votes from the network, it combines them to *CommitQC* then broadcasts the *decide*-message to the network. Replicas in the network receive the *decide*-message which executes state transition, commit the state and then start the next view.

The pipelined HotStuff

HotStuff has the 'same phase' at all times: Prepare (not an official phase), pre-commit, commit, and decide.

The flow structure: other nodes vote on a message and the leader combines the votes and broadcasts them to other nodes. These phases can be represented uniformly and pipelined

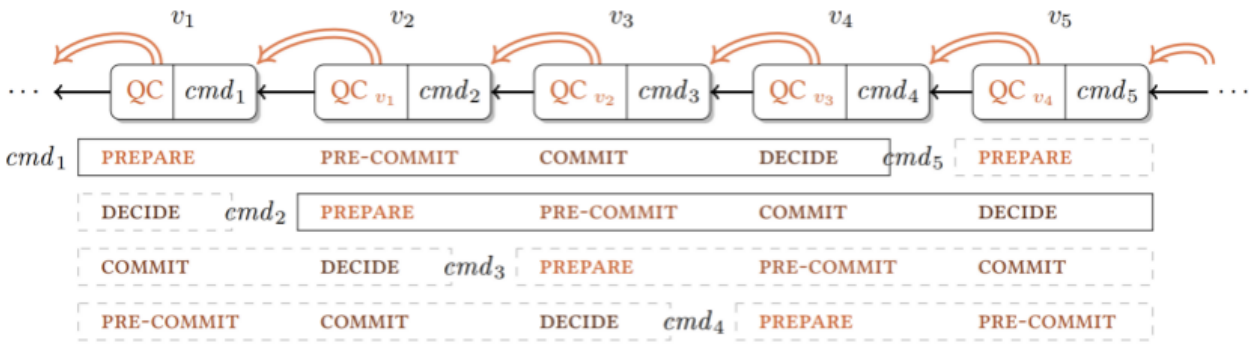

Figure 4. The HotStuff pipeline

IV. Unichain ecosystem & Incentive model

As mentioned above, UniChain is mainly designed for the UniWorld.io ecosystem. Each UniWorld sector is represented by a side-chain. A common chain is for any application and any side-chain may be created by anyone as long as it meets the conditions (as described below).

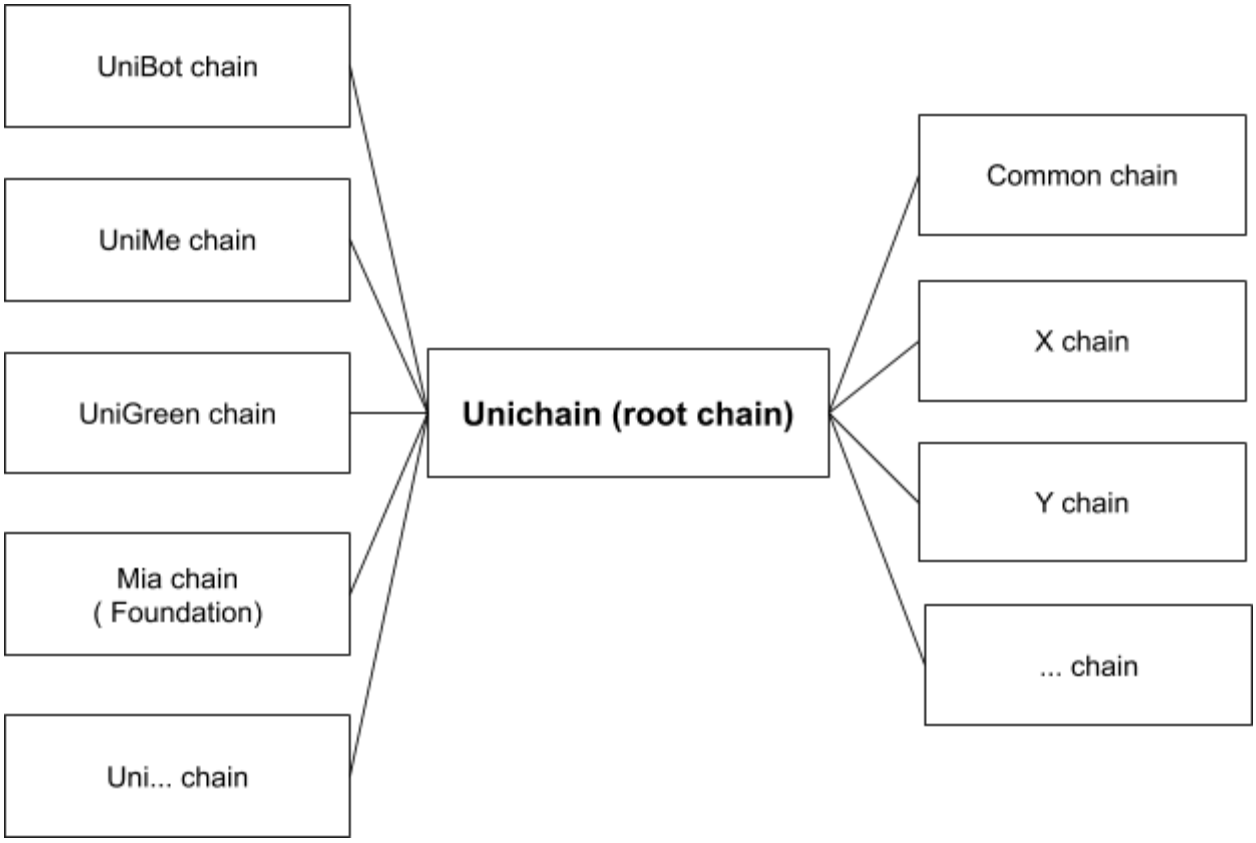

Figure 5. UniChain ecosystem

- UniBot (https://unibot.org) this chain is a Blockchain for Virtual Assistants. A chatbot AI platform. It deploys smart contracts to verify them, store the online payment history and protect fraud transactions.
- UniMe (https://unime.world) is a communication application with new concepts such as where the hosts and customers communicate with and/or through virtual assistants. UniMe acts as a bridge and connects people and bots for business and life also including payment,- and verification functionality.
- The Mia Foundation is a transparent and decentralized fund on a Blockchain network. Built by design to reform/improve industries of health care, education, environment, charity and community. (https://Mia.world). It stands for Multiple Intelligences Alliance. It also acts as a niche social network for technical people.

- The UniGreen chain combines biotechnology, Blockchain and the Internet of Things - IoT - to protect and help the environment.
- The UniChain is related to Intelligent Artificial, they will come in the future as the blockchain that combine two hottest technology trend for society 5.0 economic
- Common chain is for any applications such as finance, gaming …
- X, Y, Z … chain is the chain created for any other purposes.

UniWorld Cash (UNW)(*https://itpo.uniworld.io*) is the main token circulated on (and with) UniChain. However, each side-chain can create native tokens using a smart contract in its chain. It is worth noting that UniWorld Cash is a valid token to all chains and is meant as the medium/bridge to link the chain together. UniWorld Cash (UNW) is also used to pay for transaction fees, to protect the network from spammers or exchange with other tokens (/coins) on the UniChain exchange platform (if UniWorld Cash (UNW) is used to pay for exchange fees, the fee is reduced by 80%).

Create new side chain

Everyone can create a new side-chain if they have a minimum of 250,000.00 UNW in their wallet. These are the steps to create a side-chain:

- K creates a new wallet and deposits > 250k of UniWorld Cash to his wallet
- K creates a special transaction to request the side-chain creation (calling upon a smart contract on the root-chain)
- K's transaction is validated by the root-chain validators (witnesses), and if K meet the conditions, the transaction is valid and successfully added to the ledger returning the chainID
- K creates a side-chain with the chainID above. At this

- stage, the side chain has only one member (ie. K) and K is the *creator* of this chain.
- K invites more people to join the new side chain, operate, deploy smart contracts, and use the chain for K's purpose

Become A Witness Node

Every stakeholder can also be a witness candidate. Stakeholders must have at least 250,00.00 UniWorld Cash (UNW) in their wallet. The following steps describe how stakeholder K become a witness:

- K deposits 250,000.00 UniWorld Cash (UNW) to K's wallet
- K creates a proposal transaction to become a witness node
- If K's transaction is valid, K will be listed as witness candidate and wait in line for the voting process
- Other stakeholders can see the list of witness nodes in the pool, and start voting for trustworthy nodes. The voting power depends on the total of tokens stakeholders have.
- The 55 witness node candidates that received the most votes will become the official witness nodes. The rest will remain in the pool for the next voting process. In case of a witness node failing to produce a block in time, waiting candidates may also become full witness nodes.

Incentive Model

To attract more people to UniChain, the following incentive model has been created:

For each epoch (1670 blocks) a checkpoint is created. Witnesses at the end of epoch iteration will be responsible for calculating the network rewards.

Tokens for the network reward in one year will be ~ 1% of total token (10 Millions token). It is equal to the annual inflation rate of 1%. The total token reward for each epoch are

$$RewardToken_{epoch} = \frac{TokenPerYear}{BlockPerYear} \times BlockPerEpoch = \frac{10.000.000}{60*60*24*365} \times 1670 \simeq 530\ tokens$$

The network reward tokens are divided into two portions: The first 40% go directly to the active witness nodes and the other 60% will be shared between stakeholders that voted for the witness nodes.

The reward tokens that a witness node may receive within one day are $60 \times 60 \times 24 \times 0.4/55 \simeq 628\ tokens$
Note that if stakeholders or witness nodes don't hold tokens at the end of the reward calculation time, they will not receive reward tokens.

Burning tokens

Unlike other Blockchain platforms, transaction fees on UniChain do not go directly to the block producers (witness nodes). It goes to a special address (*0x0000000000000000000*). No one knows the private key of this address (destroyed). Alas, the tokens are burned. Burning tokens makes UniWorld Cash (UNW) more valuable in the future. The table below shows some of transaction fees corresponding to burn

Transaction type	**Fee to burn (UniWorld Cash (UNW))**
Transfer token to account	0.0001
Register as witness node	1000
Create new side chain	5000
Vote for witness node	5

Call smart contract function	Based on smart contract complexity

V. UniChain Specifications

- Blocktime: 1s
- Transactions per second (TPS): Up to millions
- Block confirmation (finality) 1/s
- Native token: UniWorld Cash (UNW)
- Total token: 1.000.000.000 (one Billion tokens)
- Transaction fee: Based on computational complexity. the normal transfer token cost 0.0001 UniWorld Cash (UNW)
- Consensus algorithm: DPoS-HotStuff
- Number of witness node: 55 nodes
- Smart contract language: Solidity. (Nodejs and Java in the future)
- Digital signature algorithm: ECDSA
- Multi chain: Yes
- Cross chain communication: Yes

Popular Blockchain Beliefs versus UniChain

Technical Spec	Bitcoin	Ethereum	IOTA	EOS	UniChain
Consensus algorithm	PoW	PoW	Tangle	DPOS-BFT	DPOS and Hotstuff
Transactions per second (TPS)	3	15	300	Hundred thousand	Millions
Block time (second)	600	15	NA	~1	~1
Confirmation time (in seconds)	1800	150	NA	~1	~1
Smart contract	x	✔	x	✔	✔
Multi chain	x	x	X	x	✔
Cross chain communication	x	x	x	x	✔

Witness Node	x	x	x	✔	✔

VI. Conclusion

In this paper, we propose the combination and modification of many cutting-edge technologies towards UniChain. We believe Unichain is one of the most powerful blockchain platforms that meet the requirements for real applications (i.e. scalability, decentralization and security).
Our target is to have customers not only use Unichain not only being used in Uniworld ecosystem but also in every decentralized application around the world.

VII. Reference

(1) *Uniword ecosystem (https://uniworld.io) including UniBot (https://unibot.org), UniGreen, UniLab, UniChain (https://UniChain.world), Mia (https://mia.world) ...*

(2) *Shiroq Al-Megren, Shada Alsalamah, Lina Altoaimy, Hessah Alsalamah, Leili Soltanisehat,Emad Almutairi.* Blockchain Use Cases in Digital Sectors: A Review of the Literature

(3) *Dejan Vujičić, Dijana Jagodić, Siniša Ranđić.* Blockchain Technology, Bitcoin, and Ethereum: A Brief Overview

(4) *Maofan Yin, Dahlia Malkhi, Michael K. Reiter, Guy Golan Gueta, Ittai Abraham.* HotStuff: BFT Consensus with Linearity and Responsiveness

(5) *Ittai Abraham, Guy Gueta, Dahlia Malkhi, Lorenzo Alvisi, Ramakrishna Kotla, and Jean-Philippe Martin. 2017. Revisiting Fast Practical Byzantine Fault Tolerance. CoRR abs/1712.01367 (2017). arXiv:1712.01367*